THE UNIVERSITY
of EDINBURGH

MOBILE, INTELLIGENT AND AUTONOMOUS POLICING TOOLS AND THE LAW

Wiebke Abel

Doctor of Philosophy

University of Edinburgh

2012

Declaration

The work in this thesis is the candidate's own and has not been submitted for any other degree or professional qualification.

……

Wiebke Abel

Edinburgh

31 August 2012

Acknowledgments

My sincere thanks and gratefulness go to my principal supervisor Prof Burkhard Schäfer, without whom this thesis could not have been written. I am eternally grateful for his incredibly generous intellectual support and encouragement.
I am also sincerely grateful to my secondary supervisors Prof James Chalmers and Prof Gerry Maher for their valuable comments on early and late drafts, and their encouragement.

This research would not have been possible without the generous support by the Arts and Humanities Research Council, and the AHRC/SCRIPT Centre for Studies in Intellectual Property and Technology Law at the University of Edinburgh. I am grateful for having had the opportunity to work in such a stimulating environment, and am indebted to all my colleagues at the SCRIPT Centre for the thought-provoking discussions and their support. I am particularly grateful to Shawn Harmon, Lilian Edwards, Rowena Rodrigues, and Erin Jackson.

I also wish to thank the people at the Amsterdam Leibniz Centre for Law at the University of Amsterdam for welcoming me as a visiting researcher and assisting me with the technical parts of my thesis. Particular thanks go to Tom van Engers and Radboud Winkels.

Without the unconditional support of my husband, Andi Winterboer, this thesis would not have been finished. I will be forever grateful.
To my son, Ben, for his patience. To Lara, simply for being there and getting me out of the house.

Thanks also to my parents and my brothers for always believing in me.

Abstract

This thesis resolves around problems arising for the existing legal framework from the use of novel software-based policing tools during criminal investigations. The increasing dependence on information and communication technologies and the Internet means that more aspects of people's lives move online, and crime follows them. This has triggered the development of innovative, autonomous investigative technologies that are increasingly replacing human officers for the policing of the online sphere. While only recently discussions of the legal status of embodied and unembodied robotical devices have gained more widespread attention, discussions of the legal status of autonomous agent technology are not new. They have focussed however in the past on applications in the private domain, enabling contract formation online. No systematic study has so far been carried out that looks at the use of autonomous agent technology when deployed by state actors, to fulfil core state functions. This thesis starts with the hypothesis that the use of automated, intelligent devices to replicate core police functions in the online world will increase in the future. Looking at first emerging technologies, but with an eye towards future deployment of much more capable software tools that fulfil policing functions on the Internet, this thesis looks at the challenges this poses for regulators and software developers. Based on extensive qualitative research interviews with stakeholders from two different jurisdictions (Germany & UK) this thesis finds that these novel policing technologies challenge existing legal frameworks, which are still premised on the parameters of the offline world. It therefore develops an alternative governance model for these policing tools, which enables their law-compliant use and prevents rights violations of suspects. In doing so it draws upon both worlds, the technical and the legal, while also incorporating the empirical research results from the interviews with experts. The first part of this thesis analyses the technical foundations of these software-based policing tools. Here, one of the key findings is that the current governance system focuses on ex-ante authorisation of very specific, individual software tools without developing a systematic classification. This contradicts the principle of sustainable law making. To overcome this piecemeal approach, as a first contribution to existing research

this work defines a new class of investigative technologies – mobile, intelligent and autonomous (MIA) policing tools- based on the findings of the technical analysis. Identifying such a natural class of present and future technologies that pose the same type of legal issues should facilitate the sustainable governance of these new policing tools. The second part of this thesis analyses two specific legal issues: cross-jurisdictional investigations and the evidentiary value of the seized data. These issues were identified as most pressing by the experts interviewed for this work. This analysis reveals that investigative activities of MIA tools are potentially in conflict with international law principles and criminal procedure law. In order to gain legitimacy, these new policing tools need to operate within the parameters of the existing legal framework. This thesis argues that given the unique technical capabilities of MIA tools, the primary approach to achieving this is to assign legal responsibility to these tools. The third part of this thesis develops a novel governance approach to ensure that MIA tools operate within the parameters of the legal framework, and therefore obtain legitimacy and relevance, also with regard to the investigative results. This approach builds on existing research identifying code as a regulatory modality and contributes to the field of legal theory. It constitutes a solution for the governance problems of MIA tools, however, it requires currently lacking collaboration among stakeholders and cross-disciplinary research.

1 INTRODUCTION

Have you realised your computer's a spy?
(Pet Shop Boys, "Legacy", YES 2009)

a) Dreaming Futures: From Fiction to Fact

In *Roadside Crosses* by the American crime novelist Jeffrey Deaver,[1] a police detective together with an expert in computer forensics search for a young murder suspect who has disappeared before he could be arrested. What they know about him is his obsession with a MMORPG, a Massively Multiplayer Online Role-Playing Game, and the skill and knowledge he acquired in the game may also inform his criminal activity in the brick and mortar world. To discover his whereabouts, and also to collect evidence about his motives, character, abilities and connections to the victims, the two investigators too acquire game characters (avatars) and enter the online world. In their quest for evidence, they interact not only with the avatars, digital representations, of other human players who knew the suspect's online persona. They also interact with a non-player character (NPC), an Artificial Intelligence (AI) construct provided by the platform operators, in the shape of an elf princess. NPCs like this can populate the fictional world of a game. They can be allies or competitors to the player characters. Sometimes, they are just parts of the scenery. Crucially though, they can also carry out routine refereeing tasks, warning for instance a player that he is infringing one of the rules of the game world such as attacking players who are deemed too new or too weak – and if necessary even enforcing a sanction at the edge of their digital swords. In that case, the NPC will be completely defined through their statistics, "skills", and "gear" which can mean for instance that the NPC is powerful enough to "kill" any player character in combat.[2] NPCs can also collect data about other player and communicate it to third parties, acting in this case like an animated road sign. It is this function that the

[1] J Deaver, *Roadside Crosses* (New York: Simon & Schuster, 2009).

[2] On Non-player characters in general see B Mac Namee, P Cunningham, "A Proposal for an Agent Architecture for Proactive Persistent Non-Player Characters" in D O'Donoghue (ed) *Proceedings of the 12th Irish Conference on AI and Cognitive Science* (Dublin: Trinity College Dublin, Department of Computer Science, TCD-CS-2001-20) 221-232; On the use of NPCs as "referees" see G Sukthankar, K Sycara, "Policy Recognition for Multi-Player Tactical Scenarios" (2007) *Proceedings of the 6th International Joint Conference on Autonomous Agents and Multiagent Systems* (AAMAS '07), ACM, New York, 1-8.

two detectives use in their investigation, and the NPC duly directs them to the virtual house of the suspect. Learning that in the online world he plays a witch doctor, who dedicates his "life" helping other player recover, they reassess his psychological evaluation. Seeing how other human players in the game related to him further convinces them that he had not the deranged personality displayed by the killer in the offline world. Too poor to study medicine in the real world and subject to irreconcilable demands by parents, peers and authorities, he was only able to create a "coherent life plan" in a virtual setting which, free from the constraints of his offline life – poverty, gang culture, physical appearance etc – resulted in a life that in many ways was more true to his self than that permitted by the physical world. It is there that he can interact with others without prejudice or undue favour, and there that he can contribute to the good of his chosen community. [3]

From this story, several important lessons can be learned, and together they describe the aim and focus of this thesis.

The technologies described by Deaver are already available and used for gaming purpose. This thesis develops the idea that the future of online policing will soon (have to) follow similar lines. There is a natural extension from the concept of a "referee" to that of a police officer or even a judge – all of them are in the business of applying and enforcing rules. One reason for this trajectory is movingly described in the story, and has found recently a legal expression in a decision of the German Federal Constitutional Court: as we conduct more and more of our lives online, it becomes an essential, not just accidental aspect of our lives and our identity.[4] We are to a great extend defined by the relations we have with others. If all one's friends are Facebook friends, or avatars encountered in an online game, then one's digital identity determines a large part of who we are. Attacks on this digital identity, by criminals or states, threaten therefore the core of our being.

[3] For the role and importance of coherent life plans for law and legal reasoning about human rights, see J Finnis, *Fundamentals of Ethics* (Washington: Georgetown University Press, 1983) 103-126. For the application of this idea to the regulation of technology, see R Black, "Ethics and the Products of Science", in R E Spier (ed) *Science and Technology Ethics* (London: Routledge, 2002) 39-59.

[4] BVerfGE, NJW 2008, 822.

Gathering the information that describes these relationships allows an observer to form a complete picture of a person.[5] Living online lives therefore creates new vulnerabilities that the law needs to address. It creates also new possibilities for criminals. The digital, virtual nature of this environment makes some of the constraints that operate in the offline world redundant. One and the same natural person can use simultaneously several online identities in different online "worlds", - from games to Facebook to newsgroups to online banks or shops – and by virtually replicating himself also multiply his ability to violate laws. This thesis argues that AI systems, such as the NPC encountered in online games, will therefore be needed to create a corresponding multiplication of police officers, collecting and analysing the increasing amount of data, and also performing at least some basic policing function such as issuing warnings (or possibly fines), seizing evidence and preventing certain types of rule transgressions. Virtual and physical spheres will increasingly leak into each other.

In the Deaver story, information about the virtual life of the suspect gave them vital clues about his offline existence needed to solve the case. In the same way in which in the story, the suspect's "real" life and identity can be said to be his virtual ID, the dividing line between the virtual and the real will continue to get blurred, creating new social and legal-regulatory problems. Psychologists and sociologists have for some time described the impact of this virtualisation of life, where everything becomes essentially information.[6] Law by contrast is still catching up with this development. Even from the short description of the novel, some immediate legal questions arise: Should (or could) the officers have identified themselves as police officers when "interrogating" the AI about the suspect, and does failure to do so render the evidence it gives them inadmissible? Is it even reasonable to use the analogy of an "interrogation" in this context? What steps could and should have the officers taken to create a record of the online interaction that is reliable and admissible? If the game platform was owned by a foreign company and the server located in a foreign country, did they violate that state's territoriality by carrying out an investigation that involved "copying" their avatars on that server's drive? Is data about an avatar ("He lives in a

[5] As we will see in chapter 2, it was this ability to form a complete picture of a person by analysing the data about them that led the German Federal Constitutional Court to argue that online lives need the full protection of the "Human dignity" provision of the German Constitution.

[6] See e.g. S Turkle, *The Second Self: Computers and the Human Spirit* (Cambridge: MIT Press, 2005); S Turkle, *Life on the Screen: Identity in the Age of the Internet* (New York: Simon and Schuster, 1995); S Turkle, *Simulation and Its Discontents* (Cambridge: MIT Press, 2009).

cave in the next village and is a green ogre") of the type the AI gave the officers "personal data" for the purpose of the *Data Protection Act*, is it "about" a natural person, or "about" another type of entity, an avatar, that the law still has to define adequately? All these questions concern the interaction of human police officers with an AI, but what legal issues arise if the AI carries out police functions itself? Some writers have advocated that autonomous and intelligent systems may have one day to be recognised as juristic persons by the law,[7] but a much less contentious question can be posed: should such a system have a "rank" that integrates it into the chain of command of the police, and circumscribes its rights towards citizens?

If I, as a human computer user, am suddenly confronted with a pop-up of an avatar (similar to the one that greets customers on the IKEA website) that identifies itself as controlled by the police and asks me for information, can I refuse until a human officer makes the request, or can the computer, following its pre-programmed algorithm, have the power to change my legal status and create a duty to cooperate for me? How can we create functional equivalents of police activity through online simulations, what gets lost in this process, what is added, and how should the law react to this necessary distortion?

Human police officers interacting with citizens, suspects or victims, will for instance have a noticeable physical presence, which can intimidate or reassure. Even though reference to this aspect of policing will not normally be found in primary legislation regulating police work, common human experience of physical spaces and their invasion will have silently informed these laws. Interest in "non verbal", not text based aspects of law and legal reasoning have only recently come to the attention of legal theorist, for instance in the AHRC funded "Beyond Text" programme and the forthcoming collection of "Beyond Text in Legal Education."[8]

How the disappearance of such a shared understanding of the physicality of space is going to change the nature of Internet policing through autonomous systems that simulate police officers, and what it means for their regulation, will go beyond the remit of this thesis. It will however outline nonetheless a wider conceptual framework within which the analysis here is located: As some of the empirical studies carried out

---

[7] See e.g. L Solum, "Legal Personhood for Artificial Intelligences" (1992) 70 *North Carolina Law Review*, 1231-1287; W Adams, "Machine Consciousness: Plausible Idea or Semantic Distortion?" (2004) 11:9 *Journal of Conscious Studies*, 46-56; D J Calverley, "Imagining a Non-Biological Machine as a Legal Person" (2008) 22 *Artificial Intelligence & Society*, 523-537.

[8] Z Bankowski, M Del Mar, P Maharg (eds) *Beyond Text, vol 1: The Arts and the Legal Academy* (Farnham, Surrey: Ashgate Publishing, 2012).

for this PhD indicate, lawyers will always tend to reason by analogy from traditional, well established legal concepts to new, technology mediated phenomena. Indeed, they often prefer this approach to new, "tailor made" legislation. Part of this thesis will address the issue how we can through computer code represent those aspects of offline police work in the online environment that is necessary to make these analogies more likely to succeed, while advocating legal reform where the difference between disembodied and embodied policing becomes too wide to be bridged by computer code alone.

These research issues therefore deal also with the legal regulation of autonomous agents. Over the past decade, there has been an increased interest in this issue, with debate stimulated through the AGENTLINK network of the European Union[9] and the "Law of Electronic Agents" workshop series.[10] However, this research focussed mainly on commercial applications of autonomous agent technology and the legal issues that this raises.[11] This is understandable, since most of the working applications are at present in this field. For these applications, the law of agency and its associated liability regimes proved flexible enough to allow for equitable solutions for most scenarios without the need for substantial legal intervention. In private law settings, there is an underlying symmetry between the involved parties, an organising bi-polar relation exemplified e.g. by "seller" and "buyer" (or injured party and injurer).[12] These however are not natural kinds with mutually exclusive membership – we all can be sometimes buyers, and sometimes sellers, and sometimes we are both in the same transaction. The cooperative aspect of private law and the commutability of legal roles

---

[9] http://www.agentlink.org/index.php.

[10] http://www.lea-online.net/; see e.g. F Andrade, P Novais, J Neves, "Will and Declaration in Acts Performed by Intelligent Software Agents - Preliminary Issues on the Question" in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005) 53-55; M Zwanenburg, H Boddens Hosang, N Wijngaards, "Humans, Agents and International Humanitarian Law: Dilemmas in Target Discrimination" in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005) 45-51.

[11] See e.g. A Rotolo, G Sartor, C Smith, "Formalization of a 'Normative Version' of Good Faith" in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005), 65-76; J Gelati, R Riveret, "DRM in a Multi-Agent System Marketplace" in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005) 123-139; J Calmet, R Endsuleit, in A Oskamp, C Cevenini, "An Agent Framework for Legal Validation of E -Transactions" (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005) 181-184

[12] See e.g. E J Weinrib *The Idea of Private Law* (Harvard: Harvard University Press, 1995).

means that there is no identifiable group that would benefit from a one-sided prohibition against extending e.g. the law of agency to autonomous agents.
In a criminal law setting however, these are not operative. We cannot simply apply the law of agency, as a police officer cannot normally confer his rights and duties to a civilian third party. Police officers often have certain rights not available to ordinary citizens – searching premises and seizing goods for instance. On the other hand, they might be under legal obligations that go beyond of what is required of ordinary citizens, such as a duty to act on knowledge of criminal activity. Unlike in private law, these special rights and duties that people have in virtue of their public law function create relatively fixed, mutually exclusive interest groups, e.g "state" vs "citizen". Regulation through markets, one of the most prominent modes of regulation of commercial technology, is therefore of limited applicability.[13]
The thesis is premised on a vision of the future where core policing functions are carried out by autonomous entities. Nonetheless, most of the discussion in the thesis will look at less sophisticated technology. This will not only ground this work in a present day, real life scenario, it will also facilitate the development of a more abstract concept of computer assisted online policing that is less dependent on any specific technology. This thesis argues in particular that the use of Trojans, a piece of software that shares some, but not all features with an autonomous agent, is already raising all those legal issues that the more "excotic" future that we glimpsed from Deaver's novel raises.

b) From Fact to Fiction

The increasing dependence on information and communication technologies (ICTs) has profoundly affected the lives of people and changed society in many ways.

> *"Often, the Internet allows people to do exactly what they have done before, yet with much greater efficiency. Such activities do not raise any genuinely new legal issues in the strict sense and at first seem wholly unremarkable, yet their ordinariness is deceptive, as they question the efficacy of legal regimes which had previously relied upon the impracticability of engaging in certain conduct."*[14]

---

[13] See in particular B Schafer, M Rodriguez-Rico, W Vandenberghe, "Undercover Agents and Agents Provocateur- Evidence Collection by Autonomous Agents and the Law", in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005) 155-170.
[14] U Kohl, *Jurisdiction and the Internet* (Cambridge: Cambridge University Press, 2007) 37.

Maybe the most drastic transformation has occurred in the area of communication, and especially data exchange and processing. The networked design of the Internet has prompted the transition to an information society that increasingly depends upon digital communication and computation infrastructures.[15] In this networked world, physical distance and country borders are irrelevant, and instant communication and data exchange primary functions. Everything that is online is data, and in this sense, all Internet laws are laws about the flow of information.

This development has significantly changed the way people interact and communicate, and exchange information and data. As a result, more aspects of people's lives have moved to digital networks and with this shift to the digital sphere, people have developed a life online. This virtual living space has created entirely new opportunities, with sometimes unprecedented consequences for societies and governments. [16]

However, this shift has also created a dependency on the Internet and digital networks, and this has created new vulnerabilities and prompted new ways for criminals to exploit these. [17] Many existing crimes can be replicated in online environments, [18] and new types of criminal behaviour, exploiting the digital infrastructure, have emerged. [19] Criminals have become more mobile in their operation, using ICTs and the Internet to form international networks that cross the borders of nation states. Terrorism in particular has moved away from strict hierarchies to flexible organisations that mimic modern business models and allow small groups high degrees of autonomy.[20]

---

[15] For an overview of the technical foundations and the history of the Internet see e.g. J Bing, "Building Cyberspace: A Brief History of Internet" in L A Bygrave, J Bing (eds.) *Internet Governance: Infrastructure and Institutions* (Oxford, New York: Oxford University Press, 2009) 8-48.

[16] One recent example for this is the use of social media applications during the Middle East revolutions. See e.g. P Beaumont, "The Truth about Twitter, Facebook and the Uprisings in the Arab World" *Guardian*, 25 February 2011, available online at: http://www.guardian.co.uk/world/2011/feb/25/twitter-facebook-uprisings-arab-libya.

[17] See e.g. D S Wall, "The Internet as a Conduit for Criminal Activity" in A Pattavina (ed) *Information Technology and the Criminal Justice System* (London: Sage Publications, 2005) 77-98, stating that the Internet has had a major impact upon criminality.

[18] See e.g. S Balganesh, "Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass" (2006) 12 *Michigan Telecommunications and Technology Law Review*, 265, for a discussion of the problems of applying real world legal concepts to the online world.

[19] See e.g. P Hunton, "The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model" (2009) 25:6 *Computer Law & Security Review*, 528-535 for an analysis and discussion of cybercrime.

[20] See e.g., B Tupman, "Where has all the money gone? The IRA as a profit-making concern" (1998) 1:4 *Journal of Moneylaundering Control*, 32-40; A Zelinsky, M Shubik, "Terrorist Groups

This shift to the digital sphere also alters the understanding of crime in different ways, an idea that is expressed in this thesis through a focus on "blurred borders". Arguably the most significant change is the shift of the crime scene from the physical to the digital sphere, and a blurring between physical reality and simulation. This development challenges existing police organisation and legal process because the characteristics of the digital world differ significantly from those of the physical world.

When thinking about the future of policing and law in an age of such porous borders, what comes to mind first are the geographical borders between states. "In cyberspace, events occur almost instantaneously across large distances, network boundaries do not align with physical and political boundaries, and everyone on the network is your neighbour."[21]

Physical crime scenes do not travel well – which is why we sometimes bring jurors to the actual scene of a crime, as the direct experience conveys information that its translation into witness statements or expert transcripts, that is data, can't. Digital evidence, generated in cyberspace, however will often exist on servers distributed over several countries, and can therefore be accessed and collected from more than one country. Crime in cyberspace is not bound by physical geography and can inflict harm across jurisdictional borders. This complicates the investigation process and reduces the chances of successful prosecution.

In conceptualising the porous borders between cyberspace and physical space, the question changes from one of geographical territory to that of "conceptual spaces". Geographical metaphors, while heuristically helpful, quickly reach here the limits of their usefulness.[22] More generally, the real issue is often one of conceptual borders between abstract legal contexts more than one of geographical borders. For example, it does not matter so much where Guantanamo Bay is located geographically, but where it is located "conceptually", that is within or outside the jurisdiction of US courts and their habeas corpus protection.

---

as Business Firms: A New Typological Framework" (2009) 21:2 Terrorism and Political Violence, 327-336.

[21] J M Balkin, N Kozlovski, "Introduction" in J M Balkin, J Grimmelmann, E Katz, N Kozlovski, S Wagman, T Zarsky (eds) *Cybercrime: Digital Cops in a Networked Environment* (New York, London: New York University Press, 2007) 1-12, 2.

[22] One could think in this context of the notion of "safe harbour", in data protection contexts, a problematic metaphorical use of a geographical notion taken from traditional international public law and applied to the conceptual issue of data transfer across borders in cyberspace.

The example of evidence collected from cyberspace indicates a second porous border, this time a border between the virtual and the real, digital evidence and concrete physical evidence. In a highly complex process, electronic traces are eventually transformed into hard, tangible printouts.[23] In crossing the border between the digital and the physical, the nature of the evidence changes, raising numerous problems for procedural law. Where, exactly, in this process is "the" evidence located? What is "the" original piece of evidence?

Traditional investigative measures, designed for the offline world, are more than often insufficient for the investigation of the online world. Thus the blurring of the digital and the physical world has prompted the development of a new cyber-policing system and new software-based investigative tools.
This indicates another porous border, which in the past was perceived as rock solid: the border between normative and descriptive discourses. Lessig's influential work on "code as code" has alerted us to the potential of cyberspace to replace traditional normative and legal debates with questions of software programming.[24] The design of the Internet, its networked software and hardware environment, is a central device for regulating network activity. Where traditional normative legal thinking analysed for instance copyright law as including a set of sanctions for copyright violations, norms that required application of the law by courts to a situation, digital rights management can be seen as a self-applying, descriptive version of the same law that makes violation of the legal norm physically impossible. This also has an enormous influence on the practical liberty and privacy that people enjoy online.[25]

This thesis predicts that the new cyber-policing system will take this to another level, by complementing or even replacing human police officers and traditional forms of policing with software-based investigative tools and cyber-policing. This new cyber-policing system will have to be at least partly automated – one has just to consider the

---

[23] For an analysis that also analyses the "borders" between physical and digital evidence see B Carrier, E Spafford, "Getting Physical with the Digital Investigation Process (2003) 2 *International Journal of Digital Evidence*, 1-20.
[24] L Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).
[25] L Tien, "Architectural Regulatioin and the Evolution of Social Norms"in J M Balkin, J Grimmelmann, E Katz, N Kozlovski, S Wagman, T Zarsky (eds) *Cybercrime: Digital Cops in a Networked Environment* (New York, London: New York University Press, 2007) 37-58.

amount of "crime data" Nigerian spam emails alone generate, something that makes every private computer, doctrinally, a potential crime scene. It is much more pervasive than traditional forms of policing and mainly preventive. It calls for ubiquitous policing of online activities to monitor, detect, prevent and control potentially malicious activities.
The architecture of this virtual cyber-policing environment is designed to enable ubiquitous surveillance and targeted monitoring of suspects.
The new cyber-cops are, contrary to human police officers, invisible and operate according to software-design paradigms instead of a mix of formal laws and human discretion.

With these new forms of policing and surveillance come new dangers for civil liberties. The new cyber-policing system is largely emerging without a dedicated legal framework. There is, as shown later in this thesis, an increasing danger that existing laws and regulations governing police operations can be sidelined debates about fundamental rights transformed into technical discussions about software protocols. The use of the investigative results of these cyber-policing systems is therefore highly questionable, and it remains to be seen whether the results they deliver would stand up in court.

It is therefore critical to develop approaches to resolve this uncertain situation. At this stage, the legal framework is ill-equipped to deal with the new policing system. Criminal procedure law fulfils the dual task of enabling policing operations on the one hand, and restricting them on the other to protect citizens from arbitrary state power. It aims to allow those policing actions that are reasonable, proportional, and accountable. Criminal procedure law is, however, deeply rooted in the traditional policing system, which is mainly reactive to crime and is tailored to the physical crime scene and evidence. It also assumes that human officers execute the policing actions and is premised on concepts such as "human discretion", "reasonable suspicion", "balance" and other concepts that refer explicitly to mental states. It thus struggles equally with the enabling and restraining of the new cyber-policing system, and particularly the use of cyber-cops.

In this thesis I draw upon both worlds, the technical and the legal, to develop a solution for the uncertain state of cyber-cops and cyber-policing.

I argue that the time to develop new legal mechanisms is now, while the cyber-policing technologies are still being developed to avoid rushed and ill-drafted legislation and policies, as well as illegitimate use of new powers.

I draw upon a recent, well-documented example of a new software-based investigative power to determine how the law currently handles the use of these technologies. One outcome of this analysis is that the precise technical nature of these new technologies needs to be determined to develop an adequate regulatory framework for their use.

By analysing recent findings in computer science and artificial intelligence, I develop a new class of policing technologies –mobile, intelligent and autonomous policing tools – and determine how these cyber-cops operate and what their policing environment is.

Based on these results and the findings of empirical research conducted for this work, I examine how the law deals with the two most pressing problems of the use of these new investigative technologies: cross-jurisdictional policing, and the use of "technologically mediated data" as evidence of the investigative results. I argue that these new software-based policing and surveillance tools are potentially in conflict with existing international law principles and criminal procedure laws.

I argue that the primary approach to achieving legitimacy for digital investigators is an application of the "equivalence principle": Just as for citizens, what is prohibited offline is also prohibited online, so for the state and its agents. Technology must not be used to circumvent rules that restrain police power, just because it is not necessarily wielded any longer by a physical being. One such response is to assign legal responsibility for their actions to these cyber-cops. Just like their human counterparts, these cyber-cops must adhere to the rules enabling and restraining their actions, but unlike human beings, at least some of these rules will have to be integrated into the software design itself, to get as close as possible to the functional online equivalent, for legal purposes, of a human state of mind.

So far, software-based investigative and surveillance tools have been developed with no attention to their unique programmability to ensure legality and legitimacy.

Legislators and courts have further contributed to this deficit by refusing, or ignoring the option, to collaborate with technical disciplines on this.

By combining legal and technical findings, I therefore develop a novel approach to ensure that the software-based investigative and surveillance tools operate within the parameters of the legal framework, and therefore obtain legitimacy and relevance, also with regard to the investigative results.

1.1 Background and Motivation

Ever since the 9/11 terrorist attacks, many western governments investigated ways to improve national security.

Among the measures implemented in the US were the *USA Patriot Act*[26] and the foundation of the Total Information Awareness Office (TIA), which was later renamed to the less ominously sounding (Terrorist) Information Awareness Office.[27]

In the UK, the *Anti-Terrorism, Crime and Security Act 2001* was introduced as a reaction to the attacks.[28] However, it has since been replaced by the *Prevention of Terrorism Act 2005*.[29] In addition, as a response to the 2005 London bombings the *Terrorism Act 2006* was introduced in the Uk.[30]

In Germany, the *Gesetz zur Bekämpfung des internationalen Terrorismus* (Terrorismusbekämpfungsgesetz – Law to fight terrorism) was introduced in the aftermath of the 9/11 attacks as a measure to combat terrorism.[31]

One reason for the rushed legislation in these countries was the inability of intelligence agencies to predict and prevent the 9/11 terrorist attacks. It became clear that the intelligence infrastructure was unable to cope with terrorism as a form of low-

---

[26] The *USA Patriot Act* was signed into law on October 26, 2001. The title of the act is an acronym that stands for "Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001.

[27] The Terrorist Information Awareness Office was discontinued when funding was repealed in September 2003 (Conference Report on H.R. 2658, Department of Defense Appropriations Act 2004, House Report 108-283).

[28] It was formally introduced in Parliament on 10 November 2001 and came into force on 14 December 2001.

[29] The *2005 Act* was a reaction to the Law Lord's ruling of 16 December 2004 that Part 4 of the *Anti-Terrorism, Crime and Security Act 2001* was incompatible with European human rights laws. The *2005 Act* stands to be repealed by the *Terrorism Prevention and Investigation Measures Bill 2011*.

[30] The Act was introduced on 12 October 2005 and came into force on 30 March 2006.

[31] The Law came into force on 1 January 2002.

intensity/low-density warfare.[32] The main problem was that different agencies involved in detecting the information trails that terrorists usually leave behind were unable to recognise, collect, and share the available information. This was also partly due to the fact that the Internet and ICTs have changed the way terrorist networks are structured.[33] They operate as covert networks, oftentimes with the single links of the network uninformed about the others.

In 2007, German law enforcement authorities officially introduced a new investigative method to address the difficulties faced by these new structures: the remote and automatic online searching of computers and other ICT devices using a specifically designed piece of software.[34] The aim of introducing this new investigative method was to clandestinely monitor web communications and information stored on ICT devices. The introduction of this method caused much discussion and debate among both legal and technical experts.

The idea of deploying a piece of software to undertake investigative actions was unprecedented and issues concerning, among others, privacy and data protection rights of affected suspects, as well as concerns regarding the sophistication of the piece of software arose.

However, the idea of clandestinely monitoring suspects online and searching the data stored on their ICT devices was compelling not only to German authorities but also to other governments in Europe and beyond.[35]

The idea that information plays a key role in fighting terrorism (or any other form of criminal conduct) stems from the Baconian idea that 'knowledge is power'.[36] Modern society, with its widespread use of ICTs, provides unprecedented possibilities to obtain data and communicate, and thus it seems that Bacon's aphorism is especially relevant within our networked 'information society'. Gaining access to this data is therefore of

---

[32] F G Hoffman, "Complex Irregular Warfare: The Next Revolution in Military Affairs" (2005) 105:1 *The Military Balance* 411-420.

[33] See for a discussion of this V E Krebs, "Uncloaking Terrorist Networks" (2002) 7:4 *First Monday*.

[34] See chapter 2 for a detailed analysis of this.

[35] See chapter 2 for a more extensive discussion of this, and for an example the recommendation of the Council of the European Union on this topic, 'Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime', 2987th Justice and Home Affairs Council meeting, 27 – 28 November 2008, available at http://www.ue2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf.

[36] F Bacon, "Meditationes Sacrae" (1597), in J Spedding, R Ellis, D Heath (eds), *The Works of Francis Bacon* (1887-1901), Vol. 7, 253.

utmost interest for law enforcement agencies, and potential legal and technical issues of new investigative methods are oftentimes ignored until acute problems emerge. Most of the times these are then addressed individually and frequently with rushed or ill-drafted measures, which do not sufficiently address the technical issues at hand, as well as the technological development of the foreseeable future.

This is also true for the introduction of the online searching of ICTs in Germany.[37] On this occasion the highest German Court for constitutional matters, the Bundesverfassungsgericht (German Constitutional Court) was called to decide upon the constitutionality of the measure. However, such high court reasoning only very rarely provides a detailed framework for the use and regulation of a new investigative measure.

On this occasion,[38] the reasoning was technically even exceptionally well grounded. The result, however, was a highly conceptual judgment about the protection of fundamental rights (particularly privacy and data protection rights) online. The judgment in itself is of great importance for future regulation of ICTs and the Internet. However, as court decisions often do, it addressed mainly the nature of the right that was infringed, and the question of legal consequences for such an infringement. It is less helpful to direct the actions of future software developers and police agencies to develop law compliant strategies, a "middle ground" between the highly abstract and conceptual reasoning of the German Federal Constitutional Court and the purely technical issues of programming standards that this thesis tries to cover. Hence at present, the legal questions, concerns and issues pertaining to the use of this investigative tool persist.[39]

The importance of the online search and similar investigative measures for future police investigations is evident given the importance that ICTs and the Internet have gained in societies. This is also confirmed by recent disclosure about the ongoing deployment of this investigative measure in Germany and other countries despite the unsolved legal and technical issues. This has been heavily criticised and it has been

[37] See for more details chapter 2.

[38] BVerfG, NJW 2008, 822.

[39] See e.g. H Bleich, "Staatstrojaner: Mehr als 50 Einsätze bundesweit" *heise*, 16.10.2011, available online at http://heise.de/-1361857 , discussing that the online searching of computers was undertaken more than 50 times since its introduction.

stated that further research into the legal and technical aspects of this investigative measure is necessary before it can be deployed legally.[40]

These acute problems combined with the future relevance of this new investigative method were the motivation for focusing on the topic of new mobile, intelligent and autonomous policing tools and the legal and technical problems thereof.

1.2 Precise Formulation, Research Goals and Questions

The question this thesis answers is whether existing legislation regulating police investigations and evidence gathering, and the admissibility and interpretation of this evidence in court is sufficient and adequate to regulate the use of mobile, intelligent and autonomous (MIA) policing tools.

1.2.1 Research Goals

1. Development of a definition of MIA policing tools as a generic concept that covers present-day Trojans and any possible future, more intelligent and autonomous, agent technology, and evaluate this technology and its use during investigations;
2. Evaluation of the existing legal framework regulating police investigations in the light of MIA policing tools;
3. Development of a novel regulatory model to adequately govern the use of MIA policing tools that demonstrates how specific legal provisions can be embedded in software code, while for other issues a conceptual rethink of legislative responses may be needed

1.2.2 Research Questions

1. What are MIA policing tools and how are they being used by law enforcement and secret service agencies?
2. How will the use of MIA policing tools influence police investigations?
3. How will the use of MIA policing tools impact/challenge the legal framework regulating police investigations.
4. In order to safeguard privacy and security of suspects and the integrity of police investigations and findings how must the use of MIA policing tools be regulated?
5. How can we represent key legal concepts from evidence law and police practice into computer code to bridge the gap between offline and online policing?
6. What legal responses are conceivable to address those remaining issues that cannot be addressed through code based solutions?

[40] See e.g. J Kuri, "Staatstrojaner: Von der 'rechtlichen Grauzone' zur Grundrechtsverletzung" *heise*, 10.10.2011, available online at http://heise.de/-1357873.

1.3 Methodology

Most of the research for this thesis is traditional doctrinal text-based research. However, this research methodology has two significant shortcomings for adequately assessing this specific topic. Firstly, publicly available information about the details of the envisaged investigative tools is scarce and oftentimes based on speculation rather than facts. Secondly, as identified above, the problem that legal scholars and practitioners are ignoring the technical aspects of the topic at hand.

This required a deviation from the traditional text-based legal research methodology. To ensure that the research conducted for this thesis is based on valid facts and therefore timely and well-grounded, empirical research in form of interviews with relevant stakeholders from Germany and the UK was conducted.[41]

Given the confidential nature of police and secret service investigations exact details about the new software-based investigative tools for investigations of the virtual living space were not released to the public domain. However, relevant research is only possible when based on facts and sufficiently detailed and reliable information. This is particularly the case if the research is focused on an entirely novel technology, in this case the new investigative software designed to conduct investigations of the virtual living space.

The stakeholders relevant for this work are representatives from relevant governmental departments (e.g. Ministry of Justice), law enforcement, regulatory authorities and Internet Service Providers (ISPs). In addition, to gain a better understanding of the technical aspects of this investigative measure, a technical expert from the Chaos Computer Club with a relevant background and understanding of the topic was selected.

These interview results significantly shaped the structure and foci of the thesis, making it highly relevant for current policymaking and practice.[42]

In addition to the empirical research element, to ensure that sufficient technical expertise was incorporated into the technical part of the thesis, a study visit to the Leibniz Center for Law at the University of Amsterdam was incorporated into the PhD study. The Leibniz Center for Law is a world-renowned research hub for studies in law and artificial intelligence. Collaboration with researchers there ensured that the

[41] See chapter 3 for details.

[42] See below section 1.4 for an outline of the thesis.

technical parts of the thesis are correct and relevant. Feedback and discussions also influenced and shaped the technical analysis.
Furthermore, empirical research conducted as a partner on two European Union projects has backed up the interview results and the legal analysis.[43]
These deviations from traditional legal research ensured that the thesis is significant and of relevance for the current and future debate of ICT based investigative tools, as well as useful to stakeholders faced with the legal and technical issues surrounding these novel investigative tools.

1.4 Thesis Outline

The structure of this thesis reflects the importance of the cross-disciplinary approach of the chosen research topic. It also highlights the relevance of the empirical research results and reflects how these are incorporated into the work.
Accordingly, the chapters are structured as follows:

Chapter 2 The Case Study – The German Federal Trojan
This chapter introduces the main focus of the thesis: the policing of the virtual living space and technical and legal problems thereof. It does so by discussing an example in point: the recent introduction of a new software-based investigative power for police and secret services in Germany, and the legal and technical problems resulting thereof.

Chapter 3 Empirical Research Results
This chapter summarises the findings from interviews with different stakeholders from the UK and Germany involved in the regulation of the online world (government, law enforcement, industry, technical experts, and regulators). These findings highlight the theoretical assumptions of this thesis, and in addition identify the problems and challenges stakeholders are currently facing.

Chapter 4 Software-Based Investigative Tools
This chapter determines the technical nature of the proposed new software-based investigative tools to undertake investigations of the virtual living space, such as online searches of ICT devices. In addition, it illustrates how the use of these software-based

[43] See chapter 3, p. 77 for more details.

investigative tools and other related technologies change the nature of criminal investigations.

Chapter 5 MIA Policing Tools

This chapter develops a new class of future software-based investigative tools – mobile, intelligent and autonomous (MIA) policing tools.

Chapter 6 Cross-Jurisdictional MIA Investigations

This chapter discusses the problem of intentional and unintentional cross-jurisdictional investigations of ICT devices resulting from the deployment of MIA tools.

Chapter 7 Double Digitality

This chapter discusses the problems of digital evidence for the law, and in particular the problems arising from the "double-digital paradigm", meaning software tools (MIA tools) seizing digital data without direct human supervision.

Chapter 8 MIA Law

This chapter builds on the technical possibilities of MIA tools, and the legal problems identified above. It develops the regulatory model: MIA law, and analyses in how far endowing MIA tools with legal reasoning capabilities is a suitable reguklatory approach for the new class of investigative technologies, building on findings in legal theory and computational legal theory.

Chapter 9 Soft MIA Law

Building on the previous chapter, a novel approach of regulation through code is introduced here. The specific legal problems identified in the previous chapters are taken into account.

Chapter 10 Conclusion

This chapter summarises the findings of the thesis and the contributions made to the field of research. It also discusses issues that are relevant but not discussed in this thesis, and identifies issues where further research is required.

2 THE CASE STUDY – THE GERMAN FEDERAL TROJAN

The nature of crime has partially changed due to the shift from the physical to the digital world, and the increased dependence of people on the Internet and ICTs. Crime scenes and evidence are now often located in the digital sphere, where the parameters of the physical world are not applicable.

A recent example illustrating this is the introduction of a new software-based investigative tool for police and secret services in Germany, which allows the remote online searching of ICT devices, and particularly computers with a piece of specifically designed software.[44]

This example serves as the main case study for this thesis and is discussed and analysed in detail in this chapter. The reasons for selecting this example as the main case study are twofold.
Firstly, this example has generated a (comparatively) large amount of policy discussions[45] and case law from both, the German Federal Court of Justice (Bundesgerichtshof - BGH)[46] and the German Federal Constitutional Court (Bundesverfassungsgericht - BVerfG).[47] These publicly available discussions are important examples of the approach currently adopted for the regulation of the new cyber-policing system, where the focus is often solely on individual new policing tools. Even though the technology is comparatively task-oriented and simple, as will be shown it exhibits already all the problematic aspects that future, more intelligent and more autonomous systems will also have to address.
Remarkably, this seems to have been spotted by the BVerfG in its judgment, which went beyond focusing solely on the legality or illegality of the specific new investigative power but developed important legal concepts and a new basic right pertaining to the

---

[44] See e.g. D Fox, "Realisierung, Grenzen und Risiken der 'Online-Durchsuchung'" (2007) 31:11 *Datenschutz und Datensicherheit*, 827-834; C Herrmann, *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität – Entstehung und Perspektiven* (Frankfurt/Main: Peter Lang, 2010); H Pohl, "Zur Technik der heimlichen Online-Durchsuchung, (2007) 31:9 *Datenschutz und Datensicherheit*, 684-688.
[45] See e.g. Kleine Anfrage Deutscher Bundestag, "Online-Durchsuchungen" (2007) *Deutscher Bundestag Drucksache* 16/4795; Kleine Anfrage Deutscher Bundestag, "Bilanz der Online-Durchsuchung" (2010) *Deutscher Bundestag Drucksache* 17/1629.
[46] BGH, NJW 2007, 930.
[47] BVerfG, NJW 2008, 822.

use of the Internet, data online and the (cyber-) policing thereof. This judgment in particular is therefore of great importance for this thesis, because it serves as a first indicator of how the cyber-policing system as a whole changes under the influence of technology, and can be classified and regulated.
Secondly, this example provides details about the type of software-based investigative tools, and highlights how these cyber-cops are deployed and operate during criminal investigations.

In addition, the introduction of this particular new investigative method has also been discussed on European level, and other countries such as the UK have indicated to deploy it, which adds to the significance of this example.

In section 2.1 of this chapter the new investigative method is briefly introduced. This is followed by a discussion of the initial German judgments by the BGH, highlighting the problems with the current approach to regulating cyber-policing techniques in section 2.2. Section 2.3 analyses the judgment of the BVerfG. In section 2.4 the newly developed basic right to confidentiality and integrity of information technology systems is discussed. Section 2.5 analyses the reasoning process of the BVerfG. Section 2.6 critically evaluates the judgment and identifies its shortcomings and existing research gaps. Section 2.7 determines the relevance of this investigative method by briefly looking at its wider European use. Section 2.8 concludes with the main findings of the chapter.

2.1 The Investigative Measure

Several terms exist in Germany for the new investigative measure: “online search”, “remote searching”, “remote forensic tool”, or “Federal Trojan”. These different names might suggest that different investigative methods are referred to, and in some cases, it can be seen that problematic connotations of the chosen term can result in legal distinctions that are not necessitated by the actual features of the software.
The names o*nline search* and *remote searching* suggest a measure similar to a traditional search of premises.
Remote forensic tool suggests that the name refers to an investigative tool that seizes evidence remotely in a forensically sound way, and results can be used as evidence in court.

By contrast *Federal Trojan* has a negative connotation and implies the use of malware-like software tools by law enforcement agencies (LEAs). While this may have been an intended outcome of coining the term, a rhetorical ploy to delegitimise it from the outset, this carries the danger that any legal response will be restricted to software that has Trojan-like features, overlooking the more worrisome aspects of the technology. In fact, all refer to the remote and clandestine infiltration of a computer or other ICT device through technical means, using a piece of software to access and copy the data stored on the device, monitor communication and transfer all results back to the investigating authority.

The existence of these different names for one and the same investigative method is an indicator for the insecurity and lack of knowledge surrounding this topic.

The proposed new investigative method has caused extensive discussion and speculation on academic[48] and political[49] level in Germany, because little publicly available, factual information about the technical and practical details of the measure exist.

At the core of the discussion were concerns pertaining to the classification of the measure and its integration into the existing rights canon regulating police investigations and protecting privacy and data protection rights of affected persons,[50] and its technical feasibility. Both, the German Federal Court of Justice (Bundesgerichtshof - BGH) and the Federal Constitutional Court (Bundesverfassungsgericht - BVerfG) were called to decide on this matter and to

---

[48] See e.g. Fox, note 44; Pohl, note 44; K Leipold, "Die Online-Durchsuchung", (2007) 4 *Neue Juristische Wochenschrift Spezial* 135; U Buermeyer, "Die 'Online-Durchsuchung' – Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme", (2007) 4 *Höchstrichterliche Rechtsprechung im Strafrecht* 154; A Roßnagel, "Verfassungspolitische und verfassungsrechtliche Fragen der Online-Durchsuchung" (2007) 8 *Deutsche Richterzeitung*, 229-230; J Rux, "Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden – Rechtsfragen der 'Online-Durchsuchung'" (2007) 6 *Juristenzeitung*, 285-295; M Kutscha, "Verdeckte 'Online-Durchsuchung' und Unverletzlichkeit der Wohnung" (2007) *Neue Juristische Wochenschrift*, 1169; G Hornung, "Ermächtigungsgrundlage für die Online-Durchsuchung und –Beschlagnahme" (2007) 31 *Datenschutz und Datensicherheit*, 575; Hansen/Pfitzmann, "Technische Grundlagen von Online-Durchsuchung und –Beschlagnahme" (2007) 8 *Deutsche Richterzeitung*, 225-228; M Gercke, "Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit" (2007) 23:4 *Computer und Recht* 245-253.

[49] See e.g. S Krempel, "Bundesregierung gibt zu: Online-Durchsuchungen laufen schon" (2007) heise, available online at http://www.heise.de/newsticker/meldung/88824; D Borchers, "Schäuble heizt nach BGH-Urteil Debatte um Online-Durchsuchung an" (2007) heise, available online at http://www.heise.de/newsticker/meldung/Schaeuble-heizt-nach-BGH-Urteil-Debatte-um-Online-Durchsuchung-an-142623.html.

[50] See e.g. Hornung, note 48.

establish legal certainty.[51] To prepare the ground for the analysis of these developments in the next sections of this chapter, a short introduction of the proposed measure is given here. This description purposefully remains brief since a more detailed analysis of the relevant technologies will follow in chapters 4 and 5 of this thesis.

Generally, this novel investigative method tries to accommodate the difficulties during investigations that emerge if criminal offenders, in particular those from extremist and terrorist groups, use the Internet for communication and the planning and commitment of criminal offences.[52] The purpose of remotely infiltrating a computer is to enable investigators to search the data stored on the hard disk and the working memory of the computer, to intercept the email traffic, and monitor web browsing habits and instant messaging.[53]

To accomplish this, a specifically designed piece of software is planted on the suspect's computer without his knowledge.[54] This software tool is capable of autonomously searching and copying specific data stored on the computer and subsequently transferring this back to the investigating authority for evaluation. This requires the software tool to be equipped with certain key abilities, such as mobility to move across platforms, acting with a degree of autonomy, and possessing a certain level of intelligence to undertake the selection and monitoring process.

Hence, such a tool shares crucial features with well-known malware, particularly viruses and Trojans.[55] The latter in particular can be used to access and extract personal data from targets, and hence is equally suitable for data collection by police authorities. As indicated above, this is why the software is often referred to as "Federal Trojan" in Germany.

The advantage of deploying this new investigative software is that it can be installed clandestinely, and without access to the suspect's house or physical premises. It is designed to be disguised as something harmless, when it actually includes malicious or harmful code, and therefore tricks the suspect into installing it. Therefore, as with their

---

[51] See BGH, NJW 2007, 930, and BVerfG, NJW 2008, 822.
[52] BVerfG, NJW 2008, 822 (826).
[53] See Leipold, note 48.
[54] See Hansen/Pfitzman, note 48.
[55] U Buermeyer, "Die 'Online-Durchsuchung' – Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme", (2007) 4 Höchstrichterliche Rechtsprechung im Strafrecht 154.

criminal counterparts, police Trojans require the unwitting cooperation of the target.[56] Such an act of cooperation can, for example, simply be the opening of an email, for instance an email that purports to come from a bona fide state agency such as the local council or the Department for Pensions. However, while the above method is a likely possibility, LEAs or the government have provided no specific indications of how the infiltration is to occur. The unwitting cooperation of the suspect in the investigative process should raise immediate legal questions. It sets the online search apart from traditional search methods – where the suspect either gives consent to the police officers entering his premises, or is compelled to suffer that intrusion through a warrant, or officers may clandestinely, but without his help enter his flat to place e.g. a listening device. Remote online searches combine aspects of both approaches, requiring a degree of cooperation while aiming at an unobserved intrusion. This should raise the question how this cooperation should be legally evaluated. If the software is thought of as a proxy of a police officer, is "permitting" it on your computer the equivalent of permitting an officer (an undercover officer?) into your house? Does this alone change your legal status?

Some of the cooperation could be designed to be quite elaborate and with the legal issues in mind. For example, a suspect accessing the council website to register his car. A pop-up window appears with a long scroll down text that requires to "tick" an acceptance of the cookie policies – but unlike normal cookie policies, this one has buried in the text a notification that the data "may" be used by police. Upon clicking the box, the software installs itself on the suspect's computer.

Maybe surprisingly, the issue of cooperation and consent has not been discussed by either courts or academic literature. It is however not as far fetched, as it may seem. The results of a survey conducted in the context of this thesis within a European Union project[57] indicated that lawyers are willing to reframe many traditionally legal aspects as issues of technology. At the same time, they indicated a strong willingness to use for the reminder analogical reasoning, forcing the new technologies into old conceptual ideas. This notion was particularly strong in civilian jurisdictions - unsurprisingly, as in the ideology of the civil law, the Codes must have an answer, which makes even a far fetched analogy permissible if the alternative is the recognition that the law does not yet answer the question.

---

[56] Buermeyer, note 48.

[57] See for a more detailed account of this chapter 3, p. 77.

If the infiltration is successful, this method offers considerable advantages for the investigating authority in comparison to traditional investigative methods. Because the method is undertaken without the knowledge of the suspect, this person is not alerted to the fact that the police consider him a target, as opposed to a traditional house search. Hence the suspect will not change his behaviour or remove data from his ICT devices.

Furthermore, this measure allows collecting encrypted data in an unencrypted form as the investigating authority can access the data while the user is typing it. Moreover, passwords and further information about the Internet usage pattern of the suspect can be collected. In addition, communication data can be identified, which enables the exposure of the new terrorism structures.[58]

This kind of information would hardly ever be possible to obtain using traditional investigative methods.[59]

2.2 Background and Initial Judgements

As transpired later on, German Federal Secret Services (Bundesamt für Verfassungsschutz) and the Federal Criminal Agency (Bundeskriminalamt - BKA) have deployed the new investigative measure and conducted online searches of computers and other ICT devices of suspects since 2005.[60] These agencies were granted this new investigative power based on an internal regulation by the then Home Secretary Schily.[61] This internal approval approach meant that the introduction of this new investigative measure remained confidential and secret at the time.

The judicial review and public debate was triggered by the application of a state attorney to the BGH to remotely search a suspect's computer in a terrorism investigation on 25 November 2006. [62] The investigating judge declined the application based on the reasoning that such an action would constitute a severe encroachment on

---

[58] See p. 20 above.

[59] BVerfG, NJW 2008, 822 (826).

[60] Tagesschau, "Schily erlaubte Online-Durchsuchungen" (2005), available online at: http://www.tagesschau.de/inland/meldung21410.html.

[61] S Krempl, "Polit-Posse um heimliche Online-Durchsuchungen unter Schily" (2007) *heise*, available online at: http://heise.de/-195563; C Rath, "Die Polizei als Hacker", (2006) *die tageszeitung*, available online at: http://www.taz.de/index.php?id=archivseite&dig=2006/12/11/a0060.

[62] BGH, Beschluss vom 25.11.2006 - Az. 1 BGs 184/2006, http://medien-internet-und-recht.de/volltext.php?mir_dok_id=486.

the basic right to informational self-determination (Article 2.1 in connection with 1.1 of the German constitution – Grundgesetz [GG]) and no legal basis allowing such an encroachment exists under German procedural criminal law. He further found that existing legislation could not be applied analogously because the new investigative measure is fundamentally different from existing investigative measures defined by German criminal law and hence, in common law parlance, ultra vires.[63] Coming to that conclusion he established that a search according to German procedural criminal law is a physical and not an electronic process, and meant to be undertaken openly and with the owner of the premise or thing to be searched present. He therefore reasoned that the analogous application of existing law regulating the search of premises to the clandestine online search of a computer would be comparable to a circumvention of the constitutionally determined reservation of legislative authority.[64]

An appeal of the state attorney to the BGH against this initial ruling created further case law on this topic. The appeal was based on the central argument that a remote search of a suspect's computer could be based on the Articles 102[65], 110[66], and 94[67] of the German Criminal Code (Strafprozessordnung- StPO), assuming a substantial similarity between the physical search of premises, regulated in these articles, and the remote access of a suspect's computer.

The BGH rejected in its judgement the analogy between a traditional search of physical premises and clandestine searches of a computer.[68] The court agreed with the investigating judge that existing legislation regulating the search of premises does not offer a legal basis allowing for such a measure to be undertaken. The court reasoned further that generally, the search and confiscation of computers during investigations is permissible under Article 102 StPO in conjunction with Articles 110 and 94 ff StPO. However, these articles require that a search is undertaken openly, with a police officer and the person affected by the measure present, and the search has to be transparent, hence the reasons for and findings of the search have to be disclosed to the suspect.[69]

---

[63] Ibid. The analogous application of laws in public law is a common procedure. It means that laws can be applied analogously to a situation similar to the one explicitly regulated by the law.
[64] Ibid.
[65] Regulates the search of premises.
[66] Regulates the seizure and search of documents and digital storage devices.
[67] Regulates the securing and seizure of evidence.
[68] BGH, NJW 2007, 930.
[69] Ibid.

An order to undertake a search secretly can therefore not be based on Articles 102 StPO in conjunction with Articles 110 and 94 ff StPO. The court explicitly stated that this is the case for both, the search of a computer with the aim to find data, and the search of a premise to find physical items.[70] The court especially dismissed the argument that a secret search could be considered less incriminating for the person affected, than an openly undertaken search where the place to be searched is entered by police officers.[71] It found that a secret search, as compared to an open search regulated in Articles 102 StPO ff, establishes a sanction due to the high interference intensity of such a measure.[72] During an open search the suspect has the opportunity to influence the length of the measure, or end it through cooperation (e.g. by handing out the items or documents in question), or to start counteractions with the help of a lawyer. This was not envisaged in a secret online search, indeed, it would have defied its very reason to be. Therefore such a measure cannot be regarded as a less incriminating measure, which would have allowed basing it on articles of the StPO.
At this point, it is important to point out that while the specific way the police wanted to use online search tools was clandestine, this is not a necessary feature of the technology. It could as well be imagined a remote online search that informs the suspect of what is going on- the experience would then be very similar to the (eerie) experience when one's computer support person "takes over" a networked computer to remedy an issue. As described above, a pop-up could formally ask for "permission to enter", and it could even be envisaged a situation where the computer negotiates autonomously on the user's behalf access rights with the forensic software. This is less far fetched than it sounds, a very similar process happens constantly on the Internet. Google uses web crawlers, pieces of software that visit autonomously websites, to extract terms for indexing. To be permitted on a site, the software has to "negotiate" permission, and it is easy for the user to include an "agent exclusion clause that prevents such a search taking place, or limits the search to parts of the site.[73] The

---

[70] Ibid.

[71] See e.g. M Hofmann, "Die Online-Durchsuchung – staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?" (2005) 25:3 *Neue Zeitschrift für Strafrecht* 121, 124 supporting this.

[72] BGH, NJW 2007, 930.

[73] For the technical aspects, see e.g. M D Dikaiakos, A Stassopoulou, L Papageorgiou, "An investigation of web crawler behavior: characterization and metrics", (2005) 28:8 *Computer Communications*, 880–897; for the legal issues of this negotiation process, see e.g. M L Boonk, D R A de Groot, F M T Brazier, A Oskamp, "Agent exclusion on websites" (2005) in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005), 13-20. For a different opinion see J Groom, "Are 'Agent' Exclusion

reason to highlight this already here is that it exemplifies one of the perennial problems of legal regulation, especially but not exclusively through courts. Even though, as will be shown below, the German Federal Constitutional Court in particular went out of its way to develop a generic, conceptual answer, it was nonetheless tied to a degree by the very specific features of the case before it. The consequence is that what the courts had to focus on, on procedural grounds alone, was the clandestine nature of the approach, which in this analysis is accidental, not decisive to the issue of software enabled evidence collection. As a consequence, the legal response faces the danger of either being too wide and prohibiting an entire class of technologies simply because its first use before the courts involved a highly problematic usage, or being too narrow and addressing only the issue of clandestine searches while leaving other, equally problematic, issues unaddressed. This in turn could give police and prosecution services an opportunity to avoid the restrictions simply by plugging one hole, while leaving the other issues wide open for abuse.

These initial judgments mainly addressed formal procedural questions, ruling that without explicit legislation, granting such a warrant request would be *ultra vires.* At this stage there were only little technological facts known about the tool and the court undertook no efforts to investigate further technical details and fully understand the concept of this new investigative method. The reasoning of the judiciary was based on a description of what should be achieved by using the tool, but with little attention to the "how". As argued above, this is in the author's opinion underestimating the legal and jurisprudential issues that are raised by the method, rather than the outcome of technology mediated evidence collection.

Nevertheless, two key findings can be extracted from this judgment. Firstly, this new investigative method cannot be subsumed under the existing regulatory framework because it fundamentally differs from traditional investigative methods and from a legal-conceptual point of view cannot be compared to either the traditional search by a human officer or the use of technical equipment facilitating the work of an officer. Secondly, as a result a new legal basis allowing the use of this measure is required. This also means that internal regulations are not sufficient as legal bases for these new investigative measures.

Clauses a Legitimate Application of the EU Database Directive?" (2004) 1:1 *SCRIPTed*, 83-118, available online at http://www.law.ed.ac.uk/ahrc/script-ed/docs/agents.asp.

This is a first indication confirming the research hypothesis of this thesis that the new software-based policing technologies challenge existing legal frameworks that are premised on the parameters of the offline world.

2.3 The German Federal Constitutional Court Judgment

On 27th February 2008, the German Federal Constitutional Court created in a landmark ruling a new constitutional right in confidentiality and integrity of information technology systems and therewith recognised for the first time the constitutional relevance of the virtual living space and data online. [74]

The judgement concerns the *North Rhine-Westphalia Constitution Protection Act* (Verfassungsschutzgesetz)[75] that authorised the Office of the Constitution of the State (nordrhein-westfälischer Verfassungsschutz) to, *inter alia*, secretly access information technology systems through the use of technical means.[76] Thus, the state of North Rhine-Westphalia created a legal basis for the online searching of computers, and in that way fulfilled the central requirement that the BGH had established as a necessary precondition to lawfully undertake online searches of computers using remote forensic software tools.[77]

Article 5.2(11) NRW-CPA was added to empower the constitution protection agency to carry out two types of investigative measures:

- Firstly, secret monitoring and other reconnaissance of the Internet (alternative 1), and
- Secondly, secret access to information technology systems, using technical aids if necessary (alternative 2).[78]

The second alternative, Article 5.2(11) NRW-CPA, establishes the legal basis for an online search of computers and other ICT devices. The *secret access of an information*

---

[74] BVerfG, NJW 2008, 822.
[75] Hereafter "NRW-CPA".
[76] Most policing functions, including some antiterrorism functions, are a devolved matter under the German constitution.
[77] See above 2.2, p. 32.
[78] GVBl. NRW 2006, S.620.

technology system according to Article 5.2(11) NRW-CPA is understood to be its technical infiltration by a piece of specifically designed software.[79]

Article 5.2 (11) NRW-CPA empowers the constitution protection authority to undertake these measures under the general preconditions for data collection of intelligence services arising from Article 5.2 in conjunction with Article 7.1 and Article 3.1 NRW-CPA. According to these provisions, the use of such investigative measures is only permissible if information on efforts or activities that are relevant to the protection of the constitution can be obtained, or the sources of such information (i.e. key figures in a terrorism network) are detected.

This law was heavily criticized and it was widely suggested that it was in violation of the constitution.[80]

In every investigation exists a conflict between the need to gain information and data about a suspect on the one hand, and the protection of privacy rights of this person on the other.[81] Law enforcement agencies need to infringe citizens' privacy rights in order to investigate crimes.[82] However, a balance has to be retained and infringements have to be necessary and proportionate. It was argued by several academics that in this particular case, this balance was not retained and Article 5.2 (11) NRW-CPA is an unconstitutional infringement of the privacy rights of affected persons.[83]

The main problem that has been identified by these authors is the relatively task-oriented and simple nature of the technology. German law distinguishes different types of data, some of it so important for privacy that no access is ever permitted; other data is of a much less important nature. While a Trojan could be programmed to copy only image files (in a child pornography case) or only text files with the word "bomb", the legal classification of data types is too subtle and requires too much world knowledge about the way we think about privacy to allow for a simple solution that ensures that the Trojan only copies permissible data.

---

[79] Landtagsdrucksache – LTDrucks 14/2211, p. 17.

[80] See e.g. Hornung, note 48, at 577; Fox, note 48, at 840; C Wegener, "Hintergründe zum Vorhaben 'Online-Durchsuchung'" 15. Workshop "Sicherheit in vernetzten Systemen", 3 available online at: http://www.wecon.net/files/14/DFN2008-HzVOD-ARTIKEL.pdf.

[81] See the privacy and data protection regulations (e.g. Articles 2.1 in connection with 1.1; 5; 8; 10 GG) of the German Constitution that establish the boundaries for investigative actions. See also the *Fourth Amendment* to the United States Constitution protecting privacy and data protection rights of suspects during investigative measures of police and secret services. See also the *UK Regulation of Investigatory Powers Act 2000*, regulating the powers of public bodies to carry out surveillance and investigation.

[82] B J Koops, A Vedder, "Criminal Investigation and Privacy: Opinions of Citizens" (2002) 18:5 *Computer Law & Security Report* 322-326 (322).

[83] See e.g. Hornung, note 48, at 577; Fox, note 48, at 840.

The BVerfG in its judgement agreed with this view and ruled that Article 5.2 (11) NRW-CPA was not in compliance with the constitution and therefore null and void. While the result itself was no surprise because of the lack of substantial and procedural privacy safeguards,[84] the expectation had been that the court would only need to apply the explicitly enumerated basic rights and existing constitutional principles to reach this conclusion. The court however found that for several reasons the existing rights canon was not sufficient to protect the constitutional rights of citizens from the potential loss of liberty that the remote searching of computers with remote forensic software tools could cause, and thus created – or maybe inferred from first principles – a new basic right in the confidentiality and integrity of information technology systems.[85]
This surprise move was partly due to the welcome fact that the court engaged in considerable depth with the specific technological issues that the legislation raised. Three of the countries leading academics in the field, Prof Felix Freiling, Prof. Dr. Andreas Pfitzmann,[86] and Prof. Dr. Dr. hc Ulrich Sieber were appointed by the court as technical experts. Maybe more unusual was the background of a fourth expert advising the court. Andreas Bogk is a freelance Hacker at Clozure Inc and CEO at Chaos Computer Club Events, one of the biggest and most influential hacker organisations. Thus, compared to the BGH judgment and the decision by the BGH investigation judge the reasoning of the BVerfG was unusually well informed about the technological aspects. This is important to note as often, shortcomings in the regulation of technology are blamed on ignorance by lawyers, something that could in principle be easily remedied. The author of this thesis for instance was involved, as part of the research, in developing a certificate in forensic computing for lawyers that is accredited by the EU,

---

[84] See e.g. G Hornung, " Ein neues Grundrecht. Der verfassungsrechtliche Schutz der "Vertraulichkeit und Integrität informationstechnischer Systeme"", (2008) 5 *Computer und Recht*, 299.

[85] Strictly speaking this new basic right is not a new constitutional right, but a new sub-group of the general personality right (W Hoffmann-Riem, "Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme" (2008) *Juristenzeitung* 1009-1022, 1018 f.). Arguably, the creation of a new right by the court would have given rise to issues of the separation of powers. In practice however, the future approach of the court may outweigh the difference between a specific right and a sub-group of the general personality right. As apparent from the development and impact of the right to informational self-determination (another sub-group of the general personality right), the German Federal Constitutional Court does not hesitate to use a non-written fundamental right to severely restrict surveillance activities by state agencies (G Hornung, R Bendrath, A Pfitzman, "Surveillance in Germany: Strategies and Counterstrategies" in S Gutwirth et al (eds.) Data Protection in a Profiled World (Berlin Heidelberg: Springer, 2010) 139-156, 142).

[86] Prof Pfitzmann died on 23 September 2010.

and has by now taught more than 400 judges and prosecutors.[87] For any problems identified with the decision of the BVerfG though, this simple explanation can be ruled out, and more intractable structural issues of the legal regulation of technology need to be looked at.

The court placed much emphasis on the importance and influence of ICTs for people's lives and their societies. The user experience and the user understanding of ICTs is critically assessed and conceptualised. The court acknowledged that the use of ICTs and the Internet is no longer a trivial activity rooted in the physical world, but has created its own, digital world that needs to be taken serious.[88] Our "home" is partly online and therefore rules protecting our physical homes should also apply to our digital habitats. As a result of this reasoning, the court found that the existing German fundamental rights canon is insufficient to guarantee the protection of this digital habitat and consequently, developed a new basic right.

2.4 The Right in Confidentiality and Integrity of Information Technology Systems

ICTs depend heavily on the processing of (private) data. In an important sense, everything that happens online is ultimately about information exchange, even though we may experience this in a different way, e.g. as "moving a player in an online game". Therefore, one could say with only a small degree of hyperbole that ultimately all Internet law is data protection law. This recognition led the court to recognise the fundamental importance of solidifying constitutional guaranties in online settings.

In this case, the court decided that a new basic right was required to ensure that citizens are sufficiently protected from violations of their rights.

Although it does not happen very often in Germany that a new basic right is established through judicial activism, the right of the court to creatively fill identified gaps in the constitution's civil rights framework is widely recognised and, unlike in the US, originalism has never been a prominent position in post-war Germany.[89]

---

[87] For more information on this see chapter 3, p.77.

[88] BVerfG, NJW 2008, 822, 841.

[89] R Alexy, R Dreier, "Statutory Interpretation in the Federal Republic of Germany", in N MacCormick and R Summers (eds) *Interpreting Statutes: A Comparative Study* (Darthmouth: Aldershot, 1991) 72-121.

Like the right to information self-determination, this new fundamental right is based on Article 2.1 German basic law (Grundgesetz – GG) in conjunction with Article 1.1 GG, and is derived from a general personality right. Article 1 GG, which states that "human dignity is inviolable, and all organs of the state have the ultimate aim to protect it" establishes a general overriding principle in the German legal system, and is designed explicitly as a stop-gap solution if legislative solutions fall behind social change. The new constitutional IT right protects, so the court, the personal and private life of rights holders from state accesses of ICTs, and in particular against state access of the information technology system as a whole, and not only of individual communication events or stored data.[90]

2.4.1 What is protected?

The court applies the guarantees of this right to information technology systems, but interestingly does not deliver a definition of such a system. Instead, it lists systems that are not protected by this right, and provides a description of minimum abilities information technology systems must possess to fall into the protection scope of this fundamental right. By doing so, it keeps the protective scope of this basic right very broad and at least regarding this aspect "future-proof" and technology neutral.[91]

Protected are information technology systems which alone, or in their technical interconnectedness, can contain personal data of the person concerned to such a degree and in such a diversity that access to the system facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of their personality.[92] Such systems are for example personal computers and laptops (used for both, private and business purposes), and mobile phones and electronic calendars, which have a large number of functions and can collect and store many kinds of personal data.

Significantly, the court decided that the mere *ability* of the system to store personal data is sufficient. Whether this capacity was actually utilised by the user in question need not be determined in the individual case.

---

[90] BVerfG, NJW 2008, 822 (846).

[91] See for a discussion on technology neutrality for example, C Reed, "Taking Sides on Technology Neutrality" (2007) 4:3 *SCRIPTed* 263-284.

[92] BVerfG, NJW 2008, 822 (846).

Furthermore, it acknowledges that systems that are part of a network (such as the Internet) do not always contain personal data themselves, but data about the person concerned can be stored on another system within the network, which however can be accessible if the system is infiltrated. The new IT basic right thus also protects data that is outsourced, for example using cloud computing technology.[93]

The new IT basic law identifies two properties worthy of constitutional protection: the confidentiality and the integrity of the system.
Confidentiality refers to the interest of a user of an information technology system in ensuring that the data created, processed and stored by the system remains confidential.[94] Thus this aspect is largely congruent with the right to informational self-determination. Integrity refers to the protection against the unauthorised access of the system to use its performance, functions and storage contents. As the experience with the British Computer Misuse Act 1990 and its very similar provision (though targeted at criminals) shows, it is virtually impossible to spy on a computer system without making some unauthorised changes to it[95] - an issue that will be of concern for this thesis later when the evidential value of evidence thus obtained is discussed.[96] It can therefore be assumed that all present, and probably most future, systems that allow information gathering without explicit consent will fall foul of this provision.

Additionally, systems are only protected if the person concerned considers the system his own, and thus may presume that he alone or others authorised by him, such as close family members, use it in a self-determined manner.[97] It could be added that increasingly, we grant access to our computer automatically, e.g. to update agents that install automatically the latest version of a program. Trusted Computing will make it a matter of course to grant access to certain software providers who will be charged with maintaining the systems safety. Even though in this case, a wide range of people not known to the owner will be given routine access, this should not be constructed as a "waiver" of protected rights –even though his consent to these measures will in reality

[93] For a discussion of Cloud Computing see: M Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law", 6:1 *SCRIPTed* 132-146.
[94] BVerfG, NJW 2008, 822 (847).
[95] See O Kerr, "Cybercrime's Scope: Interpreting Access and Authorization in Computer Misuse Statutes" (2003) 78:5 *New York University Law Review* 1596-1668.
[96] See chapter 7.
[97] BVerfGE, NJW 2008, 822 (849).

be very superficial and formal, hidden in the terms and conditions when buying a new computer.[98]

However, the use of one's own system via the use of information technology systems that are at the disposal of others is covered. This could, for example, be the remote access of one's system or external storage device via a computer in a cyber café.

2.4.2 Restrictions

As determined above (2.1), citizens' privacy rights necessarily need to be infringed by law enforcement agencies to investigate crimes. Hence, the right in confidentiality and integrity of information technology systems is not absolute. It can be restricted for both preventive purposes and to prosecute crimes. Yet, as explained above, any measure that restricts this fundamental right has to be proportionate to the violation, especially if the measure is carried out without the knowledge of the suspect.

Thus, the court has found that a measure restricting this right is only proportionate where sufficient evidence exists, that significant higher-ranking fundamental values need to be protected.[99]

The court considers higher-ranking fundamental values to be the life and integrity of other citizens, the foundations of the state, and essential values of humanity.[100]

However, the court then softens this requirement, ruling that a high level of probability that the danger will materialise in the near future is not required.[101]

Furthermore, any such measure has to be scrutinised and confirmed by a judge on a case-by-case basis to guarantee an objective and independent control prior to the execution, and it has to be based on a constitutional legal basis.[102]

A further requirement is that any measure restricting the IT basic right does not violate the core area of the private conduct of life, which includes among other things communication and information about inner feelings or deeply personal relationships. The private conduct of life is an absolute fundamental right, which cannot be restricted (Article 1.1 GG – right to human dignity). Since it will often be very difficult to differentiate between core area and non-core area data during the investigation process, the court determines that adequate procedures have to be in place for the

---

[98] B Schafer, Y Danidou, "Trusted computing and the digital crime scene" (2011) 8 *Digital Evidence and Electronic Signature Law Review* 111-123.

[99] BVerfG, NJW 2008, 822 (849).

[100] BVerfG, NJW 2008, 822 (849).

[101] BVerfG, NJW 2008, 822 (853).

[102] BVerfG, NJW 2008, 822 (854).

examination stage of the data. In particular, if core area data is detected, this data has to be deleted immediately and the use of this data by the state is prohibited.[103] However, this raises the dilemma that the requirement to delete the collected core area data cannot undo the violation of the absolute right to human dignity. Furthermore, as Kutscha points out, although the measure itself has to be permitted by a judge, the court did not establish a requirement for a judge to control the analysis process.[104] At this point, one might discuss if by ignoring the specific abilities of investigative software, an opportunity was missed here. However, as long as only the software makes a copy, and deletes irrelevant data before the police as "owner" accesses it, any infringement of privacy would be minimal or nonexistent.

2.5 Reasoning

Coming to the conclusion that a new basic right is necessary to guarantee the safeguarding of data protection and privacy rights, the court had considered and rejected the possibility that the existing basic rights canon is sufficient to ensure this. This reasoning has been discussed controversially, with some authors arguing that existing basic rights are sufficient to protect citizens from such investigative activities by state agencies.[105] The arguments of the court against the applicability of existing basic rights, and the criticism thereof, are thus important to assess the relevance of the new IT basic right.[106]

The court considered and rejected the right to secrecy of telecommunications (Article 10.1 GG), the right to inviolability of the home (Article 13.1 GG), and the right to informational self-determination (Article 2.1 in conjunction with Article 1.1 GG) as possibilities.

---

[103] Ibid.

[104] M Kutscha, "Mehr Schutz von Computerdaten durch ein neues Grundrecht?", (2008) 15 *Neue Juristische Wochenschrift*, 1042, 1043.

[105] See e.g. Hornung/Bendrath/Pfitzman, note 85, at 142.

[106] For the purpose of this thesis only the central arguments are depicted here. For a discussion of the full reasoning see W Abel, B Schafer, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822", (2009) 6:1 *SCRIPTed* 106 – 123.

2.5.1 The Secrecy of Telecommunications

Secrecy of telecommunications according to Article 10.1 GG protects the non-physical transmission of information to individual recipients with the aid of telecommunications devices.[107] Protected by this basic right is any type of telecommunication regardless of the transmission type used (cable or broadcast, analogue or digital transmission), and the data transmitted (speech, picture, sound, or other data), thus also any communication via the Internet.[108] Moreover, protected by this right are not only the contents of the communication, but also details about their general circumstances, such as details about the communication partners, and the transmission type (by email, chat, VoIP).[109]

Thus any ongoing communication via the Internet, and the data generated by such communication falls within the scope of the protection of Article 10.1 GG, regardless of whether the measure targets the transmission channel or the terminal used for telecommunication.[110]

The court however found that Article 10.1 GG does not cover an online search of data stored on the storage media of an ICT device, especially if the data is not in the public domain and the affected person has undertaken steps to protect the data from unauthorised access.[111]

Hence, the court considered that the right to secrecy of telecommunications is only applicable if the surveillance is technically restricted exclusively to data emanating from an ongoing telecommunication process, i.e. searching of the system is impossible.[112]

This reasoning of the court is conclusive. The fact that the software tool requires the suspect to be online at some point and engaged in communication does not make the search a wiretapping operation any more than a police officer who seizes a suspects

---

[107] See e.g. BVerfGE NJW 1985, 121 (136); NJW 2002, 3619 (3626).
[108] See BVerfGE, NJW 2005, 2603 (2638) for emails.
[109] See e.g. BVerfGE, NJW 1985, 121 (136); NJW, 1992, 1875 (1885).
[110] BVerfGE, NJW 2002, 3619 (3628-3629); NJW 2003, 1787 (1800-1801).
[111] BVerfG, NJW 2008, 822 (842).
[112] However, this is technically currently still impossible to ensure (See Hornung, note 84, at 299 for more details).

phone during a physical search of his premises changes the nature of the operation from a search into an interception of telecommunication.

The secret infiltration of a complex ICT system offers the opportunity to spy on the system as a whole, and is not just an intercept of an isolated exchange of communication as in a traditional wiretapping operation.[113] In particular, there is a chance that personal data stored on the computer, which is unrelated to and goes over and above the contents and circumstances of the ongoing telecommunication, is collected (even if this is unintended). Thus, the potential threat to civil liberties goes far beyond the mere surveillance of telecommunication, and also beyond the protective scope of Article 10.1 GG.

In practice, this means that hardly any search will be a "pure" communications intercept. The main aim of the software tool as discussed above is to collect data stored on a computer, and the conceptual gap to communication interception is too wide to be bridged by analogous interpretation of Article 10.1 GG. This also means that several aspects of the remote searching of computers are not covered by the guarantee of secrecy in telecommunications as provided by Article 10.1 GG.

2.5.2 The Inviolability of the Home

The guarantee of the inviolability of the home granted by Article 13.1 GG protects the private living space from intrusion by the state.

The spatial sphere in which private life takes place constitutes the interests protected by this basic right.[114] The private living space is, however, not limited to the private flat or house of the rights holder, but also includes business and office space.[115] It protects this space from physical intrusion, as well as from the use of technical measures that provide an insight into the otherwise protected happenings within the private living space. This is, for example, the acoustic and optical surveillance of a living space,[116] but also the measurement of electromagnetic radiation to monitor the use of information technology systems inside the dwelling.

The court found that Article 13.1 GG only provides protection of the private living space against the secret intrusion by police or secret service to physically manipulate

[113] BVerG, NJW 2008, 822 (842).
[114] See BVerfGE, NJW 1993, 2035 (2047); NJW 2001, 1121 (1129-1130).
[115] BVerfGE, NJW 1971, 2299 (2314).
[116] BVerfGE, NJW 2004, 999 (1029, 1047).

information technology systems, and against the infiltration of such systems to monitor the events in a flat using peripherals connected to the system (such as the use of inbuilt microphones for eavesdropping).[117]
It stated that such actions would be comparable in its nature to the traditional search of a house and would therefore be covered by Article 13 GG. However, even this protection did not go far enough, and it underestimates the importance of the digital world for today's citizens. The court argued that Article 13 GG is insufficient to protect rights holders against the general infiltration of ICT systems using a software tool to access the stored data and monitor the communication, even if the system is located in a dwelling.[118]

Hornung disagrees with this reasoning.[119] He argues that Article 13 GG is not merely aimed at protecting the physical space as such, but rather at protecting the privacy of the rights owner within this physical space and his freedom to behave as he wishes.[120] Accordingly, he comes to the conclusion that Article 13 GG covers all online activities undertaken from the private living space.

However, one specific problem created by remote online searches is that infiltration and monitoring can be performed regardless of the location of the information technology system. The introduction introduced the notion of porous borders of the Internet world, and here this problem can be observed.
A location-dependent protection is of no use if the system is located outside the private space, or on the move between "protected" areas. Especially small ICTs such as laptops, PDAs and mobile phones are designed to be carried around. The precise location of the system will often be unknown, and is also irrelevant for investigators when infiltrating the device to access stored data. This would have had the counterintuitive consequence that a citizen who starts writing an email on his laptop at home, reviews it on a park bench and completes and sends it back at home moves between protected and unprotected environments, loosing and gaining apparently arbitrarily constitutional protection and thus creating artificial distinctions in an activity that is experienced as

[117] BVerfG, NJW 2008, 822 (843).
[118] Gercke, note 48, at 250.
[119] Hornung, note 48.
[120] Ibid, at 577.

uniform by the citizen. Hornung acknowledges this problem, stating that Article 13 GG could be applied analogously to these cases.[121]

However, while it is acknowledged that this is a *possible* outcome, there is nothing that would *force* the courts to take this route. Therefore, this approach does not sufficiently recognise the importance of ICT devices and the significance the online space has gained for citizens. The concept of cloud computing[122] already challenges this approach since the data is no longer stored on a device controlled by the owner of the data at all, but a third party. Thus the concept of a "quasi-living space" applicable to mobile devices fails here. Analogies are always difficult as long-term solutions when applied to fast-developing technologies such as ICTs.

2.5.3 The Right to Informational Self-determination

The right to informational self-determination, which is not explicitly mentioned in the constitution, was derived from Article 2.1 in conjunction with Article 1.1 GG, which guarantee the right to free development of one's personality and a general "right to dignity", respectively.

This right constitutes the core of Germany's data protection law and was created by the BVerfG in a landmark ruling unrelated to ICTs.[123]

Ruling on the constitutionality of the national census, the court established a legal entitlement to the capacity of the individual to determine in principle the disclosure and use of one's personal data.[124] This right resulted from the court's recognition that the state had multiple possibilities to collect, process, and use private data, and that the evolution of electronic data processing techniques had simplified these to such an extent that a detailed image of the personality of the individual becomes feasible. This had the potential to impair confidentiality interests of the affected person, which are protected by fundamental rights. Moreover, the mere anticipation that one's data could be collected entailed an unacceptable encroachment on one's freedom of conduct,

---

[121] Ibid, at 578.

[122] See e.g. for a definition of cloud computing P Mell, T Grance, "The NIST Definition of Cloud Computing" (2011) *Computer Security*, available online at http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf.

[123] BVerfG, NJW, 1984, 419.

[124] BVerfGE, NJW, 1984, 419 (462); NJW, 1991, 2411 (2413).

encouraging people to forgo valid, and perfectly legal, lifestyle choices in the mere anticipation that information about them could be collected and leaked to third parties. This means in particular that no concrete threat has to be evident. The court stated that this is in particular the case if personal data can be used and linked in a manner, which the person concerned can neither detect nor prevent.[125] Fear of surveillance is just as limiting to the free development of a social personality as the surveillance itself.

Given the historical and teleological background of this basic right, the assumption of many scholars was that the right to informational self-determination could be applied to the data processing online and would be sufficient to regulate the online searching of ICTs.[126]

However, the court found that the right to informational self-determination does not sufficiently appreciate the fact that individuals rely on information technology systems to develop their personality and hence entrust the system with sensitive data, or inevitably provide such data by merely using the system.[127] A third party accessing such a system can obtain potentially large amounts of sensible information about an individual, without having to rely on further data collection and processing measures.

As with Article 13 GG, arguing that the right to informational self-determination would be sufficient is short sighted. Extending the protection scope of the right to ICTs and their use might be feasible at the current stage; however, the fast development of ICTs and their integration into people's life means that an ever-increasing amount of private data is stored online and ICTs become ever more important for the private and business life of people. In a way, one could say that the Internet and ICTs cut out the "man in the middle". The data comes already pre-processed and arranged by the data subject's computer.
Since the older data protection decision focused on the process of data handling and organisation, there is the danger that the new surveillance technologies circumvent this right. The active, if unwitting, participation of the suspect that is crucial for the functioning of the software tool has therefore also the potential to deprive the suspect of protection otherwise taken for granted.

---

[125] BVerfG, NJW 2008, 822 (844).
[126] See e.g. Hornung/Bendrath/Pfitzman, note 85, at 142.
[127] Ibid.

Another crucial aspect that is overlooked by scholars arguing in favour of the applicability of the right to informational self-determination is the automation of the policing activities and the resulting modification of the existing policing system, which is traditionally rooted in the reasonable exercise of human judgment. We expect for instance from prosecution agencies to issue warrants only if there is a *reasonable* suspicion against a suspect, the search must have a (subjective) *likelihood* to produce relevant evidence (that is, is a goal directed, intentional process) and the gains must on balance justify the infringement of certain rights and liberties. Law enforcement is therefore always also an exercise in practical reason and practical reasonableness. We control the exercise of this discretionary reasoning through various means, some of them procedural, others more substantive. Procedurally, we often link the right to make such a decision to a certain degree of proven experience, expressed in hierarchical organisations such as the police typically through a rank. Only officers of a certain rank, and with that, a certain degree of track record of getting it right and the relevant life experience that this carries will be permitted to make certain decisions. Laws on police procedure will typically prescribe and in varying degrees regiment the exercise of this discretionary reasoning, by linking legal consequences directly to the internal mental state of police officers, "reasonable suspicion" as a trigger condition for search rights again being the paradigmatic example. Finally, courts will be able to scrutinise if this discretion was wielded appropriately, engaging in their own practical reasoning in the process. All this is necessary for the rule of law – police officers exercise their power with their subjective knowledge and understanding of the laws that confer them to them, and the courts can if required validate or invalidate post factum this reasoning process. By replacing officers through an automated process, or even by shifting the emphasis away from the human controller of the software (if there is still such a person) to the program carries with it the potential to shortcut these safeguards, transforming what ought to be a normative-evaluative process of practical reasoning into a purely factual question of technology performing according to its design parameters. Empirical research that the author carried out in the context of this thesis within the European project mentioned above on Admissibility of Electronic Evidence in court bears out this concern.[128] A substantial number of the respondents to the questionnaire acknowledged that they had little or no understanding of computer

[128] A more detailed account of this research will be given in chapter 3.

technology, and were therefore happy to "black box" large parts of the investigative process, putting their trust in computer forensics experts who could testify to the correct functioning of their diagnostic tools. But by changing the conceptual framing of the question from one of practical reasonableness and law conformant exercise of power by a human being to one of software technology, many of the probing questions a judge or defence solicitor may have asked of a police officer ("did you *really* hear a scream before you entered the flat?") fell by the wayside, and computer experts who were perceived as neutral and objective scientists were given a much less rigorous level of scrutiny.

Online searching of a computer is of a severity for the personality of the affected person that goes beyond mere individual data collection, against which the right to information self-determination provides protection, and it is therefore correct to reason that it is not covered by the fundamental right to informational self-determination.

2.6 Evaluation

The academic discussion of the judgment has mainly focused on the new basic right and the court's dismissal of the applicability of the existing rights canon.
The court, however, delivered a forward-looking piece of regulation that is more complex than it appears at first glance. Hidden in the court's reasoning on the applicability of the existing rights canon to novel software-based investigative measures are important new approaches to the future policing of the Internet and data online.
What has slipped the attention of most scholars is the court's recognition of the existence of a virtual living space and the acknowledgment of its constitutional relevance.[129]

2.6.1 Virtual Living Space

Little attention has so far been paid in the legal discussion of this judgment to the court's recognition of a virtual living space as a concept of constitutional relevance. The reason for this could be that the court fails to explicitly refer to this new concept in the

[129] BVerfG, NJW 2008, 822 (835ff).

judgment. The court's recognition of this concept can however be derived from the court's reasoning on the use of ICTs and the Internet.

The court establishes in its judgment that the use of ICTs has gained an importance and significance for the personality and the development of individuals that could not have been foreseen.[130] It states that modern ICTs provide the individual with new possibilities and are now omnipresent and that their use is central to the lives of many citizens. It goes on to find that the performance of ICT systems and their significance for the development of the personality increase further if such systems are networked with one another, which is more and more becoming the norm, in particular because of the increased use of the Internet by large groups of the population.[131]
Hence, the court acknowledges that ICT systems are an integral part of citizens' lives and are shaping the way people live and work, and societies function. It furthermore recognises that citizens are entrusting ICT systems with increasingly more sensible information, which leads to new types of endangerment for the personality of citizens.

These endangerments can in particular materialise if LEAs monitor the usage of ICT devices and their applications, and collect data stored on those devices and generated during communications. This data can be of sensitive nature and provide LEAs with a detailed image of the personality of the suspect, as well as details about his habits and activities in the virtual living space. Accessing this data can therefore lead to violations of privacy and data protection rights. With the establishment of the new IT basic right the court acknowledges the constitutional relevance of the virtual living space, and the need to protect citizens from violations thereof.

The acknowledgment of the virtual living space as a legal concept of constitutional relevance and the establishment of the new IT basic right is a logical consequence of the analysis of the state-of-the-art of ICTs and their likely future development.

The growing significance of the virtual living space means that the borders between the digital and analogue realm are increasingly blurred. The importance of the virtual living space has its roots in the development and advancement of ICTs. We no longer

[130] BVerfG, NJW 2008, 822 (827).
[131] BVerfG, NJW 2008, 822 (827).

provide machines with commands; we enter into dialogues, navigate simulated worlds, and create virtual realities. Further, these dialogues are no longer limited to one-on-one person/machine interactions. Millions of people now interact with one another via computers on networks, where they have the opportunity to talk, to exchange ideas and feelings, and to assume personae of their own creation.[132] This leads to the development of a "second self" or "digital identity" in the virtual living space, and these two identities – the virtual and the analogue – increasingly fuse. Actions in the virtual living space have consequences upon the analogue self and vice versa.

As this case study shows, this leads to questions regarding the policing of this virtual living space. The more people entrust the virtual living space with information and live online, the greater is the interest of LEAs to monitor and police this space. The significance of the development of the new IT basic law and the acknowledgment of the virtual living space as a concept of fundamental value becomes evident here. The growing importance of the virtual living space triggers the introduction of novel, software-based investigative tools. As shown, their unique abilities, however, threaten fundamental values and rights. With its judgment, the court has established that the policing of the virtual living space can only occur within the parameters of the constitution. It recognises however also the essential difference between virtual and offline lifes, a difference prominent enough to force the court to develop a new constitutional right.

2.6.2 The New Investigative Tools

The judgment of the German Federal Constitutional Court (necessarily) has its shortcomings. In particular, it lacks a deeper technical analysis of the proposed software tool envisaged to deploy during online searches. The focus of the court was on the *target* of an invasive investigative act, and the *rights* violated in the process. This is of course typical for court based reasoning, which occurs only after a right was potentially violated. Precluded, partly for procedural reasons, was therefore an analysis of the details of the *process*, and how in the future law compliant software-based investigative tools should be structured. Or with other words, while the court discussed the virtual living space as a sui generis regulatory space, it did not yet discuss the virtual police officer.

---

[132] Turkle (2005), note 6.

2.7 Relevance

Despite the national (German) focus of this case study, the online searching of computers is an international phenomenon. The reason for focusing on the German case instead of choosing a more general European approach is the important and detailed case law generated by the BVerfG. While this judgment only has a direct legal impact in Germany, the findings are of great significance for other countries given the transnational nature of the Internet and the data stored online.

This is particularly relevant, since the Council of the European Union (EU) recommended in 2008 that member states should undertake clandestine remote searches of computers of suspects, if provided for under national law, and thus encouraged the EU members to introduce this new investigative method.[133] This recommendation is part of a framework strategy developed to more effectively combat cybercrime and the increase in crimes committed using computer technology. Following this recommendation, several member states discussed the general legality of this measure, and the need to implement legislation allowing for the online searching of computers. In addition, the German government initiated the foundation of a working group – the so-called *Remote Forensic Software User Group* – to exchange information about the technical details of the online searching of computers.[134] The core participants of this group are Germany, the Netherlands, Belgium and Switzerland.

In the UK, according to the Association of Chief Police Officers (Acpo), 194 clandestine searches had been undertaken within one year of people's homes, offices and hotel rooms.[135]
Here, the remote searching of computers is currently based on existing legislation. Since 1994, an amendment to the *Computer Misuse Act 1990* made state hacking possible. Section 162 of the *Criminal Justice and Public Order Act 1994* amended section

[133] Council of the European Union, 'Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime', 2987th Justice and Home Affairs Council meeting, 27 – 28 November 2008, available at http://www.ue2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf
[134] A Wilkens, "BKA initiierte internationale Staatstrojaner-Arbeitsgruppe" (2011) *heise*, available online at http://heise.de/-1378367
[135] D Leppard, "Police set to step up hacking of home PCs" (2009) *The Sunday Times*, available online at http://www.timesonline.co.uk/tol/news/politics/article5439604.ece.

10 of the *Computer Misuse Act 1990* (saving for certain law enforcement powers) to allow access to computer material by constables and other enforcement officers. However, such intrusive surveillance is closely regulated under the *Regulation of Investigatory Powers Act 2000* (RIPA).

RIPA allows in Section II for covert directed surveillance of persons. Directed surveillance is defined as covert surveillance, which is undertaken for a specific investigation or operation that is likely to obtain private information about a person, and for the purpose of preventing or detecting a serious crime. Furthermore, the action needs to be authorised. This is the case, if the officer undertaking the measure believes, at the time of executing it, that the action is necessary to prevent or detect serious crime, and is proportionate to what it seeks to achieve.

The author notes that the wording of RIPA refers directly to the beliefs of relevant officers of the right rank, opening up the possibility to either circumvent RIPA through autonomous tools, or to prohibit them altogether because of the absence of such mental states. This thesis will argue that a better solution is to be open about both the dangers and possibilities of remote forensic software tools, which however need to be able to perfom the functional equivalents of the deliberative steps ("necessary to detect") and to recognise this ability, not by ascribing to them legal personality, but the equivalent of a "police rank", a solution which this thesis argues is less philosophically loaded as speculation about "robot consciousness" inevitably are.

Other European countries have also discussed the introduction of the online searching of ICTs as an investigative measure.[136] Most recently, Finland has published in February 2011 a draft amendment of the Coercive Measures Act, which would grant police the power to undertake online searches of computers.[137]

---

[136] Both Switzerland and Austria had public discussions about the introduction of this measure. Similarly to the UK, Switzerland does not have a specific legal basis allowing this investigative measure. However, a law regulating the surveillance of the post- and telecommunications traffic enables police to undertake this measure (see e.g. E Platz, "Rechtliche Zulässigkeit von Remote Forensic Software in der Schweiz" (2008) *sic-online*, available online at http://www.sic-online.ch/2008/documents/838.pdf). In Austria, the introduction of a legal basis allowing the online searching of computers is still being debated (see e.g. D AJ Sokolov, "Österreich: Arbeitsgruppe Online-Durchsuchung legt Bericht vor, (2008) *heise*, available online at: http://heise.de/-198121).

[137] Helsinki Times, "Finnish government wants police to have spyware powers" (2011) *Helsinki Times*, available online at: http://www.helsinkitimes.fi/htimes/domestic-news/politics/14409-finnish-government-wants-police-to-have-spyware-powers.html.

In Germany, following the BVerfG judgment and the conditions set out therein, several legal bases for the online searching of computers have been introduced.

On federal level, the law defining the powers of the Federal Criminal Agency (*Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten* – BKA Gesetz) has been amended to include the power to undertake an online search of computers.[138] Article 20k was added to the list of powers to allow the German Federal Criminal Agency (Bundeskriminalamt -BKA) to secretly access, without the knowledge of the affected person, information technology systems under certain conditions.[139]

On federal state level, two federal states, Bavaria and Rhineland-Palatinate, have introduced legislation allowing the online searching of ICT devices.
Bavaria amended its *Police Power Code* (*Polizeiaufgabengesetz* - PAG) on 3rd July 2008 to include the power to search computers remotely.[140]
However, this amendment was altered to ensure its constitutionality after the opposition party filed a constitutional complaint against the regulation.[141] The currently valid version came into effect on 14th July 2009.[142]
Rhineland-Palatinate amended its *Police Code* (*Polizei- und Ordnungsbehördengesetz* - POG) to include the power to remotely and clandestinely search the computer of suspects on 27th January 2011.[143]
Article 31c (1) POG grants police the power to access information technology systems to prevent a danger for the life and integrity of another person, the foundations of the state, and essential values of humanity.[144]

---

[138] BKAGes. i. d. F. v. 25. 12. 2008, BGBl. I 3083 ff; S Krempl, "Bundestag verabschiedet BKA-Gesetz mit heimlichen Online-Durchsuchungen" (2008) *heise*, available online at http://heise.de/-216645.
[139] Article 20k Bundeskriminalamt Gesetz, available at http://www.gesetze-im-internet.de/bkag_1997/__20k.html.
[140] S Krempl, "Bayrischer Landtag setzt den 'Bayerntrojaner' frei" (2008) *heise*, available online at http://heise.de/-183633.
[141] S Krempl, "SPD legt Verfassungsbeschwerde gegen den 'Bayerntrojaner' ein" (2008) *heise*, available online at http://heise.de/-207807.
[142] http://by.juris.de/by/PolAufgG_BY_1990_Art34d.htm; M Emert, "Münchener Koalition beschließt Änderungen beim 'Bayerntrojaner'" (2009) *heise*, available online at http://heise.de/-5939.
[143] S Krempl, "Rheinland-Pfalz lässt den Landestrojaner von der Leine" (2011) *heise*, available online at http://heise.de/-1178650.
[144] http://rlp.juris.de/rlp/PolG_RP_P31c.htm .

All new legal bases have been drafted to adhere to the requirements developed by the BVerfG in its judgment. Thus all require that a danger for the foundations of the state or a federal state, essential values of humanity, or the life and integrity of another person exists for the measure to be permissible.

However, the new BKA law has already been challenged before the BVerfG.[145] The complaint is still pending but it remains to be seen whether the court will find this law constitutional, and provide further general guidance on the topic, and interpretation of the IT basic right in its judgment.

2.8 Conclusion

The growing significance of ICTs and the Internet for people's lives leads to a fusion of the online and offline world. More and more, people develop a life online and entrust ICTs with core private data.

As a result, LEAs are increasingly interested in monitoring online activities and accessing the data stored there. The policing of the online living space, however, requires novel, software-based investigative methods. These novel methods, like the online searching of computers, rely on technologies that gradually replace human officers for core policing tasks. They can be regarded as cyber-cops, operating autonomously, without the direct intervention of human operators.

These tools are executing potentially infringing tasks, like the search of private data and monitoring of conversations. The BVerfG therefore established in its judgment that the online living sphere is of constitutional value and any executive acts potentially infringing this need to be in accordance with the constitutional right to confidentiality and integrity of information technology systems.

This means that the new investigative technologies need to operate in compliance with existing legislation regulating police investigations. This, however, poses the problem of adjusting the legal framework that relies so prominently on human agency and intent, like suspicion, to autonomous software tools.

---

[145] S Lüders, "Verfassungsbeschwerde gegen BKA-Gesetz" (2009) *Humanistischer Presseverband*, available online at http://hpd.de/node/6228.

3 EMPIRICAL STUDY RESULTS

The previous chapter (2) has raised a number of questions about the technical feasibility and legality of the use of new software-based investigative methods – such as the online searching of ICTs. In particular, the analysis of the case law has highlighted that legal practitioners disagree about the legality of these new investigative technologies. The judgment of the BVerfG,[146] while important in itself, did not provide sufficiently detailed reasoning about the precise legal requirements for the lawful use of this new investigative technology. It is a High Court ruling, which is focused on the definition of general new concepts, instead of developing detailed requirements for the lawful use of new new software-based investigative tools.

As discussed in the previous chapter, these new legal concepts, in particular the acknowledgment of the virtual living space, are of great importance for future law-making and policing of the digital sphere. However, the judgment did not fully resolve the debate surrounding the online searching of ICTs in particular, and of new software-based investigative tools in general. This leaves lawmakers and legal practitioners with a legal uncertainty about the usability of this method, as well as citizens insecure about the limits and restrictions of the policing of the virtual living space. This is particularly significant because, as discussed in the previous chapter, several European governments are already deploying this investigative method, or planning to introduce it in due course.[147]

Therefore, an urgent need exists to determine the most pressing problems for legal practitioners and other stakeholders concerned with the implementation and use of these new investigative technologies, and those stakeholders necessarily involved in this process, such as Internet Service Providers (ISPs). This ensures that the technical and legal analysis in this thesis is important and relevant for practitioners.

The analysis of the case study in the previous chapter has highlighted that only few details about the technical specifics of the new investigative measure, as well as the legal concerns of those concerned with its operation, are known. One reason for this is, as analysed in the previous chapter, the need for a certain degree of secrecy.[148] The

[146] BVerfG, NJW, 2008, 822.
[147] See section 2.7, p. 53.
[148] See p. 23.

disclosure of too many technical details can interfere with the clandestine use of the tool. This is also the reason why legislation drafted after the BVerfG judgment does not go beyond the requirements developed by the judges therein. A more detailed legal basis could reveal details about the tool, as well as the measure itself. In addition, more specific legislation would be more liable to constitutional challenges and scrutiny. However, despite this need for secrecy, thorough research into the technical specifics of these investigative tools is required to conduct informed legal evaluation and analysis about these tools. Particularly relevant is information about the problems these tools cause for practitioners involved in and affected by their use. Such information enables focusing on relevant topics and problems, and undertaking informed reasoning, which increases the practical relevance of the work.

Due to the lack of relevant publications and more detailed case law, it is impossible to determine these factors based on doctrinal, text-based research alone. Thus a different method is required to gain relevant insights and information.

To gain a better understanding, one part of the research for this thesis has therefore consisted of interviews with relevant stakeholders and experts in the United Kingdom (UK) and Germany. The results from these interviews have considerably influenced the structure and focus of the technical and legal analysis of this work.

3.1 Interviewees – The Different Stakeholders

The selection of the interviewees was to some extent influenced by the availability of relevant stakeholders.

Generally, the aim was to interview representatives from relevant governmental departments, law enforcement agencies, ISPs, and regulatory authorities from both the UK and Germany. In addition, to gain a better understanding of the technical aspects of this investigative measure, a neutral technical expert with a relevant background and understanding of the specific topic was selected.

As indicated, the relevant topic is of sensitive nature, and no detailed information is available in the public domain. The condition for the interviews was therefore that no statements can directly be quoted. The interviewed stakeholders can be named, and the information can be worked into the thesis, but no statement can directly be linked to one stakeholder. While this to some extend restricts the use of the empirical data, its value and importance for this work outweighs these limitations.

3.1.1 Interviewees Germany

The following stakeholders and experts were interviewed in Germany:

Organisation	Name	Function
Bundesministerium für Wirtschaft und Technologie (Federal Ministry for Economics and Technology)	Rolf Bender	Senior Officer for Media Law and New Services
Bundesministerium für Justiz (Federal Ministry of Justice)	Marcus Schladebach	Senior Officer for Media Law
BITKOM (Federal Association for Information Technology)	Guido Brinkel	Head of Media Policy
FSM (Association for the voluntary self-control of the Internet)	Sabine Frank	Managing Director
eco (Association of German Internet Industry)	Frank Ackermann	Director Self-Regulation
Deutsche Telekom AG	Veronica Frey, Andreas Goeckel	Senior Officers Multimedia and Internet Law
Chaos Computer Club	Volker Birk	Member

In Germany, the attempt to interview a relevant law enforcement agency was unsuccessful. No agency was willed (or cleared) to discuss this investigative method. However, the representatives of the federal ministries were able to answer all questions, because they closely collaborate with the German Federal Criminal Agency (Bundeskriminalamt).

As technical expert a member of the German Chaos Computer Club (CCC) was chosen, because the CCC was technical advisor to the BVerfG. This means that members are well informed about the technical details and capabilities of the tools deployed.
The BITKOM, FSM and eco are regulatory authorities, which collaborate with both the government and stakeholders from the so-called Internet value chain, most prominently ISPs.[149] These regulatory authorities are important for ensuring that a balance is kept between the regulatory requests of the government, and the protection of the citizens and the stakeholders of the value chain.

3.1.2 Interviewees UK

Organisation	**Name**	**Function**
Ministry for Business, Innovation, and Skills	Nigel Hickson	Head of Global ICT Policy
SOCA e-crime unit	Jonathan Flaherty, Richard Hyams	Technical Senior Officers
OFCOM	Jeremy Olivier	Head of Multimedia
ISPA UK	Andrew Kernahan	Policy Officer
Vodafone	Neil Brown Stephen Deadman Richard Feasey	Legal Advisor Executive Solicitor and Vodafone's Group Privacy Officer Public Policy Director
HM Revenue and Customs	Simon Bird	Data Analytics Team – Web Robot

OFCOM and ISPA UK are both regulatory authorities concerned with the balancing of interests of governments and industry stakeholders. The interviewees of the SOCA e-crime unit and the HM Revenue and Customs department were of particular relevance, because both are involved in the development and deployment of software-based investigative technologies. The interviews therefore provided crucial insights into the problems and challenges faced by investigators during the development and deployment of these new investigative technologies.

[149] For more information on the Internet value chain, see e.g. S J Barnes, "The Mobile Commerce Value Chain: Anlysis and Future Developments" (2002) 22:2 *International Journal of Information Management*, 91-108.

3.2 Methodology

For this thesis, the chosen methodology to collect the empirical data was to conduct qualitative research interviews. The reason for choosing this methodology, over for example quantitative interviews in form of questionnaires, is that this is an exploratory study that aims to establish the general problems and challenges faced by the different stakeholders with regard to the new investigative technologies.

A qualitative research approach is particularly well suited for collecting empirical data about a vague and complex topic. As Field and Morse put it, qualitative research is particularly useful for studying "phenomenon or events about which little is known."[150] Principally, qualitative research methods should be used when there is little known about a subject. Quantitative research methods are particularly useful when the phenomenon or topic is already well researched, and the aim of the study is to confirm a new theory. Or to put it differently "quantitative research seeks causes and facts from the epic or 'world view' perspective.[151]

As stated above, only very little is known about the technical details of the new software-based investigative tools, as well as the legal and practical problems caused by their usage for the stakeholders involved in the process. Qualitative research is therefore the adequate methodology to collect relevant data and information about these issues.

Qualitative research interviews try to establish something from the subject's point of view, and uncover the meaning of their experiences.[152] Hence this approach focuses on individuals' experiences and perspectives and can therefore provide a detailed description and insight into previously unexplored topics.

Interviews in particular allow people to convey to others a situation from their own perspective and in their own words.[153]

Collecting data through face-to-face interviews has many advantages, and was therefore the preferred method over, for example, telephone interviews. Among other things, a face-to-face communication enables a better control over the interview process. The interviewee can be put at ease by the use of effective interpersonal skills, and questions can be reworded if necessary. Hence the interviewer can clarify

---

[150] J M Morse, P A Field, *Nursing Research: The Application of Qualitative Approaches* (Cheltenham: Nelson Thornes, 2002, 3rd ed) 8.

[151] Morse/Field, ibid, at 9.

[152] S Kvale, *Interviews: An Introduction to Qualitative Research Interviewing* (Thousand Oaks California: Sage Publications, 1996) 30.

[153] Kvale, ibid, at 35.

ambiguous or unclear questions, as well as misunderstandings and misinterpretations by the interviewee. This contributes to the reliability and validity of the collected data. According to Gillham, quantitative research questions can generally be defined according to the following criteria:[154]

1. Questions asked, or topics raised, are 'open' with the interviewee determining their own answer. This is a key distinction from questionnaires where normally the researcher not only asks the questions but also provides the answers in some sort of choice format, for example, ranking preferences in order, circling one item on a 'very satisfactory' to 'very unsatisfactory' scale, and so on.

2. The relationship between interviewer and interviewee is responsive or interactive, allowing for a degree of 'adjustment': clarification, exploration, for example: *Tell me more about that,* or *I don't think I quite understand.*

3. There is structure and purpose on the part of the interviewer even when the context, like informal questioning in real-life settings, is 'natural' or at least naturalistic in the sense of taking advantage of opportunities that arise.

Throughout the interviews in this research study, the open question methodology was applied. By using general and open-ended questions the interviewees are encouraged to provide their own views, and explain their own experiences. This means that more detailed and relevant information can be obtained deploying this methodology instead of a more stringent and structured methodology approach.
Nevertheless, a framework of questions was developed, which was the basis for all interviews, to ensure that the general structure of the interviews was identical, and thus the collected data comparable.[155] These questions were emailed to the interviewees before the interviews, so that they had a chance to prepare themselves adequately, and thus feel more at ease during the interviews.
The interviews in this study lasted between approximately 60 to 120 minutes. All interviews were conducted at the premises of the interviewees. Hence the settings varied. Because most of the interviewees objected to the recording of the interview due

[154] B Gillham, *Research Interviewing: The Range of Techniques* (Berkshire: Open University Press, 2005) 3.
[155] See Appendix I for a list of these questions.

to confidentiality regulations, notes were taken during the interviews. These transcripts were turned into field notes after every interview highlighting the areas of key significance.

This type of qualitative research produces vast amounts of rich data, which need to be systematically analysed in a logical fashion.[156] This is particularly important for this study, because the interviews were conducted with different stakeholders, looking at the issue from different perspectives and with different motivations. This means that there was only very limited consensus among the interviewees. This was further complicated by the fact that the interviews were undertaken in two different countries, which means that different jurisdictions, and different (legal) backgrounds with regards to the new software-based investigative tools influenced the statements of the interviewees.

To enable the subtraction of key statements and determine whether common concerns among all stakeholders existed, the data was subjected to the three-stage qualitative data analysis method described by Miles and Huberman: *data reduction*, *data display* and *data conclusion drawing*.[157]

Data reduction refers to the process of "selecting, focusing, simplifying, abstracting and transforming" the data.[158] This process ensures that data is presented in such a way that final conclusions can be drawn.

For this study, the interview transcripts were re-written after the interviews and then checked for overlapping data in response to the different questions. These overlaps were highlighted. This was followed by a selection of the key statements of each interview, which were collided into a new document. This list of key statements for each of the questions highlighted the different views of the interviewees on the topic. It also highlighted where problems and challenges arising from the use of the new tools for the stakeholders differed, and where these were the same. This was particularly important for the integration of the interview results into the remainder of the thesis.

Data display refers to the representation and visualisation of the relevant data. In this case, the data were presented in the form of a narrative text, supported by excerpts from the data results. This form of data display was chosen in particular because, as discussed above, the individual statements could not be directly linked to the relevant

---

[156] M B Miles, A M Huberman, *Qualitative Data Analysis: An Expanded Sourcebook* (Thousand Oaks, California: Sage Publications, 1994, 2nd ed) 34.

[157] M B Miles, A M Huberman, *Qualitative Data Analysis: A Sourcebook of New Methods* (Thousand Oaks, California: Sage Publications, 1984) 20ff.

[158] Ibid, at 21.

stakeholder for confidentially reasons. A narrative text was therefore the best-suited approach.

Data conclusion drawing refers to the subtraction of conclusions from the collected data, and their verification. The conclusions relevant for this thesis were drawn from the key statement document, and verified during the analysis of the data and where necessary, confirmed by the relevant stakeholder.

3.3 Interview Settings

As indicated above, the interview topic is highly sensible and interviews were difficult to arrange. Generally, all interviews had to be conducted at the sites of the interviewees. Particularly for the interviews with the governmental bodies, extensive clearance processes were required before the interviews were approved. In some cases, the interview questions also had to be cleared before the interviews were approved.

As stated above, the overarching condition of most interviewees for participating in the interviews was that no direct quotes were to be made in the writing up of the results. Additionally, some of the interviewees required a copy of the write-up to check that no direct quotes were made, and only approved information was used.

In addition to these prior checks, some of the interviews were strictly monitored. On one occasion, the interviewees were not physically present in the same room. The interview was conducted via video link. Present with the interviewees was a legal advisor. The reason for conducting the interview via video link was that the sound could be muted whenever the interviewees were uncertain whether they were allowed to answer a question, and if so, how and were able to consult with the legal advisor in private. This interview was the shortest of all, and was suspended by the legal advisor when he had the impression that all authorised information had been provided. This was the interview with the strictest security measures in place and the least possibilities to influence the course of events.

Security measures during other interviews included the recording of the interview, the search of bags for recording devices, and frequently the presence of a legal advisor. However, while these security measures meant that some restrictions about the type of questions that could be asked and the amount of information given existed, these measure in itself also highlight the sensitive nature of this topic, and the confusion and insecurity surrounding it. Even those directly involved in the implementation (whether

pertaining to the legal or technical aspects) are still highly insecure about the measure and its legality and technical feasibility.

3.4 Interview Results

The interview results are depicted here in one narrative text, highlighting the key findings and conclusions. For the purpose of this chapter, these are divided into technical, and legal/regulatory findings. This is in line with the structure of this thesis. While the first necessarily impacts on the latter, the basic structure of these two areas differs significantly and thus a separation of these areas leads to more clarity and accuracy.

3.4.1 Technical Results

The overarching goal of the interviews with the technical experts, and those involved in the development of new investigative technologies was to establish whether the proposed investigative measures are technically feasible, and to determine the technological foundations of the new investigative technologies. Only very limited information about these matters is publicly available, however, more details are of great importance for the technical analysis in the following chapters, as well as the discussion of the legal challenges and the development of a regulatory approach in chapters 6 – 9.

The analysis of the case law produced by German courts, and the discussion of the online searching of computers by technical and legal experts in Germany in the previous chapter has sketched out a framework of desirable features these new investigative tools should possess. However, the source and validity of this information is mostly unknown, and thus the data is less reliable.

The interviews were broadly divided into two parts. The first part was concerned with questions about the feasibility of the specific investigative measure, the second with questions about the underlying software of this new generation of cyber-cops.

The concept of remote online searches of ICT devices by a piece of software can appear challenging or unrealistic to a technical layman. The technical feasibility of this investigative method, and the development of such a complex tool seem unlikely. This view was confirmed by the few technical details publicly available about the proposed online search, and contradictory statements from various technical and non-technical

experts.[159] This scepticism and lack of knowledge about the technical feasibility of the method is problematic and contra-productive for an informed discussion about the legal problems of these new investigative technologies.

The interviews with the technical experts have yielded that principally software-based investigative tools have been developed and used for investigative purposes for the past 10 years.

However, all stakeholders confirmed that thus far, the general approach to software-based investigative technologies was to acquire and utilise existing technologies. Hence, the capabilities of these technologies were limited by their pre-determined design, which was defined by developers not linked to law enforcement agencies. In most cases, the technologies used were developed with fundamentally different applications in mind (such as web-crawlers designed for e-commerce applications or search engines). This caused several problems, but the most significant are the limited benefits to investigations, the unreliability of the tools, and the reliance on external developers. In addition, another significant problem of this approach is that the software products used are not exclusively designed for law enforcement authorities. This means that these products are also used commercially, as well as by private persons, and among other things for criminal purposes.
One example of such a technology are so-called web crawlers,[160] which have been used since 2003 by authorities in the UK to stroll the Internet and collect suspicious material from websites. This software operates based on information retrieval techniques that select data based on key words that are pre-defined by the operators. The problem with this approach is that it is impossible to update or modify the software because it was developed externally. As a result, while the Internet and ICT technologies advance and develop further, the technology becomes outdated and results are therefore less meaningful and valuable. Another problem is that because the technology is also commercially available, protection measures against it are easy to develop. Hence, the value of this technology for investigations is limited.

---

[159] See chapter 4 p. 86 for more details on this.
[160] A web crawler is a computer program that browses the Internet in an automated and predetermined manner. See: S Brin, L Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine", (1998) 30(1) *Computer Networks and ISDN Systems*, 107.

Thus more recently, a different approach has been pursued by law enforcement agencies. All stakeholders stated that the widespread of and heavy reliance on ICT devices and the Internet has led to a need for more adequate investigative tools. To avoid the above problems, software developers have been recruited to develop in-house technologies for investigative purposes. The advantage is that these technologies can be tailored to the needs of the relevant authority, and details are kept confidential in-house.

Two major concerns with this approach exist. Firstly, the costs of developing these tools are comparatively high, and this is the main reason why this task has been outsourced so far. Thus, the development heavily relies on the available budget. In addition, some of the technical experts have indicated in the interviews that payment for excellent software developers is much better in industry compared to what the government pays. In addition, skilled software developers (and in particular hackers, who often develop the most advanced software tools) oftentimes have a work ethic that contradicts with working for the government and, in particular, for law enforcement agencies. This work ethic has its roots in the principle that the Internet should be an unregulated space. This means that skilled software developers are often not willed to work for the government. This was also confirmed for the specific case of the online search software in Germany. The government had advertised positions for software developers and directly approached the hacking community.[161] The general consent there, as indicated by one of the interviewees was that these jobs were not something highly skilled software developers or hackers would be interested in. Hence, the development of these tools is problematic, because the costs are high and finding skilled developers can be difficult.

Secondly, all technical experts expressed their concern over the fact that developing more complex software-based investigative tools means entering into an "arms race" with Internet and ICT users with criminal intent. The development of malicious software, as well as protection and anomymisation software is advancing continuously, and mainstream products can be purchased or downloaded free of charge. Hence, protection measures against new investigative tools can easily be developed once details about the tools are known. This means that law enforcement agencies in turn have to enhance their tools or develop more sophisticated ones to cope with the newly

[161] See for a recent example of such a job advertisement V Briegleb, "30 Planstellen für den Staatstrojaner" (2012) *heise*, available online at: http://heise.de/-1414154.

developed protection measures. This leads to the so called "arms race", which refers to the continuous need for updating of software and ICT tools by governments and users to enable the investigation of the Internet and ICT devices, and the protection from these investigative actions respectively.

Furthermore, investigative software is in most cases at least rudimentary based on already existing software classes,[162] which means that technically versed Internet users can detect investigative software tools and use these for their own purposes, or develop counter measures.

These problems are unavoidable consequences of the development and use of ICT investigative tools. It is hoped that the in-house development of these tools and the associated confidentiality of the developing process minimises them.[163]

Another problem discussed by some of the technical experts is the lack of technical knowledge of the investigators using the ICT-based investigative tools. These require a certain amount of technical understanding and many law enforcement officers are overstrained with the operation of these tools. Training, however, is expensive and time-consuming. Hence, mistakes are being made and as a result, seized data becomes unusable. The establishment of specialist units is still a concept in its infancy, and currently the necessary funding is often problematic. Only very few of these units already exist (one example for such a unit is the SOCA e-crime unit).

In addition to the lack of funding, the reason for this is also that governments have only recently realised the need for these investigative tools and the resulting need for specialists, both developers and operators.

All experts confirmed that the development of a software-based investigative tool to remotely search ICTs, and thus the measure itself, is feasible from a technical point of view.

---

[162] See chapter 4 for a discussion of this.

[163] The problem of relying on commercial software products for investigative purposes was demonstrated by the Chaos Computer Club in Germany in late 2011, when members got hold of the software deployed for online searches of ICT devices and analysed this and published the results. While internally developed software could equally be leaked to the public the risks for this happening are considerably smaller the fewer institutions are involved in the development. See: Chaos Computer Club, *Analyse einer Regierungs-Malware*, 08.10.2011, available online at: http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf; DJ Walker-Morgan, "CCC Cracks Government Trojan" (2011) *The H Security*, available online at: http://h-online.com/-1357755.

The consent among experts was that such a piece of software has great similarities with existing spyware and malware, as well as autonomous agent software. The only difference is that it is government designed and operated.

This means that even without knowing all technical details of the new investigative tools, it can be established that these can be designed to be capable of any actions related technology is. The general consent was, that the investigative tool is principally capable of clandestinely infiltrating an ICT device, and autonomously searching and seizing relevant data.

One of the technical experts explained that the degree of autonomy and other capabilities of the software tools depend on their design, and thus of the decisions of the software developers. However, it was stated that it is generally possible to implement the required capabilities into software.

One significant problem, however, was identified, namely the infiltration of a specific ICT device. It was explained by one of the experts that guaranteeing that the system of a specific user is infiltrated requires the collaboration of another party. This could either – unknowingly - be the target person,[164] or a third party involved in the transfer of the data (for example the ISP) or the developer of the hardware or software.[165]

The involvement of third parties is very problematic. All interviewed stakeholders discussed this aspect.

The interesting observation made here was that different stakeholders came to different conclusions. While this was to be expected to some degree, because law enforcement and governmental agencies have different interests than other stakeholders in the value chain (such as ISPs, software developers etc), and therefore perspectives on this aspect, a more unified opinion and approach had been expected.

Government and law enforcement agencies stated that security aspects should have precedence over privacy and data protection concerns, as well as economic concerns of

---

[164] See chapter 2, p. 31 for a longer discussion of this possibility.

[165] An example in point for this is the attempt by the Chinese government to mandate the implementation of software into new PCs by manufacturers, which provides a "back door" into the PCs, and thus access to all data and processes. See for a summary of this e.g. G Duncan, "China to Mandate Internet Filtering Software on PCs" (2009) *Digitaltrends*, available online at http://www.digitaltrends.com/international/china-to-mandate-internet-filtering-software-on-pcs/.

the relevant stakeholders.[166] Some of the interviewees from law enforcement expressed that they regard their work to be hindered by what they referred to as "uncooperative behaviour" of other relevant stakeholders. They also stated that ultimately they would not see any other option but the full cooperation of third parties on these matters.

Governmental departments regard compulsory cooperation of third parties as an option, but are currently exploring all possibilities without further formulating demands. However, cooperation is regarded to be vital in the future for cases of serious crime.

Third parties affected by this on the other hand stated that they regard themselves not in a position to cooperate with governmental and law enforcement demands. Particularly, because they have a contract with their customers, that is build on trust. If customers become aware of the fact that these companies cooperate with law enforcement to facilitate access to customer's data, they would terminate their contract, or choose other provider. Also, stakeholders stated that they consider having a duty towards their customers to protect them from unjust acts if at all possible.

They discussed further that they regard a compromise such as cooperation in cases of (suspected) serious crime as a "slippery slope" problem. Meaning that they fear that once they agree to assist in, for example, child pornography cases, they would make themselves liable to cooperate also in other cases, which are less severe.

However, the remarkable outcome was that none to very little direct discussion has so far occurred between affected stakeholders. This means that no compromise can be reached, unless legislation introducing a duty of care or duty to cooperate is implemented.

The technical results of the interviews confirmed that theoretically, software could be designed to execute an online search of ICT devices,[167] and more generally, to introduce cyber-cops replacing humans for policing tasks. These technical details are used as a basis for the detailed analysis of the relevant technologies in the technical chapters of this work.

---

[166] Identified as relevant stakeholders were particularly ISPs and software developer.

[167] This was also confirmed by the analysis of the "Federal Trojan" software by the Chaos Computer Club. See Chaos Computer Club, note 171, F Rötzer, "CCC entlarvt Bundestrojaner und Sicherheitspolitik" (2011) *TELEPOLIS*, available online at http://www.heise.de/tp/artikel/35/35648/1.html.

3.4.2 Legal and Regulatory Findings

The goal of the interviews was to determine the legal and regulatory challenges that arise from the use of ICT-based investigative tools for online searches of ICTs specifically, and the use of cyber-cops for policing activities of the virtual living space in general. The problem of the valid legal basis is so far the only issue that has been analysed and discussed at length. Hence, this legal issue was not discussed further with the experts.

For the purpose of the interviews, it was assumed that a valid legal basis for such actions exists. Since the BVerfG established in its judgment that these investigative tools and measures are not generally unconstitutional,[168] and the EU has recommended the introduction and facilitation of online searches, it can be assumed that the question of a valid legal basis will not be a problem in the future. As discussed in the previous chapter, several German federal states have already introduced a legal basis based on the BVerfG judgment.[169] While the constitutionality of these laws has been challenged again,[170] it is unlikely that the BVerfG will rule the measure to be generally unconstitutional. The Court might take this opportunity to develop more detailed conditions for the use of this new investigative measure. Ruling this generally unconstitutional, however, would contradict the previous judgment.

It needs to be highlighted, however, that when stakeholders mentioned the legal basis issue, those from Germany identified it as a more serious problem than those from the UK. In the UK, stakeholders generally identified other legal issues as the more pressing ones, and assumed that such investigative actions are covered by existing legislation, in particular the *Regulation of Investigatory Powers Act 2000* (RIPA).

Thus the interviews focused on determining other pressing legal and regulatory issues arising from the use of these new investigative tools for legal practitioners. To the best knowledge of the author, this has not been undertaken so far, and thus the analysis of these legal and regulatory problems, and the development of a solution for these is an important contribution.

All stakeholders pointed out that there is a dichotomy between what is technically possible and legally allowed. The problem is oftentimes that investigative tools are developed without the legal requirements and challenges in mind, and these only

---

[168] BVerfGE, NJW, 2008, 822.

[169] See p. 55.

[170] At the time of finishing this thesis the constitutional complaints were still pending.

materialise once the tools are deployed. Because the regulation and policing of the Internet and ICT devices is such a new area, few if any laws exist that deal explicitly with the regulation of ICT-based investigative tools. Hence legal practitioners deploying these tools are insecure about the legality of certain investigative measures.
Generally, the legal and regulatory issues exist on two levels, the national and the international level.
On the international level, stakeholders from both jurisdictions (Germany and UK) pointed out that there is a lack of cooperation and harmonisation on this topic. It was stated that the biggest problem is the lack of consistency in how countries approach this matter. Some member states chose a restrictive approach, while others introduced, or plan to introduce these software based investigative tools without any technical or legal restrictions. Others have no plans to introduce these tools at all, and have also not formed an opinion on this. While the different handling of criminal investigations is a very common phenomenon in different jurisdictions, and does not usually cause problems, the problem with this particular investigative measure is that the online searching of computers can have extraterritorial consequences. The Internet is a space where national borders are not represented in the same way as they are in the offline world.
All interviewees identified the extraterritorial risk as one of the most pressing problems of the use of cyber cops. The particular problem is that the infiltration of ICT devices can occur while these are located in a different jurisdiction, or these new investigative tools, given their networked operating environment, can access data that is stored in a different jurisdiction. This can happen intentionally and unintentionally. The specific problems identified were (1) whether the accessing of data and infiltration of an ICT device constitutes an extraterritorial violation. Furthermore, (2) in which cases, if at all, are such extraterritorial actions allowed? Is this only in cases of (suspected) serious criminal activities the case, or also in less serious cases. (3) Are any formal requests of assistance necessary in these cases, given that no human officer enters foreign territory? (4) What kind of checks are necessary to determine whether an ICT device or relevant digital data is located abroad. And (5) how can extraterritorial violations be avoided.

The interviewees indicated that this is an entirely new problem, and no solutions have so far been discussed on national or international level to solve these issues. In particular, the stakeholders concerned with the operation of the tools indicated that

these are very pressing and worrying matters, and solutions need to be developed to ensure legal certainty.

This also requires an international discussion and agreement about the use and regulation of these tools in other jurisdictions.

It was further stated, that generally the problem of introducing legislation dealing with the policing and regulation of the Internet is that recent attempts in both jurisdictions (Germany and UK) to draft such legislation have been highly problematic and controversial.

In Germany, the law to complicate access to child pornographic material (*Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen* -Zugangserschwerungsgesetz)[171] was drafted in 2009, and came into force in 2010. The law requires the German Federal Criminal Police Office (Bundeskriminalamt - BKA) to compile a list with domain names, IP addresses and URLs of websites containing child pornographic material or linking to websites containing such material, which needs to be updated daily. ISPs with more than 10,000 customers are then obliged to block access to the websites on this list, at least on the DNS level.

The law was heavily criticised for being ill drafted and ineffective. The concept of blocking content is very controversial, among other things because there is a risk of Internet state censoring of content since there is no objective controller entity verifying that the content to be blocked is indeed unlawful.

Due to the enormous public criticism of this law, the government agreed that the BKA would not compile a blacklist, nor ask ISPs to block content, and a law was drafted which annulled the Zugangserschwerungsgesetz in 2011.

In the UK, the *Digital Economy Act* (DEA) was adopted in April 2010. It includes eleven topics, one of which introduces a graduate response system to copyright infringements.[172] After a certain number of copyright infringements (i.e. the downloading and uploading of copyright infringing material online), an ISP may be required to disconnect a subscriber from the Internet. In addition, the Secretary of State may impose technical obligations on ISPs, obliging them to undertake measures against its subscribers, such as a limit of speed or capacity, a block or limit on

---

[171] http://www2.bgbl.de/Xaver/start.xav?startbk=Bundesanzeiger_BGBl.

[172] http://www.opsi.gov.uk/acts/acts2010/pdf/ukpga_20100024_en.pdf. Explanatory memorandum: http://www.publications.parliament.uk/pa/ld200910/ldbills/001/2010001.pdf. See also for an earlier consultation: http://www.berr.gov.uk/consultations/page51696.html.

subscriber's access to certain material or a limit on or suspension of the service to the subscriber.[173]

The DEA was heavily criticised by consumer rights and privacy groups, as well as academics working in the field of Internet regulation.[174] The criticism focused primarily on the requirement to disconnect users, and the lack of protection for institutions offering Internet access, such as libraries and universities.

The High Court of Justice granted a judicial review of the DEA on November 10 2010.[175] In April 2011 the Court, in its decision about the judicial review, upheld most of the criticised provisions.[176] However, the Court of Appeal has granted on 7 October 2011 the permission to appeal against the High Court ruling that upheld most of the criticised provisions.[177]

Both controversial regulatory attempts, and the criticism and problems associated with the enactment of these laws, have left governments and policy makers insecure and reluctant to introduce new legislation dealing with the policing and regulation of the Internet.

Furthermore, as indicated in the previous section,[178] the involvement of intermediaries such as ISPs is highly problematic. As discussed there, intermediaries have a trust-based relationship with customers, who pay for services and expect in return a certain degree of confidentiality and protection of their data. In addition, particularly in Germany the regulations on the secrecy of telecommunications restrict the possibilities of intermediaries to carry out certain technical measures, and release, or enable access to private data.

---

[173] See also: http://www.berr.gov.uk/consultations/page51696.html.

[174] See e.g., C Doctorow, "Britain's New Internet Law -- As Bad as Everyone's Been Saying, And Worse. Much, Much Worse", (2009) *boingboing*, available at http://www.boingboing.net/2009/11/20/britains-new-interne.html; L Edwards, "Mandy and Me: Some Thoughts on the Digital Economy Bill", (2009) 6:3 *SCRIPTed*, 534, available at http://www.law.ed.ac.uk/ahrc/script-ed/vol6-3/editorial.asp.

[175] Out-Law, "Digital Economy Act to be Reviewed by Courts and Parliament" (2010) *out-law* http://www.out-law.com/page-11538.

[176] P Bradwell, "Judicial Review of the Digital Economy Act" (2011) European Digital Rights, available online at: http://www.edri.org/edrigram/number9.7/judicial-review-digital-economy-bill.

[177] BBC News, "BT and TalkTalk to Appeal Digital Economy Act" (2011) available online at: http://www.bbc.co.uk/news/technology-15212651.

[178] See p. 71.

On national level, most stakeholders identified the issue of reliability and usability of the data seized by a software tool as one of the most pressing problems.
The deployment of autonomously operating software tools that carry out actions usually undertaken by human officers, such as the search and seizure of relevant evidence, raises questions about the reliability of this evidence. Additionally, the problem is that the evidence collected is only available in digital format. Those stakeholders concerned with the collection and use of evidentiary material pointed out that digital evidence is still an underdeveloped area of law. There exists great legal uncertainty about the general admissibility and reliability of this type of evidence.
The technical experts added that the particular problem with digital data seized during an online search is that the software tool used to undertake the search necessarily compromises the target system. This causes problems for the reliability of the data.
The specific problems identified were (1) whether digital data seized by software tools can be regarded as admissible and reliable evidence. (2) In how far the use of an autonomous software tool to seize the data impacts the reliability and admissibility of the data as evidence. (3) How the potential compromise of the target system impacts the reliability and admissibility of the evidence, and (4) in how far digital data seized from a live system can be used as evidence.

The interviews showed that the subject of digital data as evidence, and in particular digital data seized by software tools and from live systems is still a grey area in both jurisdictions. However, this subject is of particular relevance for the digital data seized during cyber-investigations because it is oftentimes the main evidence in contrast to digital data that is seized during traditional investigations, which merely functions as a supplement. In line with the judgment of the BVerfG, which established that the virtual living space is as important as the physical world, future investigations will oftentimes solely focus on the virtual living space, hence any evidence will be in digital format and often seized from live systems using software based investigative tools.
This means that the evidentiary value of this data is extremely important for future investigations.
However, it was pointed out by several stakeholders that to date, this is an unresolved matter, and great legal uncertainty exists about this issue. Costly investigative measures though are only of any real value if the results can be used further during later legal procedures.

In addition, particularly German stakeholders pointed out that similarly to the harmonisation required on international level, this is also required on national level. All matters of police powers are federal state law in Germany; hence the different federal states can have different regulations on this topic. If these vary too much, the regulation of the above-discussed problems becomes even more difficult.

Another primary concern that most stakeholders from both jurisdictions shared concerned the adequate regulation of these investigative tools. As shown in the previous chapter, these new investigative tools carry out core policing tasks autonomously. Ensuring that these autonomously operating tools obey relevant laws and regulations during the investigative actions is a new challenge. All stakeholders pointed out that no existing regulatory methods exist at the moment that could deal with this challenge.

Other legal and regulatory problems were raised during the interviews. Some stakeholders mentioned the problem of software executing tasks normally carried out by a human officer. It was briefly discussed that depending on the degree of autonomy this could prompt problems for existing legal concepts tailored to human officers. Another concern that was raised by some of the stakeholders was the issue of liability for the actions of the software tool. In case damage or harm occurs, the question of liability needs to be established. Given that the tools operate autonomously, and solely the tools and not the human operator will undertake some decisions and legal reasoning, this becomes a pertinent issue.

3.5 Complementary Research Results

The sensitivity of the topic has, as explained above, shaped and restricted to some extend the interviews. To minimise the problems arising from the strict security protocols, anonymous interview statements, and qualitative interview approach for the results, the above outcomes are correlated with those of another survey that was carried out. This survey consisted of questionnaire-based interviews, combined with reports from experts. While the main aim of the survey had a different focus, the involvement of the author in designing the questionnaire, conducting the research and evaluating the outcome allowed aligning some of the issues with the problems

discussed here. In particular, it tried to give empirical backing to the theories on how lawyers cope with technology.

The survey was part of a project, which was partially funded by the European Union under the AGIS Programme, and focused on determining how legal practitioners deal with ICTs and their outputs, and in particular digital evidence and its admissibility to court proceedings, and whether specific regulations dealing with this type of evidence exist in their respective jurisdiction.[179] The methodological approach chosen for this study is indebted to the socio-legal tradition in comparative law.[180] Rather than asking simply what rules and regulations in different countries say, it tried to get a feel for the way in which lawyers make *sense* of these regulations in their practice. To achieve this goal, a two-pronged strategy was followed. Country reports were commissioned for 16 jurisdictions, where experts in academia gave an account of the legal situation, which was (admittedly to a limited degree) reviewed by the consortium members including this author. We took the resulting accounts as a good proxy for the "real" legal situation in these countries – and without analysing too deeply what "real" in this context means. In the second stage, questionnaires involving free text answers to problem questions together with simple tick box sections were send to practitioners in these countries – judges, prosecutors, forensic experts and defence lawyers. The return rate did not allow a statistically valid evaluation, therefore they were followed up with data coming from *in-depth interviews:* at the very least one representative from every professional group in each of the sixteen countries studied was interviewed, with questions based on those issues highlighted in the questionnaires from that country. The objective was to combine for each country a diverse and heterogeneous range of participants who can express different opinions with respect to how they are working in practice, advantages, inconveniences and future perspectives when dealing with *electronic evidence.* For this part of the fieldwork, we used three different protocols: one for lawyers, one for computer forensic experts, and a third for commercial actors. The total sample of field observations is made up of one hundred twenty-five questionnaires,

---

[179] Admissibility of Electronic Evidence (A.E.E.C.): Fighting against High-Tech Crime. For details on the project see F Insa, "The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime – Results of a European Study" (2007) 1:4 *Journal of Digital Forensic Practice*, 285-289.

[180] B Markesinis, "Judicial Mentality: Mental Disposition or Outlook as a Factor Impeding Recourse to Foreign Law" (2006) 80 *Tulane Law Review* 1325-1375.

This approach allowed us to identify if there were particular concerns and anxieties amongst lawyers about digital evidence, and whether their confidence, or lack thereof, matched their true understanding of the field (hence the prior evaluation of the laws by experts).

The aim was to get an idea of the "sense making" activities that lawyers perform when challenged by technological developments. We tried to visualise the data using "semantic networks", a method often employed in comparative and applied linguistics.[181]

The idea is to see how central concepts are for cognition by analysing how they are connected to other concepts. One graph that was derived from this project shall be shown here for illustrating purposes:

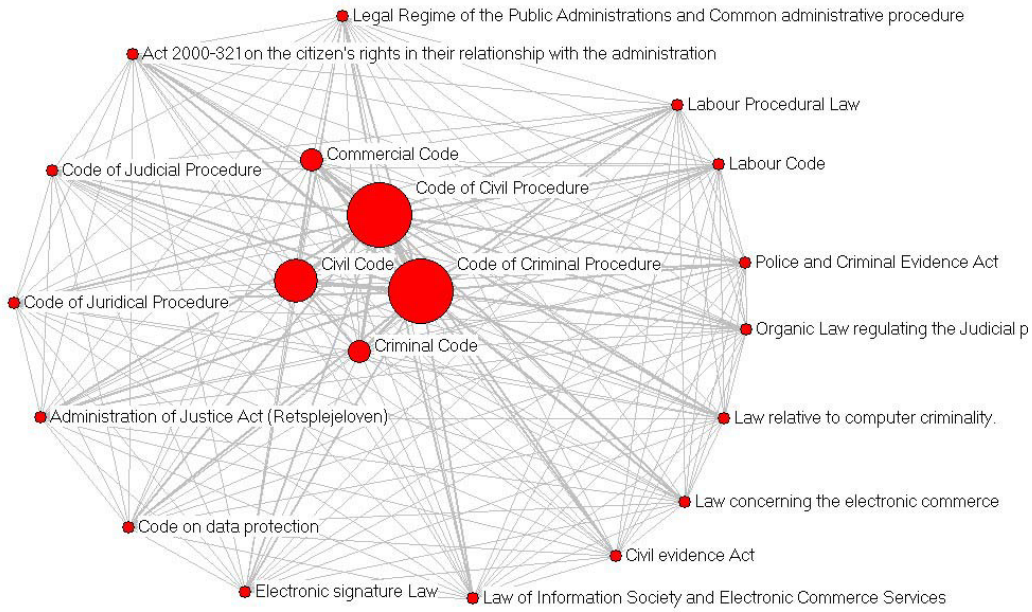

Figure 1: Visualisation of source texts

In this case, it tries to depict the source texts lawyers used to build analogies in response to the problem question given to them in the questionnaire.

[181] K M Carley, D S Kaufer, "Semantic Connectivity: An Approach for Analyzing Symbols in Semantic Networks" (1993) 3:3 *Communication Theory*, 183-213.

Even though the response rate precludes a rigorous mathematical analysis, certain trends emerged from the responses that are relevant for this thesis.

Generally, most interviewees from all countries stated that uncertainty exists about the regulation of ICTs and handling of digital data, which they identified as a source of concern. There seemed to be little connection between the correctness of their understanding of the technological issues and the confidence they expressed in handling them should the issue arise in court. Broadly speaking, the majority expressed their worries about their ignorance of the technological side, while affirming their belief that their legal skill sets would nonetheless allow them to come to a legally correct solution of any problem. As a preferred method to address these problems, two strategies emerged. One was to "black box" the entire question: this is a question of fact best left to the properly trained forensic experts, and we can implicitly trust their analysis. No further scrutiny, by a judge or under cross-examination, is necessary provided the proper procedure in determining the expert's expertise were followed.

The second strategy is the analogous application of existing legislation to the new issues. However, most interviewees stated that for this approach, knowledge about and understanding of the technical details of the respective technologies is required to develop successful analogies. They indicated that thus far, legal practitioners are not suitably educated in this area and expressed the concern that this will remain an issue in the future.

Paradoxically, it seems that the less they knew about the actual ability and limitations of (any type of) computer forensic technology, the more willing they were to make far reaching analogies to comprehend it. The introduction of new legislation however, was not a primary desiderata of legal practitioners to address this situation, with one notable exception: The international nature of cybercrime and digital evidence was recognised by all respondents, and to the extend that regulation and harmonisation was requested, it was to address perceived problems with the procedure in countries other than the respondents, to ensure that evidence obtained abroad could if necessary be used in the domestic court. This fits to the observation about the role of "trust" made above – lawyers are willing to trust in their compatriots, but are much less certain about "foreigners".

The results of these quantitative interviews are remarkably similar to those of the qualitative interviews depicted above. Particularly the points that legal practitioners recognise that they often lack the necessary knowledge about ICTs and their outputs,

but nevertheless use confidently and willingly often far reaching analogous applications of existing legislation to new settings. What they would like the most is for some authoritative source to confirm that their analogies are valid, rather than legislative intervention.

These results mean for this work that successful and correct analogies that achieve the equivalent to the analogue regulatory regime have to be facilitated, which requires that software-based investigative tools have to be developed with the cognitive coping mechanisms of legal pracititoners in mind. The question is how this problem is best addressed for the software-based investigative tools discussed in this work. Given the lack of technical knowledge of legal practitioners, the focus needs to be on designing the software tools to enable successful analogies. An analogy can be called "successful" in this sense if it achieves the equivalent regulatory effect. So in the example of the "Federal Trojan", to think of the software as the equivalent of a police officer is a legally valid analogy if it succeeds to protect the citizen from state intrusion just as much as if a real officer had tried to gain access to information about them, and gives the police access to the same data that they would have been able to acquire in the traditional form. With other words, the mere use of technology should not place either police or citizen in a better or worse position.

I hypothesise that analogies are more likely to be valid in this sense if it is realistic, that is if the lawyer does not attribute too much, or indeed too little, capacity to the autonomous forensic tool because he thinks of it as a "digital police officer". This can be achieved in two ways, both of which are discussed in this thesis: by better understanding the *legally relevant* features and limitations of the software tools, and by "forcing" the metaphor onto real life, that is, by ensuring computationally that the software does indeed exhibit facilities and capacities that are of the kind that in human police officers are attached to legal consequences That is they should have the computational equivalent to "having a reasonable suspicion", but need not have the equivalent of "liking donuts a lot".

How this can be accomplished to avoid reliability issues of for example a "black box" solution, where legal practitioners provide the input commands and the technology executes the reasoning and provides the outcome, which means that the responsibility

for the correct reasoning lies solely with the software engineers, and legal scrutiny of the reasoning process is impossible, is discussed in chapters 8 and 9 of this thesis.

This outcome however, supports the key argument of this thesis that software-based investigative tools are increasingly operating as "autonomous cyber-cops" assisting or replacing human officers for policing tasks.

3.6 Conclusion

The interviews provided some very important results for this thesis. The technical experts contributed that the use of complex software tools during investigative measures is not per se a new concept. However, the degree of autonomy of currently developed cyber-cops developed to undertake, for example, online searches of computers is novel. It was confirmed that the development of tools featuring the desired capabilities and necessary degree of autonomy is possible, albeit expensive. Technical experts also identified related software tools, which will likely serve as the basis for these new investigative tools. This is extremely important for the technical analysis in the following chapters, where this information, together with information publicly released by various governmental bodies, courts and other experts forms the basis for the analysis about the technical nature of the envisaged software based investigative tools.

Legal experts identified the most pressing issues that legal practitioners currently face during the introduction phase of these software tools and the new investigative measure.
These are (1) the extraterritorial impact, (2) the evidential value of the seized data, and (3) the regulation of the tools.
While other matters were mentioned and discussed, all stakeholders highlighted these issues as the most pressing problems. The reason why these issues were identified as such important matters, is that these challenge existing core concepts that have been tailored to human officers and investigations of the offline world. In addition, these are fundamental problems, which, if not solved, could potentially jeopardise the use of these tools and violate rights of suspects.
This evaluation of legal and regulatory problems by stakeholders directly concerned with the development and use of these new investigative tools is profoundly important

for this thesis. Analysing problems that are of high relevance to practitioners means that the work of this thesis has the potential to directly impact on policy making. Some of the stakeholders asked to receive a copy of the completed work and discuss the results further, hoping that some of the analysis of this thesis could be significant for their work.

More generally, these interviews have highlighted that the current approach to technology regulation, dealing with problems when they are pressing, is problematic. All stakeholders have highlighted that foresight is necessary for the regulation of these new investigative tools, and more generally the policing and regulation of the virtual living space. Recent examples, such as the rushed DEA in the UK and the Zugangserschwerungsgesetz in Germany, highlight that it is important to foresee legal and regulatory problems, and draft legislation carefully.

Another problem that has become evident is that several stakeholders are involved in the policing of the virtual living space, and the development and use of new ICT-based investigative measures. Among others, private bodies, usually intermediaries are affected. However, when the boundaries between public and private bodies are blurred, problems arise because fundamentally different perspectives clash. However, no cooperation or discussion between these different stakeholders occurs. This needs to be changed to enable the development of a legally sound compromise.

In addition, the policing and investigation of the virtual living space requires more international cooperation and harmonisation because national borders, which traditionally served as sovereignty indicators and boundaries, do not exist in the virtual living space. It is therefore crucial that sufficient agreements are in place, to avoid violations of international laws, and enable the proper and lawful use of new investigative technologies.
It was stated that one of the German regulatory authorities organised a meeting of international e-crime units, which was the first of its kind and well received. The aim of the meeting was to establish contacts and networks for future collaboration. However, it would be important to have policy makers present, so that they become more aware of the practical problems these new investigative measures cause, and can discuss and develop national and international legislation to solve these.

The partially very strict clearance procedures prior to the interviews and the settings of some of the interviews highlight the sensitivity of this topic, but also the great insecurity of all involved stakeholders. Specific questions about the technical details of the tools, as well as questions about the past and current conduction of online searches were often not answered (where a legal advisor was present, these questions were always discussed with him). This silence is telling in itself. It highlights again not only the need for confidentiality on this matter, but also the lack of knowledge and insecurity surrounding the use of software based investigative tools and the policing of the virtual living space.
The consequences of this insecurity, as well as lack of harmonisation on national and international level mean that legal practitioners directly involved in the use of these new investigative tools face a great legal uncertainty. Lawyers, for example, are faced with the problem of not knowing in how far evidence presented by state attorneys is authentic. Judges face the same problem of not knowing whether the evidence is or should be admitted.

The consensus of all interviewees was therefore that more legal and technical analysis of the most pressing issues is required to establish legal certainty for the future use of these tools.

4 SOFTWARE-BASED INVESTIGATIVE TOOLS

One central problem identified in the previous chapters is the lack of detailed technical knowledge about the new software-based investigative tools. This is partly due to confidentiality reasons as chapter 3 indicated, but also highlights that legal practitioners often have little or no understanding of computer technology and try to avoid (commissioning) deeper technical analysis of such new software-based tools. Instead, the focus is often on the rights violations of such investigative acts (the BVerfG judgment is an example in point) and legal procedural topics, such as a valid legal basis. The preferred methodology is the application of legal analogies to the new situation.

However, the lack of technical details constraints a deeper legal conceptual analysis of such software-based investigative tools and their actions. This is particularly problematic if the tools significantly impact existing policing structures, such as the introduction of virtual police officers, which can fully replace human officers for some policing functions. The successful application of analogies to such new circumstances becomes problematic, if not impossible.

Given the significance of the virtual living space for people's lives it is important to develop a successful regulatory approach for software-based investigative tools.

This chapter analyses the technical details of software-based investigative tools, focusing primarily on the software tools deployed for online searches of ICTs. As discussed, this is currently still a comparatively task-oriented and simple technology but already triggers all problematic aspects that future, more autonomous, advanced, and intelligent software tools also feature. In a second step, an already more sophisticated technology is analysed that shares crucial features with the online search software and is already used by LEAs.

In the first part of this chapter, the specific technology underlying the remote online searching of computers is presented in section 4.1. As starting points for this analysis serve both the public debate about the specifics of the technology, and the interview results. This is followed by a classification of this technology in section 4.2. Section 4.3 evaluates the legal status of this technology. In section 4.4 a related technology,

autonomous software agents, which shares some attributes with the software used to remotely search computers, and is equally used by authorities already, is discussed. One example of the application of this technology in law enforcement activities is introduced in section 4.5. Provisional conclusions are drawn in section 4.6.

4.1 Technical Details of the Online Searching of Computers – The Public Discussion

The discussion about the specific type of software used to undertake the online searching of computers and its potential capabilities was manifold in several European countries, but particularly in Germany. This discussion was accompanied by debates about the feasibility of the proposed activities. This section provides an account of these debates and summarises the main arguments, before analysing the state of the art of the relevant technologies in section 4.2 to draw a realistic conclusion about abilities and feasibility at the end of that section.

4.1.1 Proposed Type of Software and its Abilities

Technical details about the type of software to be used to undertake online searches of computers, or its abilities, have not officially been disclosed by the governments in any of the countries discussed in this thesis.[182] As discussed in the previous chapter, the reason for this is that information about such measures is classified as highly sensitive, to complicate the detection of the software on a system and the development of potential countermeasures.

The German government, in an official request for information about the topic of online searches by the then oppositional German liberal party *FDP*, confirmed this need for secrecy about the particulars of the software, stating that information about the technology can only be disclosed to involved authorities.[183] An investigating judge of the German Federal Court of Justice (BGH), when approving a request to undertake an online search of an ICT device prior to the BGH ruling,[184] was the first member of the

---

[182] During the research for this thesis, the author has also not come across information released about technical details of similar measures by governments of countries other than those discussed here.

[183] BT-Drucksache 16/4997, "Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Sabine Leutheusser-Schnarrenberger, Jörg van Essen, weiterer Abgeordneter und der Fraktion der FDP" 10.04.2007, p.2, available online at http://dip21.bundestag.de/dip21/btd/16/049/1604997.pdf.

[184] See e.g BGH, Beschluss vom 21.02.2006 – Az. 3 BGs 31/2006, http://www.hrr-strafrecht.de/hrr/3/06/3-bgs-31-06.php; Leipold, note 48, at 315.

judiciary to comment on the desirable technical abilities of the proposed software. He stated that a specifically designed piece of software would infiltrate the computer of the suspect "from outside" to copy the stored data and subsequently transport it back to the investigating authority.[185]

This was followed by the decision of the BGH on the legitimacy of online searches, which was the first judicial authority to officially publish details on the proposed software. However, the court remained very vague and merely stated that "a specifically designed computer program would be passed on to the suspect for installation on his computer to allow authorities to access the data stored on its storage media".[186] It did not provide any details about the type of software and what its precise abilities are.

The North Rhine-Westphalian government, as described above in chapter 2, was the first legislative authority specifying in its amendment of Article 5.2(11) NRW-CPA the online search as an investigative method. However, the North Rhine-Westphalian government remained even less specific about the technical details of the described measure. It merely stated that the online search of a computer may be accomplished by "technical means".[187] The term "technical means" does not allow drawing conclusions about the specifics of these means, and whether this will be a software or hardware solution.

The situation is identical in the UK and other European countries, where no information has been released about the particulars of the software used to undertake remote searches. Equally on EU level, no technical details were released in the Council Conclusions about how the remote searches should be undertaken.

However, a fairly clear picture about the technical details of remote searches of ICT devices has evolved in the literature. The technical feasibility of these proposed technical details is, however, controversially discussed. An overview of these opinions is provided in this section, before evaluating in the following section (4.1.2) whether the discussed methods are technically grounded and feasible.

Böckenförde established that generally, thus also for law enforcement agencies, the way to gain access to the data stored on private computers varies.[188] It can be similar to

---

[185] BGH Beschluss, ibid.
[186] BGH, NJW 2007, 930.
[187] Article 5.2(11) NRW-CPA, available online at http://www.im.nrw.de/sch/doks/vs/vsg_nrw_2007.pdf.
[188] T Böckenförde, *Die Ermittlung im Netz* (2003, Tübingen: Mohr Siebeck) at 209.

predominantly malicious activities such as "hacking" and "cracking"[189], or by making use of channels specifically designed for accessing the data. According to Böckenförde, which method to choose depends on the type of target system.[190] He establishes that the most promising method to gain access to a private computer in its singularity,[191] is by infiltrating the specific system with a software specifically designed to spy on the data stored on the target machine, which he specifies to be *Trojan software*.[192]
Although, these conclusions were drawn for generic online investigations in general, and not the online search of an ICT device in particular, he has been among the first authors to specify the type of software required by law enforcement agencies to infiltrate computers of suspects. Authors reasoning about the technical feasibility of the online search picked up these findings and discussed them in the light of the recent developments.
Gercke was one of the first authors to embark on defining the technological details of the online search of computers. He states that remote access to suspects' computers is accomplished through the use of very specific software. He specifies further that this software is similar to hacking tools, particularly to Trojan software, thereby confirming the findings of Böckenförde with regards to the online search.[193] He states that this software can be either installed on the target computer through legitimate software updates that include, unknown to the suspect, the specific code, or through backdoors, which additionally also provide access to the ICT device as a whole and not only the data stored on it.[194]

---

[189] These terms are sometimes used interchangeably, without making a clear differentiation between them. The following definition of "Hacker" and "Cracker" serves to better distinguish between these terms. "A *hacker* is a person intensely interested in the arcane and recondite workings of any computer operating system. Most often, hackers are programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They may know of holes within systems and the reasons for such holes. Hackers constantly seek further knowledge, freely share what they have discovered, and never, ever intentionally damage data (Anonymous, *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network* [Canada: SAMS, 2002], p. 47)." "A *cracker* is a person who breaks into or otherwise violates the system integrity of remote machines, with malicious intent. Crackers, having gained unauthorized access, destroy vital data, deny legitimate users service, or basically cause problems for their targets. Crackers can easily be identified because their actions are malicious (*Ibid*)."
[190] Böckenförde, note 188, at 210.
[191] Thus a machine that is not part of a network and hence not designed to be accessed from outside.
[192] Böckenförde, note 188, at 211.
[193] M Gercke, "Telekommunikationsüberwachung" in F Roggan, M Kutscha (eds.) *Handbuch zum Recht der inneren Sicherheit* (Berlin: Berliner Wissenschafts-Verlag, 2006) 146-182, at 168.
[194] *Ibid*, at 169.

Many authors writing on the topic of online search, both from a legal and technical perspective confirmed these initial findings.[195]

However, this initial reasoning remained rather unspecific and no technical details about the software or its abilities were provided at this early stage. As stated above, this was in line with the information policy of the German government, which equally did not release any detailed information about the software and only confirmed that it was testing the technical feasibility of such a measure.[196] It did specify that an initial amount of € 200.000 would be required to design this tool in addition to the payment of two programmers, however, this information does not give an indication about the specifics of the technology.[197]

This initial general debate was followed by more in-depth studies about the type of software required and its abilities, and the general feasibility of an online search. These studies established that the software to be used for this measure would not be a completely novel product, but rather rely on existing malware tools and previous research undertaken in this field, and in particular research on Trojan software.[198] It was argued that this type of software already possesses attributes that make it ideal for use by law enforcement agencies to remotely search ICT devices of suspects. Particularly, because Trojan software is designed to operate hidden from the view of the user of the computer. Furthermore, because such software is able to receive commands through a hidden input port, collect data on the infiltrated system, and send this data back to the operators through a hidden output port.[199] Apart from ascertaining the type of technology most likely to be used, these studies also focus on

---

[195] See e.g. Leipold, note 48; Hornung, note 48; Kutscha, note 48; Rux, note 48; M Kemper, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten" (2007) 40:4 *Zeitschrift f*ür *Rechtspolitik,* 105-109, 105; P Schaar, "Anmerkung zum Beschluss des BGH vom 31.1.2007 - StB 18/06 - zur verdeckten Online-Durchsuchung", (2007) 10:4 *Kommunikation und Recht* 202-205, 202; K Cornelius, "Anmerkung zum Beschluss des BGH zur verdeckten Online-Durchsuchung", (2007) 62:15/16 *Juristenzeitung* 285-295, 286; Gercke, note 48, at 226.

[196] BT-Drucksache 16/4997, note 181, at 2.

[197] BT-Drucksache 16/3973, "Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Petra Pau, Kersten Naumann und der Fraktion DIE LINKE", 28.12.2006, p. 4, available online at http://dip21.bundestag.de/dip21/btd/16/039/1603973.pdf.

[198] U Buermeyer, note 48, at 154; Hansen/Pfitzmann, note 48, at 225; F C Freiling, "Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07", 29.09.2007, 1-7, at 4, available online at http://pi1.informatik.uni-mannheim.de/filepool/publications/stellungnahme-online-durchsuchung.pdf.

[199] Hansen/Pfitzmann, note 48, at 225.

the abilities of the software, specifying that the scope of abilities of this type of software can be potentially large.[200] According to these authors, these tools are able to:

- Undertake a system analysis of the target device, including gaining information about the installed operating system, programs and user accounts;
- Compile an overview of the directories; search these directories for certain file names and undertake full-text search for key words;
- Undertake a search of attached internal and external data storage devices (such as USB sticks, CDs/DVDs, flash-memory, external hard drives);
- Download specific documents (text, pictures);
- Use a key logger;
- Deactivate software;
- Log the user's Internet access;
- Log the user's passwords;
- Generate messages on the target computer (to influence the user behaviour);
- Scan the network;
- Generate and transmit screen shots;
- Monitor the ICT devices' surrroundings (by activating an in-built camera and/or microphone).[201]

It is important to remember that the software will not necessarily possess all of the above-described abilities, but could only possess some of them or even more, if programmed accordingly.

Having discussed the likely type of software to be used and its potential abilities, these studies further explore how the online search will be conducted. Here, the crucial (and technically most demanding)[202] phase is the infiltration of the target machine and installation of the software. Without the ability to infiltrate a specific system, an online search cannot be conducted, unless, as Hansen and Pfitzmann point out, the measure is

---

[200] Bundesministerium des Inneren, "Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien", 22.08.2007, available online at http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf; Bundesministerium des Inneren, "Fragenkatalog des Bundesministeriums der Justiz", 22.08.2007, available online at http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf; D Fox, Secorvo Security Consulting GmbH, "Stellungnahme zur ‚Online-Durchsuchung' Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07", 29.09.2007, 1-17, at 7, available online at http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf.

[201] This list is not necessarily complete. It only represents the abilities that have officially been named in the literature.

[202] Fox, note 200, at 6.

undertaken without infiltrating the ICT device.[203] This, however, significantly limits the extent and type of data that can be collected.

It is possible to analyse the electromagnetic radiation of the target system and thereby collecting information about optical signals, such as an image of the monitor, received (directly or indirectly through a window)[204] acoustical signals (every key on a keyboard makes a different noise when used),[205] and electromagnetic signals of the different components build into the IT systems (such as graphic cards, sound cards, keyboards and CPUs).[206] Despite the fact that these methods can be technically very advanced, the amount of data that can be accessed is limited (this dependents on the suspect's behaviour, e.g. the websites and files accessed, and passwords typed), and the authority gains no control over the ICT device. The advantage of this method is that the violation of privacy and data protection rights of the affected person can be smaller and the risk that a third person is affected can be eliminated faster, thus the measure could be more in line with existing legislation and therefore regarded to be proportionate and in accordance with the constitution (in countries that have one) or human rights (such as the UK 1998 *Human Rights Act*, *European Convention on Human Rights*). However, due to the above mentioned limitations it is unlikely that an online search will be undertaken without infiltrating the system. This is also confirmed by the above-mentioned statements by authorities, confirming the development of a piece of software to be used during an online search, which would not be necessary if there was no need to infiltrate an ICT device.

---

[203] M Hansen, A Pfitzmann, "Techniken der Online-Durchsuchung" in F Roggan (ed.), *Online-Durchsuchungen – Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008* (Berlin: Berliner Wissenschafts-Verlag, 2008) 131-157, 134.

[204] M G Kuhn, "Optical Time-Domain Eavesdropping Risks of CRT Displays" (2002) *Proceedings IEEE Symposium on Security and Privacy*, 3-18, 3; M Backes, M Dürmuth, D Unruh, "Compromising Reflections – or – How to Read LCD Monitors Around the Corner" (2008) *Proceedings IEEE Symposium on Security and Privacy*, 158-169.

[205] L Zhuang, "Security Inference from Noisy Data", (2008), Unpublished PhD thesis, University of California, Berkeley, available online at http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-32.pdf.

[206] M G Kuhn, R J Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations" in D Aucsmith (ed.), *Information Hiding* (Berlin, Heidelberg: Springer, 1998) 124-142; R J Anderson, M G Kuhn, "Soft Tempest – An Opportunity for NATO" (1999) *Protecting NATO Information Systems in the 21 Century, IST Symposium, Washington DC, USA, 25–27 Oct*, available online at http://www.cl.cam.ac.uk/~rja14/Papers/nato-tempest.pdf; M G Kuhn, "Electromagnetic Eavesdropping Risks of Flat-Panel Displays" (2004) *Workshop on Privacy Enhancing Technology, 26–28 May 2004, Toronto, Canada*, available online at http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf.

4.1.2 Infiltration Methods

The possible infiltration methods were briefly mentioned in chapter 2,[207] but the findings of the studies are depicted in more detail here. Generally, the tenor is that several potential approaches exist to infiltrate an ICT device with the above described software solutions.

One possible infiltration method concerns the physical accessing of the target computer and the manual installation of the investigative software.[208] This method provides a very high certainty that the software is installed successfully and on the specific ICT device of the suspect. However, it requires the physical intrusion of the private space of the suspect and the manual manipulation of the machine by the authorities. There might be no opportunity to do this and password protected machines can complicate the access. Furthermore, if the executing authority is located in a country other than the suspect physically accessing the space of the suspect might be impossible.[209] In addition the amount of required human labour is relatively high for this method, and therefore makes it expensive. This method can therefore be excluded as a likely means of infiltration.

The alternative options discussed do not require physical access to the ICT devices. These methods are similar to those developed for the infiltration of ICT devices with malware, and can be divided into two categories: a) those requiring the (unknowing) cooperation of the suspect, and b) those that do not rely on any actions of the suspect. In the first category, the infiltration and installation of the software is hidden in a different application ("host" application), which needs to be executed by the user of the computer, and will then install itself in the background (hidden from the view of the user). Such "host applications" can be:

- *Email attachments*: The relevant software can be hidden in the attachment of an email, which, once opened, is started and can install itself in the background. The enticement to open the attachment can be increased by making it look to be

---

[207] See p. 31.

[208] See e.g. Hansen/Pfitzmann, note 203, at 135; Hansen/Pfitzmann, note 48, at 227; Fox, note 44, at 6; U Sieber, "Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen", 09.10.2007, 1-24, at 12, available online at http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf; Freiling, note 198, at 4; Pohl, note 43, at 686.

[209] See chapter 6 for more details about the legal problems of cross-jurisdictional online searches.

sent from an authority, such as the tax office, and include important information in the attachment.

- *Software updates*: The software is included in a manipulated software update, which is forwarded to the suspect. The software update itself can be genuine, but include the particular code, which will again be installed in the background. The advantage is that the user might be prompted to install the software with administrator rights.
- *Manipulated Website*: A website (ideally one often visited by the suspect or one specifically designed for this purpose) is modified to include code, which will start an installation program once the target has accessed the site. The installation program will then be downloaded and install the software tool on the suspect's computer.
- *CD/DVD*: A manipulated CD or DVD, which is passed on to the suspect, includes the software, which is installed by an autorun function in the background when the CD/DVD is inserted.
- *USB stick*: A manipulated USB stick, which includes the software that is installed by an autorun function in the background.

In all of the above cases the software installs itself on the machine without the need for further supervision by an operator. Once the manipulated "host" has been prepared and distributed, the software will work autonomously.

The second category comprises techniques that do not require the cooperation of the suspect and are executed remotely by a human operator. This is the exploitation of so called backdoors, where authorities hack into the system of a suspect by exploiting security holes in the operating system, that are still relatively unknown and therefore still "open". A human operator then directly installs the software on the computer of the suspect. Alternatively, authorities could collaborate with software producers to have their own backdoors included into software. However, this would cause several problems, starting with the willingness of the software producers due to potential loss of consumer trust. Furthermore, there would be the very real risk that the backdoor would be detected by criminals and used for their own purpose.
Another possibility is to force Internet Service Providers (ISPs) to manipulate genuine software downloads of suspects to include the specific code. However, this would again

bear the risk of loss of consumer trust outlined above.[210] The German government has stated that it would not enact such an obligation to co-operate for private parties. This might also be the case because highly sensitive information (such as identification of suspects) would have to be disclosed to third parties, and could therefore be potentially exploited by internal employees of these companies.

The above-discussed infiltration methods have been discussed in the literature in great detail, but no single method has been identified as the most likely one to be used. Moreover, no feasibility study of the different approaches exists.
Hence concluding it can be summarised that even the more in-depth studies have failed to precisely identify the type of software to be used and determine its abilities and more importantly, the feasibility of the measure, which has even been doubted by some authors.[211]

However, one key conclusion can be drawn from the above analysis of existing literature, which is relevant for the following section, where the details about the software are analysed further. Consent exists that the investigative software is similar to existing malware, particularly Trojan horses and related software applications. As illustrated in chapter 3, the interviewed technical expert also confirmed this.[212] Furthermore, these studies have succeeded in identifying the desirable abilities of the software tool.

For the analysis of the legal challenges in the following chapters of this thesis, it is essential to understand the technological details of the proposed tool. Only with a detailed understanding of the technology is it possible to evaluate its current and future abilities, and thus the impact on police investigations and the legal framework regulating these activities. An analysis of the state-of-the-art of relevant malware,

---

[210] See also the interview results on this in chapter 3 at p. 70.
[211] J Schmidt, "Bundestrojaner: Geht was – was geht. Technische Optionen für die Online-Durchsuchung"(2007) *heise*, available online at http://www.heise.de/security/Bundestrojaner-Geht-was-was-geht--/artikel/86415; Fox, note 44; S Berlit, T Wegewitz, "Mythos „Bundestrojaner" - Auf dem Weg zur legalen Onlineüberwachung – ", (2008) *1. Workshop IT-Sicherheitsmanagement*, available online at http://wi.f4.htw-berlin.de/users/messer/LV/Globals/ISM-Workshops/Workshop-WS07/Mythos%20Bundestrojaner%200.pdf.
[212] See p. 71.

specifically Trojan software is undertaken in the next section, to classify and define the type of software and its current and future abilities for the purpose of this thesis.

4.2 Relevant Malware – A Classification

Before determining the abilities of the software tool to be used to remotely search an ICT device of a suspect, it is necessary to understand the underlying technology. What precisely is a software Trojan horse and to which class of software does it belong? In this section, the technology is introduced, its origins provided, and a classification into an existing class of software is undertaken. This classification also enables the application of existing research findings to this new software tool.

As established in the previous section, many authors who write about technology to be used to search ICT devices online, as well as the technical expert interviewed, state that such a tool shares crucial attributes with existing malware.[213] Thus in a first step, it needs to be established what precisely malware is.

Generally, the term malware stems from malicious software and describes intentionally dysfunctional software.[214] It is also referred to as software with a malicious intent,[215] or software that is developed for the purpose of doing harm to computers or via computers.[216] Furthermore, it is designed to circumvent security mechanisms in place to prevent such harm doing, by coercing the user to circumvent it, or exploiting vulnerabilities somewhere in the system to spread itself or act.[217] However, these are very broad definitions from which no categorisation about the abilities of this type of software can be drawn. The reason for this is that malware includes various types of software, which although ultimately all having the same aim of unauthorised accessing

---

[213] See e.g. G Hornung, C Schnabel, "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention" (2009) 25:2 *Computer Law & Security Review* 115-122; Hornung/Bendrath/Pfitzman, note 85.
[214] K Brunnstein, "From AntiVirus to AntiMalware Software and Beyond: Another Approach to the Protection of Customers from Dysfunctional System Behaviour" in *22nd National Information Systems Security Conference* (Virgina,USA, 1999); M Swimmer, "Malicious Software in Ubiquitous Computing" in M Petkovic, W Jonker (eds.) *Security, Privacy, and Trust in Modern Data Management* (Berlin Heidelberg: Springer, 2007) 451-466, 452.
[215] H Chen et al., "Back to the Future: A Framework for Automatic Malware Removal and System Repair", (2006) *Proceedings 22nd Computer Security Application Conference* 257-268, 257.
[216] The Linux Information Project, Definition of Malware, available online at http://www.linfo.org/malware.html.
[217] Swimmer, note 214, at 451.

computers with a malicious intent, can vary significantly in terms of abilities and characteristics. These different types, the most commonly known being viruses, worms and Trojans, were all designed with a different application in mind and have been developed and further enhanced since the early 1980s, when the first malicious piece of software in form of a virus appeared.[218] However, as shown above, the online search has very specific requirements for the investigative software to be successful. Hence referring to the domain malware as a whole can be misleading, as not all of the applications falling into this category fulfill all the necessary requirements. Computer viruses, for example, are primarily self-replicating programs that infect other programs by modifying them to include a copy of themselves.[219] Thus, this type of malware does not possess the abilities required for an online search of an ICT device, where the focus is on the searching and copying of data stored on the target device and the monitoring of communication.

The class of malware designed to be surreptitiously installed on a user's computer, and to monitor the user's behaviour and report this back to a third party is called spyware.[220] However, when searching for a definition of this term, it becomes clear that not one single widely accepted definition of spyware exists. Taking the term literally, spyware is ware that spies on you. The US Federal Trade Commission has defined spyware as "software that aids in gathering information about a person or organisation without their knowledge, which may send such information to another entity without the consumer's consent, or asserts control over a computer without the

---

[218] J Leyden, "Computer Virus turns 25", (2007) *The Register*, available online at http://www.theregister.co.uk/2007/07/13/virus_silver_jubilee/, who explains that the first malware ever released was a computer virus, which spread between Apple II computers via infected floppy disks, called Elk Cloner in 1982.

[219] M Karresand, "Seperating Trojan Horses, Viruses, and Worms – A Proposed Taxonomy of Software Weapons" (2003) *Proceedings of 2003 IEEE Workshop on Information Assurance*, 127-134, 127; F Cohen, "Computer Viruses – Theory and Experiments" (1987) 6:1 *Computer Security*, 22-35, 23.

[220] J C Sipior, B T Ward, "Trust, privacy, and legal protection in the use of software with surreptitiously installed operations: An empirical evaluation" (2008) 10:3 *Information Systems Frontiers*, 3-18, 3; E Doyle,"Not All Spyware is as Harmless as Cookies: Block it or Your Business Could Pay Dearly", (2003) *Computer Weekly*, available online at http://www.computerweekly.com/Articles/2003/11/26/198884/not-all-spyware-is-as-harmless-as-cookies.htm; T F Stafford, A Urbaczewski, "Spyware: The Ghost in the Machine" (2004) 14 *Communications of the Association for the Information Systems*, 291-306, 291.

consumer's knowledge".[221] Another definition is "any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet [...]. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers."[222] Furthermore, spyware is able to collect personal information stored or typed into a computer and can also install other spyware programs.[223] It can capture user's keystrokes and mouse clicks during web navigation and local computer use, and scan hard drives to obtain information from user's files and application programs such as email, word processors and games.[224] Spyware is essentially software that asserts control over a user's computer without the user's consent and knowledge.[225] Spyware usually arrives hidden in other software downloads without the knowledge of the user.[226]

All these definitions have two general concepts in common: 1) spyware is installed on a user's device without the user's consent and 2) spyware tracks the user behaviour online and transmits that information to unknown parties.[227]

These definitions and descriptions of the domain spyware show that its characteristics are very similar to the specifications and requirements developed for the online search software tool. Therefore, it can be concluded that this is the appropriate domain to derive information about characteristics and abilities of this class of software and apply these to the software underlying the online search. This, however, requires to further specify the precise type of spyware relevant for this analysis. The general domain of

---

[221] Federal Trade Commission, "Public workshop: monitoring software on your PC: spyware, adware, and other software" 2004, available online at: http://www.ftc.gov/bcp/workshops/spyware/extension.pdf .

[222] Webopedia, "Spyware" available online at http://www.webopedia.com/TERM/s/spyware.html.

[223] Sipior/Ward, note 220, at 4.

[224] R R Urbach, G A Kibel, "Adware/Spyware: An Update Regarding Pending Litigation and Legislation", (2004) 16:7 *Intellectual Property and Technology Law Journal*, 12-16, 12; Sipior/Ward, note 227, at 3.

[225] Stafford/Urbaczewski, note 220, at 292.

[226] Sipior/Ward, note 220, at 4.

[227] K McDowell, "Now That We Are All So Well-Educated about Spyware, Can We Put the Bad Guys out of Business?" (2006) *Proceedings of the 34th annual ACM SIGUCCS conference on User services*, 235 – 239, 236.

spyware includes the sub-categories adware,[228] key loggers,[229] and Trojan horses.[230] However, all these sub-categories were developed for different applications and thus feature different specific abilities. As already indicated by the literature review on the technical details of the online search,[231] and by the technical expert interviewed for this thesis,[232] Trojan horse software is a sub-category featuring the most relevant characteristics and abilities, and therefore a closer analysis of this class is performed in the next section, to gain a better understanding of its abilities and characteristics.

4.2.1 A Trojan Horse – A Conqueror of Troy?

As with spyware, there is no one single widely accepted definition of a software Trojan horse (Trojan). The term stems from the Trojan horse myth in Greek mythology.[233] Software Trojans have been around since the late 1980s. The first Trojan detected was the *PC-Write Trojan* in 1986.[234] Another famous example of this early generation is the Aids Information Disk Trojan, also referred to as *AIDS Trojan*.[235] These early Trojans

---

[228] Adware refers to software applications that reside on an individual's computer and are not related to, or authorized by, the underlying website that the user may be viewing at that time. These advertisements can take the form of pop-up or pop-under ads, web banners, redirected webpages, and spam email. Some adware may alter a homepage by hijacking a web browser, or add URLs to bookmarks, to persistently present a competitor's website or a look-alike site, disallowing the user web acces for his own purpose. Personal information such as financial data, passwords, and identification-tagged downloads can be transmitted, without the user's knowledge or consent to the adware author or a third party (Urbach/Kibel, note 224, at 12; Sipior/Ward, note 220, at 4).

[229] Keyloggers are programs that run silently in the background and record keystrokes and mouse clicks on a computer. The data can then be played back to reconstruct what a user did (T S Chan, "Spyware" in H Bidgoli (ed.) *Handbook of Information Security Volume 1* (Wiley: Hoboken, New Jersey, 2005) 136).

[230] Stafford/Urbaczewski, note 220, at 292.

[231] See p. 86.

[232] See p. 66.

[233] According to Greek mythology, the Greeks built a huge, wooden figure of a horse in which a select force of men hid. The Greeks pretended to sail away, and the Trojans pulled the Horse into their city as a victory trophy. That night the Greek force crept out of the Horse and opened the gates for the rest of the Greek army, which had sailed back under cover of night. The Greek army entered and destroyed the city, decisively ending the war (Wikipedia, "Trojan Horse" available online at http://en.wikipedia.org/wiki/Trojan_Horse).

[234] The PC-Write Trojan, appeared in 1986, pretending to be version 2.72 of the shareware word processor, PC-Write. (Quicksoft, the company that made PC-Write, did not release a version 2.72.) When a user launched what she believed to be PC-Write 2.72, she really started the PC-Write Trojan, which then performed two actions: one, it wiped out the FAT (file allocation table; system a PC uses to organize contents on the hard drive); and two, it formatted the hard drive, deleting all saved data (K Dickey, "Tales of Trojan Horses – Why You Should Beware of Those Bearing Gifts" 9:2 *Smart Computing* 12-16, 13).

[235] In late 1989, 20.000 floppy disks containing this trojan were mailed to addresses stolen from PC Business World and the World Health Organization, by a company called 'PC Cyborg'. The

had in common that they only possessed limited, pre-determined abilities and were distributed via traditional channels (such as posting the floppy disk containing the AIDS Trojan to the victim).

Initial definitions of Trojans were based on the state-of-the-art of this generation. One well-known definition is included in the now obsolete first draft of the Site Security Handbook RFC 1244:

> *"A Trojan Horse program can be a program that does something useful, or merely something interesting. It always does something unexpected, like steal passwords or copy files without your knowledge."*[236]

To the same generation of definitions also belongs the copybook definition given by most anti-virus vendors:

> *"A Trojan is a non-replicating program that appears to be legitimate but is designed to carry out some harmful action on the victim computer".*[237]

At this time, Trojans were relatively rare compared to viruses, because they could not spread as easily due to their lack of self-replicating abilities. As previously mentioned, their abilities were also still relatively restricted and the execution of their tasks dependent upon the behaviour of the user of the infected machine. For example in the AIDS example, in which the PC had to be booted 90 times before the Trojan executed the pre-determined task.

While the above definitions reflect these limitations, they do provide a good basic description of a software Trojan and some of the characteristics provided have remained true until today, which will become clear in the definitions of the next generation Trojans.

The emergence of the World Wide Web, making the spreading of Trojans considerably easier, facilitated the development of a new generation of Trojans. Good examples of

---

disks supposedly contained information about HIV. When the user ran the installation program, the Trojan wrote itself to the hard disk, created its own hidden files and directories and modified system files. After the PC had been booted 90 times, the trojan encrypted the contents of the hard disk, making the data inaccessible. The only accessible file remaining on the disk was a README file: this contained a bill and a PO Box address in Panama for payment (D Emm, "Focus on Trojans – holding data to ransom" (2006) 6 *Network Security*, 4-7, 4.).

[236] Site Security Policy Handbook Working Group, Site Security Policy Handbook RFC 1244, 1991, 50, available online at http://www.faqs.org/ftp/rfc/pdf/rfc1244.txt.pdf.

[237] Emm, note 235, at 4.

this generation are the Polyglot Trojan[238] in 1999 and the Cytron Trojan[239] in 2002. This new generation was not only making use of new distribution channels (such as emails) but was also more advanced in design. These Trojans did not rely any longer on actions of the user of the infiltrated computer to trigger the execution of their tasks, and were able to perform more complex tasks (such as in the case of Polyglot the scanning of specific data and the sending of this data to a designated email account) autonomously. Furthermore, the focus of these Trojans was not any longer on generally destroying or pampering with all data, but rather on the spying on selected data (whereby this selection was undertaken by the software itself).

Hence new definitions were developed to honor these facts and move away from the early concepts and attempts of classifying this technology.

Brunnstein defines this generation of Trojans as:

> *"A software or module that, in addition to its specified functions, has one or more additional hidden functions (called "Trojanic functions") that are added to a given module in a contamination process (trojanization) usually unobservable for a user. These hidden functions may activate depending upon specific (trigger) conditions".*[240]

Bontchev offer the following definition:

> *"A Trojan Horse is a program which performs (or claims to perform) something useful, while at the same time intentionally performs, unknowingly to the user, some kind of destructive function. This destructive function is usually called a payload."*[241]

---

[238] In 1999, many users received an email message that included a Y2Kcount.exe attachment and looked as if Microsoft sent it. Users believed double-clicking the attachment would launch a program that displayed a countdown to New Year's Day 2000. Instead, opening the file displayed an error message. Then, while users read the error message and tried to diagnose the "problem," a Trojan horse named Polyglot ran in the background, installing itself on the system and editing configuration files to monitor user Internet activity. Whenever Polyglot noted data transmission over the Internet, it would scan the data for passwords and other sensitive information and log the information into a TMP (temporary) file. Periodically, the Trojan horse sent this type of keystroke log to an email account, where a cracker could easily retrieve its contents (Dickey, note 233, at 13).

[239] In September 2002, antivirus software developers (and others) discovered the Cytron Trojan horse. A user receives an email message that claims the user can pick up an ecard from a friend by clicking a graphic of a hand holding an envelope. When the recipient clicks the graphic, a designated Web site loads in the browser window. Then, if the user accepts the Digital Certificate that appears on-screen, Cytron begins sending full-screen pop-up ads for pornographic Web sites to the user (Dickey, note 233, at 14).

[240] Brunnstein, note 214.

[241] V V Bontchev, *Methodology of Computer Anti-Virus Research* (University of Hamburg: Doctoral Thesis, 1998).

What these definitions show is that there is a reason why not one widely accepted definition of a Trojan but several exist. The new generations of Trojans, while sharing some characteristics, such as the non-replicative code and the masquerading as something useful, are more advanced and therefore feature more specific abilities and serve very specific purposes. These characteristics are difficult to generalise in one definition. Therefore, the existing definitions of Trojans are weak, because they are not specific enough to be applied to all types of Trojans and to enable the detection and classification of all the different types of Trojans. Thus, no working definition of a Trojan is developed for the purpose of this thesis, but rather existing Trojans are classified according to their specific abilities.

Today's Trojans have not significantly changed from the second generation of Trojans. They have, however, become more sophisticated in their specific tasks, and infiltration methods are now more reliable.

As Emm points out:

> *"Things have moved on considerably since the days when most 'copybook' Trojans were written. Far from appearing to be something benign, most Trojans don't appear at all […]. They install silently and the victim has no idea the Trojan is there".*[242]

The fact that Trojans have become invisible to the user of the targeted machine is important for the use of this software by law enforcement agencies. The objective is that the suspect should not under any circumstances detect the software used to undertake an online search

Some of the general abilities of today's Trojans are the starting and stopping of computer processes, stealing of information (for example passwords), and the opening of a backdoor that allows an outside attacker to control the compromised computer.[243] However, Trojans can have many faces and each one is purpose-built to carry out a specific function on the victim machine. Hence different sub-classes of Trojans have evolved and those relevant for the purpose of this thesis are depicted below.[244] What is relevant for this discussion is the awareness that all these sub-categories feature the above-mentioned general abilities and characteristics of a Trojan. They possess

---

[242] Emm, note 235, at 5.

[243] L A Hughes, G J DeLone, "Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both?" (2007) 25 *Social Sciences Computer Review*, 78-97, 81.

[244] For a full list of all sub-categories of Trojans see e.g. McDowell, note 227; Anonymous, note 189, at 360 ff.

additional specific features making them distinguishable from earlier generation Trojans.

4.2.1.1 Backdoor Trojans

Backdoor Trojans possess the additional feature of being able to also open a backdoor[245] to the target system. They are sometimes referred to as Remote Access Trojans (RAT).[246] This is the most widespread and also the most dangerous type of Trojan. Backdoor Trojans are so particularly dangerous because they have the potential to allow remote administration of the target system by the author or operator of the Trojan.[247] This means that they allow the operator (i.e. a hacker in the case of malicious Trojans, a police officer in the case of a government Trojan, like the software deployed during an online search) to pretend that he was sitting at the keyboard of the target machine. The capabilities of these Trojans can be extensive:

- Use the target system and Internet connection to send spam;
- Steal online and offline passwords of the user, credit card numbers, address details, phone numbers, and other information stored on the computer that could be used for identity theft, or other financial fraud;
- Log user activity, read email, view and download contents of documents, pictures, videos and other private data;
- Send, receive, execute and delete files;
- Use the computer and Internet connection, in conjunction with other computers to launch Distributed Denial of Service (DDoS) attacks;
- Modify system files, disable antivirus, delete files, change system settings, to cover tracks, or just to wreak havoc.[248]

---

[245] A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program or hardware device (Wikipedia, "Backdoor (computing)" available online at http://en.wikipedia.org/wiki/Backdoor_(computing)).

[246] These types of Trojans are sometimes classed into different sub-categories. However, since they are identical in their specific abilities it is not differentiate between them.

[247] Emm, note 235, at 6; M Sunner, "The Rise of the Targeted Trojans" (2007) 12 *Network Security* 4-7, at 6.

[248] Blair, "What is a Backdoor Trojan" (2007) *Geeks to Go*, available online at http://www.geekstogo.com/2007/10/03/what-is-a-backdoor-trojan/.

However, unlike legitimate remote administration utilities they install, launch and run invisibly, without the consent or knowledge of the user.[249]

4.2.1.2 Data-Sending Trojans

Data-sending Trojans are used to send data back to the hacker with information such as passwords, or confidential information such as credit card details, chat logs, address lists, etc.[250] The Trojan could look for specific information in particular locations or it could install a key-logger and simply send all recorded keystrokes to the hacker (who in turn can extract the passwords from that data).

Captured data can be sent back to the attacker's email address, which in most cases is located at some free web-based email provider for anonymity. Alternatively, captured data can be sent by connecting to a hacker's website - perhaps using a free web page provider - and submitting data via a web-form. Both methods would go unnoticed and can be done from any machine on any network with Internet and email access. Both internal and external hackers can use data-sending Trojans to gain access to confidential information about a company.[251]

4.2.1.3 Trojan Spies

Trojan spies are designed to track user activity and save the information to the user's hard disk and then forward it to the author or operator of the Trojan. The range of information collected by these Trojans includes:

- Keystrokes;
- Screenshots;
- Logs of active applications;
- Other user actions.[252]

4.2.1.4 Targeted Trojans

Targeted Trojans are a very recent development.[253] These Trojans aim at specific targets instead of randomly targeting a large number of victims, and are therefore

---

[249] Emm, note 235, at 6.
[250] GFI, "The corporate threat posed by email trojans" Whitepaper, available online at http://www.gfi.com/whitepapers/network-protection-against-trojans.pdf.
[251] Ibid.
[252] Emm, note 235, at 6.

harder to detect by antivirus protection measures. They are designed to collect information about data stored on the hard drive of the computer and, in particular, communication data, such as emails.

They are custom-written and one-offs, usually exploiting new or little-known security problems in popular applications, such as Microsoft Word, Excel or PowerPoint applications, masquerading as business emails. These document types are more likely not to be stripped out by a virus scanner and therefore reach the target more often.[254] Furthermore, custom-written, one-off Trojans are more likely to circumvent traditional anti-virus programs. This is the case because traditional anti-virus programs rely on DNA-like 'signatures' extracted from live viruses to prevent future attacks. In other words, virus researchers wait for a widespread attack to happen before they can find the antidote and distribute it.[255] Hence, as McDowell puts it, "the intent is to write malware that bypasses basic defenses and appeals to the personal interests of users to induce them to open documents or click on links that load malicious code".[256]

On June 26 2007, MessageLabs[257] intercepted 514 targeted Trojan attacks using an email with a Microsoft Word document attached, which contained embedded executable code.[258] Among those (successfully) targeted by this type of Trojans were leading companies in Israel.[259] The remarkable point of this case is that the attacks only came to light when one of the targets found passages of a book he had written online, despite the fact that these passages had only ever been stored on his PC.[260] This shows how difficult it is for antivirus software to detect this type of Trojan and how successfully these are being deployed. The 514 Trojans detected by MessageLabs were thus only a small fraction of those actually in use.

The analysis of the different sub-categories of Trojans has shown that this technology is very advanced and technically robust. It features the abilities that are required for the

---

[253] McDowell, note 227, at 237.

[254] Messagelabs, "Targeted Trojans: A New Online Threat to Businesses", Whitepaper, available online at http://whitepapers.theregister.co.uk/paper/view/330/eav-whitepaper-targetedtrojans-a4.pdf.

[255] Ibid; J Evers, "The future of malware: Trojan horses" (2006) *CNETnews.com*, available online at http://www.zdnetasia.com/news/security/0,39044215,61960021,00.htm.

[256] McDowell, note 227, at 238.

[257] http://www.messagelabs.com/

[258] Sunner, note 247, at 5.

[259] J E Dunn, "Israeli Police Uncover Massive, Trojan Horse-Based Industrial Spy Ring", (2005) *Techworld.com*, available online at http://www.pcworld.com/article/121081/israeli_police_uncover_massive_trojan_horsebased_industrial_spy_ring.html.

[260] Ibid.

software deployed during online searches of ICT devices, and is therefore the most likely source for information about the tool. More importantly, the above analysis has shown that technology capable of the tasks required during an online search already exists. Furthermore, this technology is already "successfully" used, which highlights that the online search software, featuring similar characteristics, will be able to perform the same tasks, such as infiltrating an ICT device of a suspect and search and copy the data stored on it, and then send it back to the operator.
As presented in more detail in chapter 3,[261] the interviewed technical expert confirmed the above findings, stating that such software is able to do anything that other, already existing software does. Furthermore, he confirmed that the software would be able to circumvent installed protection measures, such as antivirus software and firewalls, because already existing malware is able to do precisely this.[262] He also confirmed that the online search software is able to conduct the search autonomously and without direct intervention or supervision of the operator or designer.

Hence, it can be concluded that the software required to undertake an online search shares crucial attributes with existing spyware, and particularly backdoor, spy, and targeted Trojans.

4.3 Trojans – A Program or a Warrior?

The above analysis of spyware and particularly Trojans has shown that these software tools are executing complex tasks without direct intervention or supervision by the operator or designer. During an online search of an ICT device, this degree of autonomy results in the software tool carrying out tasks that a human officer would do during a normal search of a premise. For example, searching the data on the computer and selecting the information relevant for the investigation, and monitoring communication traffic for important information. This fact leads to the question whether a software Trojan is comparable to any other program, such as Microsoft Word, and can thus be classified as such, or whether it needs to be classified as a different entity.

---

[261] See p. 105.
[262] See Oxford Dictionaries, "Botnet", http://oxforddictionaries.com/definition/english/botnet.

Generally, computer programs can be defined as sequences of instructions for the computer.[263] Furthermore, every piece of software can be regarded as a mere process, that is pieces of code with data and states.[264]

These definitions seem well suited for simple word processing programs, such as Microsoft Word, which translate the keystrokes of users into machine-readable code. Here, the emphasis is on the fact that these types of software rely on input from a human user (directly, for example, in case of a word processing program, indirectly in case of the underlying operating system) and are depended on commands to function. This understanding of software is predominant, and applies to most of the commercial software products available. However, when examining the example of a word processing program closer, it seems doubtful that all programs and their additional functions can be subsumed under these definitions and notions.

A spell checker, for example, is an application that flags words, which have been mistyped by the user and offers correctly spelled alternatives.[265] Hence, this program fulfils a function without any direct input from the user. Such a program works by comparing every written word against those found in an implemented dictionary. If it cannot find a word, it will flag it and suggest similar alternatives. Here users provide input, namely the misspelled word to trigger the functioning of the application. Furthermore, it is the user making the decision whether the word is indeed misspelled, and if any of the suggestions the program provides are correct and fit the purpose. Therefore, an application such as a spell checker still falls into the notion of a program, as provided above.

However, these definitions appear inadequate when thinking of a piece of software, such as a Trojan. As described in the last paragraph, these applications can function autonomously and execute highly complex tasks. While operating systems, for example, also perform complex computing tasks, the difference is that a Trojan operates in an unfamiliar environment and solves tasks and makes decisions beyond the control of the designer and operator. This is of particular relevance if these software tools are used to investigate crimes and collect evidence.

---

[263] R M Stair, G W Reynolds, *Principles of Information Systems* (Course Technology Press: Boston, 2009), 134.

[264] F Brazier et al., "Are Law-Abiding Agents Realistic?" (2002) *Proceedings of the workshop on the Law of Electronic Agents (LEA02)*, 151-155, 152.

[265] Oxford Dictionaries, "Spell Checker" http://oxforddictionaries.com/definition/english/spellchecker?q=Spell+Checker.

Hence the existing notion of a program seems to be less appropriate for this type of application. However, if this is the case the questions arise how these applications can be classified and what this means for their use by law enforcement agencies.

The obvious question arising is whether the increase in autonomy and intelligence transforms them into some type of "persona".[266]
There have been debates on the legal status of software tools in the past; however, these have mainly focused on the question whether software tools can be regarded as persons in the civil law sense, that is, whether a software tool is capable of entering into legal transactions and is liable for its activities.[267] This debate arose due to the frequent use of autonomous agent software for e-commerce applications.[268] The common concern was whether existing civil law concepts were adequate to deal with this use. The main focus was on the question whether software tools can enter into contractual negotiations, and if such contracts, solely concluded by software tools without any human supervision are valid and binding. The problem debated here was in particular the contractual requirement of a "meeting of the minds" and in how far software tools can fulfil this. This debate has now reached a considerable maturity and it has been shown that the above problems can all sufficiently be addressed by the notion of agency and its associated liability regimes.[269]

However, when such software tools are used by law enforcement agencies and are replacing human officers for certain tasks, the question of legal status becomes an important issue again. Contrary to contractual transactions, where the concept of agenthood offered a suitable solution to the problem of legal status of intelligent software tools, a police officer cannot defer his duties and rights to another person.[270]

---

[266] S Franklin, A Grasser, "Is it an agent, or just a program? A taxonomy for autonomous agents" in J Miller, M Wooldridge, N Jennings (eds) *Intelligent Agents III: Agent Theories, Architectures, and Languages* (Springer Verlag, Berlin: 1997), 21 – 35.
[267] See e.g. E Weitzenböck, "Electronic Agents and the Formation of Contracts" (2001) 9:3 *International Journal of Law and Information Technology*, 204-234; E Weitzenböck, "Good faith and fair dealing in contracts formed and performed by electronic agents" (2004) 12:1-2 *Artifical Intelligence and Law*, 83-110; S Wettig, E Zehedner, "The electronic agent: a legal personality under German law?" in A Oskamp, E Weitzenbök *The Law and Electronic Agents (LEA 2003)* (Unipub, Oslo: 2003) 97-113; J Bing, G Sartor (eds) *The Law of Electronic Agents* (Oslo: Norwegian Research Center for Computers and Law, 2003).
[268] See below section 4.4, p.108 for a detailed analysis of this technology.
[269] C Sorge, "Conclusion of contracts by electronic agents" (2005) *Proceedings of the 10th international conference on Artificial intelligence and law*, 210-214, 211.
[270] B Schafer, "The taming of the Sleuth—problems and potential of autonomous agents in crime

Thus while the question of classification of intelligent software could be avoided for the civil law setting, it remains an important issue for the use by law enforcement agencies.

During investigations, law enforcement officers often have rights that are not available to the normal citizen, such as the right to search the premises of a suspect. Furthermore, they have duties, which do not apply to ordinary citizens, such as the duty to investigate a crime. These rights and duties must be executed in accordance with existing legislation, best practice guidelines and codes of practice. Furthermore, some of these rights and duties may be formulated in an intentionalistic language, using terms such as "reasonable suspicion". These terms not only refer to a relevant state of mind of the investigating officer, they also use vague concepts such as "reasonable" that cannot be straightforwardly implemented in programming code.[271] However, these concepts and regulations also apply to investigative acts undertaken by, or with the help of the software tool and need to be obeyed. Otherwise, the privacy rights of citizens could be at scrutiny or the evidence collected inadmissible in court.

Thus from the above analysis it can be concluded that when and if a software tool executes some of these rights and duties, its role goes beyond that of a computer program, which can be regarded as a mere tool assisting an officer in his work, and hence its status during investigations needs to be clarified. Therefore, the software tool deployed during an online search is not a mere program, but rather an autonomous "cyber-cop". This finding particularly affects the reasoning about the legal consequences of this technology deployed during investigations. Chapters 6 and 7 explore how this impacts investigations and the evidence collected by these tools.[272]

4.4 Software Agents

As mentioned in the previous section (4.3), the discussion about the legal status of intelligent software has predominantly focused on software agents, also referred to as electronic or autonomous agents. This is equally a technology capable of acting autonomously and without direct intervention by a human operator. Furthermore, law enforcement and administrative authorities are already deploying this technology to

---

investigation and prosecution" (2006) 20:1 *International Review of Law, Computers & Technology*, 63-76, 65.

[271] Ibid, at 66.

[272] See also Schafer, note 270, for a more detailed discussion of the question of classification.

assist them with their duties and to perform previously impossible investigations. This means that it is very likely that this technology significantly influences the development of the investigative tool used for online searches, and generally the new class of software-based investigative tools.
For this reason, this technology is introduced in more depth in this section.

4.4.1 What Is A Software Agent? The Definition Disaster

There does neither exist a single, widely accepted definition of what an autonomous agent is, nor a set of attributes agreed upon for autonomous agents.[273] In fact, even several terms referring to this technology now exist, ranging from the generic *autonomous agents*, *software agents*, *electronic agents* and *intelligent agents*, to the more specific *interface agents*.[274]
However, the lack of a universally accepted definition is now generally recognised, and it is common practice for researchers in this area to develop their own definitions. Thus in a first step, some of these definitions are examined here. This leads to a better understanding of this technology and also explains why no universally accepted definition of this technology exists.
An autonomous agent has been defined as a "persistent software entity dedicated to a specific purpose".[275] *Persistent* is used here to distinguish it from subroutines and highlight that agents have their own ideas about how to accomplish tasks and their own agendas. *Special purpose* differentiates it from entire multifunction applications, highlighting that agents are typically much smaller. Another attempt at defining autonomous agents is "computer programs that simulate a human relationship by doing something that another person could do for you".[276] This definition focuses on the traditional notion of agency existing between biological agents. It is very broad and seems to suggest that a software agent is capable of replacing humans and engaging in a relationship with a human. The choice of the term *relationship* suggests that a software agent possesses the relevant states of mind necessary for this. In biological

---

[273] S Nwana, "Software Agents: An Overview" (1996) 11:3 *Knowledge Engineering Review*, 1-40, 2.
[274] M d'Inverno, M Luck, *Understanding Agent Systems* (Berlin: Springer, 2004), 3.
[275] D C Smith, A Cypher, J Spohrer, "Programming agents without a programming language" (1994) 37:7 *Communications of the ACM*, 55-67, 60.
[276] T Selker, "Coach: A Teaching Agent that Learns" (1994) 37:7 *Communications of the ACM*, 92-99, 92.

agents, these states of mind are a result of needs, desires and urges that evolve over generations; in artificial agents these drives have to be built in by its programmers.[277] As opposed to this definition, Riecken defines an agent much more loosely as an "integrated reasoning process".[278] This definition is very general and does not focus on the notion of agency at all.

Others take agents to be "anything that can be viewed as perceiving its environment through sensors and acting upon that environment through actuators".[279] This definition contributes to the idea that artificial agents require an environment to act and need to be capable of understanding this environment and reacting to it appropriately. However, this definition relies on the understanding of *environment* and the definition of *perceiving* and *acting*. As it is, this definition is very broad and without defining these terms in more detail, this definition could apply to almost every existing program or application. Maes has attempted to provide more details about this by defining agents as "computational systems that inhabit some complex, dynamic environment, sense and act autonomously in this environment, and by doing so realize a set of goals and tasks for which they are designed."[280] This definition clarifies that agents should be capable of acting autonomously. Furthermore, Maes restricts environments to being complex and dynamic, thereby excluding simpler processes and applications.

Franklin and Graesser take an agent as "a system situated within and a part of an environment that senses that environment and acts on it, over time, in pursuit of its agenda and so as to effect what it senses in the future".[281] Here, the ability of foreseeing the results of one's actions is incorporated into the notion of artificial agency.

This richness in definitions and their divergence stems from the fact that there is a wide range of applications for which artificial agents are designed. These range from operating systems interfaces,[282] electronic commerce,[283] air-traffic control,[284] business

---

[277] Schafer, note 270, at 65.

[278] D Riecken, "An architecture of integrated agents" (1994) 37:7 *Communications of the ACM*, 107-116, 107.

[279] S Russel, P Norvig, *Artificial Inteligence: A Modern Approach* (Prentice Hall: New Jersey: 2003) 32.

[280] P Maes, "Artificial Life Meets Entertainment: Life like Autonomous Agents" (1995) 38:11 *Communications of the ACM*, 108-114, 108.

[281] Franklin/Graesser, note 266, at 25.

[282] O Etzioni et al., "The Softbot Approach to OS Interfaces," (1995) 12:4 *IEEE Software*, 42-51.

[283] Guttman et al., "Agent-mediated electronic commerce: a survey" (1998) 13:2 *Knowledge Engineering Review*, 147-159.

process management,[285] to engineering applications.[286] Thus, the focus of these different streams of research varies significantly and hence the agent ability requirements, and therefore the focus of the definitions differ as well. The lack of consensus about the meaning of the term autonomous agent is therefore not surprising.[287] However, this leads to the problem that the term *software agent* becomes almost meaningless, unless one refers to a particular concept of agent.

To solve this problem, several authors have undertaken a different approach at specifying the term software agents. Instead of attempting to formulate a definition of this technology, they focus on characterising agents along certain dimensions, and thus determine what constitutes agency.

4.4.2 The Characteristics of a Software Agent

The previous section has established, that the difficulty of agreeing on one definition of the term *software agent* stems primarily from the fact that people tend to have a different understanding of this technology, due to the variety of application areas and their different backgrounds. Therefore, the term *software agent* can best be seen as an umbrella term for programs that to some extent display attributes commonly associated with agency.[288] In this section, it is analysed in more detail, which attributes are associated with software agents and are essential to establish a basic type of agency. The assumption is that this approach is more application neutral and therefore applicable to the whole class of software agents instead of a specific sub-class, only. Furthermore, this will provide a better understanding of this technology and establish minimum abilities that constitute the notion of agency.

According to Gilbert, agency is the degree of autonomy and authority vested in a software agent.[289] In others words, in order to meet their design objectives agents must

---

[284] D Kinny, M Georgeff, A Rao, "A methodology and modeling technique for systems of BDI agents" in Y Demazeau, J-P Müller, M Tambe (eds.) *Agents Breaking Away: Proceedings of the Seventh Eurpean Workshop on Modelling Autonomous Agents in a Multi-Agent World, LNAI 1038* (Berlin: Springer, 1996), 56-71.

[285] N R Jennings et al., "Agent-based business process management" (1996) 5:2&3 *International Journal of Cooperative Information Systems*, 105-130.

[286] Q Hao, W Shen, Z Zhang, "An autonomous agent development environment for engineering applications" (2005) 19:2 *Advanced Engineering Informatics*, 123-134.

[287] d'Inverno/Luck, note 274, at 3.

[288] Nwana, note 273, at 27.

[289] D Gilbert et al., "IBM Intelligent Agent Strategy", (1995) White Paper, IBM Corporation.

be able to operate without the direct intervention of humans and should be in control of their own actions and internal state.[290]

Although opinions differ as to what an accurate description of a software agent is, it is possible to discern some common features from existing definitions that apply to all types of software agents, and thus assist in determining what agency is. Classifying these attributes as belonging to a weak and strong notion of agency is now a universally accepted approach, which was first coined by Wooldridge and Jennings in their now seminal survey of the agent field.[291]

According to these findings, a weak notion of agency can be attributed to software possessing the following attributes:[292]

- *autonomy:* agents operate without the direct intervention of humans or others, and possesse some degree of control over their actions and internal states;
- *social ability*: agents interact with other agents and possibly humans via a shared communication language;
- r*eactivity*: allowing agents to perceive and respond to a changing environment;
- p*ro-activity*: allowing agents to demonstrate goal-directed activity by taking the initiative.

These characteristics are to some extend broadly accepted by many as representative of the key qualities that can be used to assess "agentness".[293]

The stronger notion of agency incorporates all of the above-introduced abilities but is additionally associated with a higher level of intelligence. The stronger notion of agency is represented in the ability to reason using mentalistic notions such as knowledge, belief, desire, intention, and obligation.[294] The authors established in a later paper that the characteristics of the weak notion establish the essence of agenthood, hence are the minimum criteria an application must possess to be classified as an agent.[295]

---

[290] N R Jennings, M Wooldridge, *Agent Technology, Foundations, Applications and Markets* (Berlin: Springer, 1998), 4.

[291] M Wooldridge, N R Jennings, "Intelligent Agents: Theory and Practice" (1995) 10:2 *The Knowledge Engineering Review*, 115-152.

[292] Ibid, at 119.

[293] d'Inverno/Luck, note 274, at 4.

[294] Wooldridge/Jennings, note 291, at 120.

[295] N R Jennings, K Sycara, M Wooldridge, "A roadmap of agent research and development" (1998), 1:1 *Autonomous Agents and Multi-Agent Systems* 275-306, 277.

Similarly, Etzioni and Weld define desirable agent characteristics as including *autonomy*, which they further characterise as requiring that agents are *goal-oriented* and thus accept high-level requests, *collaborative* in that they can modify these requests and clarify them, *flexible* in not having scripted actions, and *self-starting* in that they can sense changes to their environment and decide when to take actions. Furthermore, *temporal continuity,* by which an agent is not simply a "one-shot" computation, *character* in that an agent has a believable personality and emotional state, *communication ability* with other agents or people, *adaptability* to user preferences based on previous experiences, and *mobility* which allows an agent to be transported across different machines and architectures.[296]
Franklin and Graesser have also determined a number of properties they regard as essential to establish agenthood. These are *reactivity,* which means that the agent responds in a timely fashion to changes in the environment, *autonomy* in that the agent is able to exercise control over its own actions, *goal-orientation* and thus the capability of acting purposefully and not merely acting in response to the environment, and *temporal continuity,* thus the agent is a continuously running process.[297] Furthermore, they have defined a number of variable properties, which can complement the core properties, thereby creating useful classes of agents, such as mobile, learning agents. These properties are *communicative,* thus the ability to communicate with other agents and people, *learning* in that an agent changes its behaviour based on its previous experience, *mobile* and hence capable of moving between machines, *flexible,* which means that the actions of an agent are not prescribed, and *character*, thus the possession of a believable personality and emotional state.[298]

From the analysis of these different attempts to determine the characteristics of agency, it becomes clear that there is no central common denominator. Hence, the problem of a lack of consensus established in section 4.3.1 about the terminology *agent* and what establishes agency continues here. However, opposed to the problems with defining the term agent, this approach has proven to be more successful in that it has established that a certain degree of similarity exists between the different attempts to determine the characteristics of agency.

---

[296] O Etzioni, D S Weld, "Intelligent agents on the internet: Fact, fiction and forecast", (1995) 12:4 *IEEE Expert* 41-51, 43.
[297] Franklin/Graesser, note 266, at 27.
[298] Ibid.

Autonomy, reactivity, the ability to communicate and *goal-orientation* are common denominators of the different approaches. Thus, while a universally accepted notion of agency does not exist, these common denominators, along with the other characteristics provided by the above-illustrated approaches, provide a better understanding of what a software agent is capable of. It becomes clear that this technology is highly advanced and able to execute complex tasks without the supervision of a human controller. Comparing this technology to Trojan software, it becomes clear that these technologies share crucial attributes, namely the degree of autonomy and intelligence in executing tasks, as well as the ability to move around different platforms.

To summarise, there is a distinct lack of precision and concensus about the notion of agency. However, the above analysis of attempts to determine the essence of agency has led to a better understanding of the technical specifics of software agents.

4.4.3 Multi-Agent Systems

The previous sections of this chapter on Trojan software and software agents have depicted the unique features of these technologies, and in particular the ability to act autonomously without direct supervision of an (human) operator.

However, the above discussion has thus far focused on the use of single entities of these technologies. Hence, the results and consequences of the acts of these entities were eventually analysed by human operators.

However, the distinct abilities of software agents to act autonomously, react to a given environment and communicate with other entities have prompted research into the design of multi-agent systems. Precisely because of these abilities, software agents in a specific environment are affected by the acts of other agents (software or human) working in the same environment.

Due to these reasons a multi-agent system can be regarded as a set of agents that interact together to coordinate their behavior and often cooperate to achieve some

collective goal.[299] Typically, multi-agent systems are distributed systems in which several distinct components, each of which is an independent problem-solving agent come together to form some coherent whole.[300] Thus these agents are cooperating to combine their efforts to accomplish as a group what the single entity cannot, or in the case of competition several agents try to achieve what only some of them can.[301] Importantly, there is not usually a pre-established architecture or configuration incorporating the agents, and the interactions between them are not pre-defined, as is usually the case with traditional processes in concurrent programs. More significantly, there is no global system goal; the agents are heterogeneous with their own goals and capabilities.[302]

Thus multi-agents systems provide several advantages over single-entity systems. They are more efficient because a system with multiple agents allows for parallel and asynchronous computation. In a multi-agent system, tasks can be broken down into several independent tasks and computed simultaneously by different agents.[303] Furthermore, these systems are more robust than single-entity systems. Multi-agent systems can have built-in redundancy. If the responsibility for certain tasks is shared among different agents, the system can tolerate failures from individual agents.[304] On the contrary, when a single-entity system fails, the whole program or application fails. Moreover, multi-agent systems are more scalable and flexible than single-entity systems. They can operate effectively without any limits to their size, thus new agents can be added or old one's removed without affecting the performance of the system.[305] Furthermore, they can cope with a growing application domain by increasing the nubmer of agents, each agent's capabilities, the computational resources available to

---

[299] J Ferber, O Gutknecht, F Michel, "From Agents to Organizations: an Organizational View of Multi-Agent Systems" in P Giorgini, J Müller, J Odell (eds.) *Agent-Oriented Software Engineering (AOSE) IV* (LNCS 2935, 2004) 214-230, 214.

[300] d'Inverno/Luck, note 274, at 6.

[301] G Weiss (ed), *Multiagent systems: a modern approach to distributed artificial intelligence* (MIT Press: Cambridge, MA, 1999) 1.

[302] d'Inverno/Luck, note 274, at 6.

[303] N Vlassis, *A Concise Introduction to Multiagent Systems and Distributed Artificial* (Morgan & Claypool: San Rafael, CA, 2007) 3.

[304] S Parsons, M Klein, "Towards robust multi-agent systems: Handling communication exceptions in double auctions" (2004) *Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multiagent Systems*, 1482-1489, 1482.

[305] P Marrow, "Scalability in Multi-Agent Systems: The DIET Project" (2001) *Agents'01 Workshop on Infrastructure and Scalability for Agents*, ACM Press, New York, available online at www.cs.cf.ac.uk/User/O.F.Rana/agents2001/ papers/18_howden.pdf.

each agent, or the infrastructure needed by the agents to make them more productive.[306] Lastly, multi-agent systems are capable of producing emergent behaviour. By letting multiple (reactive) agents interact within an agent system, "smartness" can arise out of the emergent behaviour of the interactions of the various modules.[307]

The above analysis of multi-agent systems highlights that these systems posses unique capabilities. These systems operate with a much higher degree of autonomy and the actions of the whole system, or a single entity within such a system are even less predictable than those of single-entities, such as Trojan software or software agents. Due to the advantages and capabilities depicted above, these systems are also potentially capable of undertaking much more complex tasks than single-entities. Just in the same way as humans can often achieve better results when working in groups, as opposed to working alone.

However, the increase in autonomy and intelligence of multi-agent systems gives rise to conceptual and legal problems, particularly when used by law enforcement agencies and secret services. The above discussion (section 4.2) on the status and classification of autonomously and intelligently operating software entities becomes even more relevant for multi-agent systems, where the human influence on the actions of these entities is minimal.

When analysing the software agent domain, the logical question arising is in how far the above described abilities, both of single-agent and multi-agent systems have already or will in the future be realistically implemented into systems. In any high-technology domain, the systems deployed in commercial and industrial settings often tend to embody research findings somewhat behind the leading edge of academic research. It is therefore important to gain a clear understanding of the current and future state of the art of agent research when attempting to assess the impact of this technology on law enforcement and police work. Luck et al. have created an *Agent Roadmap*, which provides an overview of the current and future abilities of software

[306] M N Huhns, "Agent Societies: Magnitude and Duration" (2002) *IEEE Internet Computing* 2-4, 3.
[307] Nwana, note 273, at 27.

agent systems.[308] The Agentlink Roadmap distinguishes four broad phases of current and future development. These phases have been updated and adapted to the technical progress by Schermer, and this updated and more relevant version is depicted here.[309]

a. Phase I: Closed agent systems (2005-2008)

The first phase of software agents and multi-agent systems can best be characterised as *closed*. This breed of agent systems is usually employed within a single (corporate) environment with participating agents sharing common high-level goals within this domain.[310] Usually the software agents used in closed agent systems cannot be considered intelligent. This is not only due to the limitations of agent technology during this phase but was also an issue of trust: people did not feel comfortable with the idea of intelligent, autonomous software applications.[311]

b. Phase II: Cross-boundary systems (2008-2012)

In the second phase of the agent-technology development, systems are increasingly designed to operate on multi-platforms (as opposed to the closed systems of the first pahse), though typically it is still a single design team that develops an agent system. While agents in this phase might have fewer goals in common they still operate within a single domain and share common domain knowledge.[312] Standardisation of communication and interaction protocols such as defined by the FIPA (Foundation for Intelligent Physical Agents) is becoming evermore important.[313]

c. Phase III: Open systems (2012-2015)

---

[308] M Luck, P McBurney, P Preist, "Agent Technology: Enabling Next Generation Computing. A Roadmap for Agent-Based Computing" (2003) AgentLink II, IST-1999-29003, available online at http://eprints.ecs.soton.ac.uk/7309/.
[309] B W Schermer, *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance* (Leiden University Press: Leiden, 2007), 30.
[310] Luck/McBurney/Preist, see note 308, at 34.
[311] B W Schermer, M Durinck, L Bijmans, *Juridische Aspecten van Autonome Systemen* (Leidenschendam: ECP.NL, 2005).
[312] Luck/McBurney/Preist, see note 308, at 34.
[313] Schermer, see note 309, at 31.

In the third phase more multi-platform systems will emerge. These systems will allow multiple heterogeneous agents from different design teams to operate on the same agent platform, provided the agents adhere to the publicly stated requirements and standards of the agent platform.[314]

d. Phase IV: Fully scalable systems (2015 and beyond)

The final phase of software-agent development will see fully scalable systems capable of supporting almost limitless amounts of agents. It is likely that in this phase agents will be highly mobile, pro-active, and capable of learning new skills on the entry of a system. The agents will thus be more intelligent and capable of performing more difficult tasks. It is to be expected that over time people will have grown to be accustomed to the use of intelligent, autonomous agents and will no longer have fears when it comes to employing agent technology.[315]
This roadmap highlights that current deployment of software agents and multi-agent systems has already reached a considerable maturity. It depicts that current systems are mostly closed, meaning that they are only applied in specific environments and do not interact with other agent systems yet. However, reaching the next phases over the coming years, the development will be away from these closed systems towards more open and scalable multi-agent systems that allow agents to travel from one agent system to another and learn new skills on the way.

Hence this roadmap shows that agent technology is already deployed in commercial settings but is currently mainly limited to the use of single-agents or multi-agent systems in specifically designed environments. However, it also highlights that deployment of more advanced agent systems will happen in the foreseeable future. In any case, the currently used single- and multi-agent systems should not be underestimated. To show what current software agents are capable of and how these are being used, one example of how law enforcement and administrative agencies are deploying software agent technology is provided in the next section.

---

[314] Luck/McBurney/Preist, see note 308, at 35.
[315] Schermer, see note 309, at 31.

4.5 Current Use of Software Agents

COPLINK[316] is a good example of how an agent-enabled data-mining application can make law enforcement more efficient and effective. COPLINK is a system used by law enforcement agencies in the United States to aid in criminal investigations. The COPLINK system was developed to provide a solution to the lack of integration in law enforcement information systems. COPLINK software organises and analyses vast quantities of structured and seemingly unrelated data, housed in various incompatible databases and record management systems, over an intranet-based platform.[317] COPLINK integrates different data sources and facilitates subject-based inquiries. Apart from integrating disparate databases COPLINK uses a collaboration and notification tool called 'Active Agent'. This component of the COPLINK system is a tool that can be set to watch for new data meeting user-specified parameters and then automatically notify the user(s) when such data is migrated into COPLINK.[318] The COPLINK Active Agent thus automates the task of running repetitive or periodic database queries. The Active Agent also allows an investigator to collaborate with others who are conducting similar queries. If collaboration is set as active, the agent notifies other investigators running similar queries. This can quickly bring together incidents involving the same suspect or other database objects that are under investigation by different investigators, or by different jurisdictions.

4.6 Conclusion

This chapter has identified the technical foundations of the software-based investigative tools that are being developed for online searches of ICT devices. The analysis has yielded that the technology is similar in nature to existing malware, and more specifically Trojan software. The interview statements of the experts on the topic were crucial factors for this analysis, given that governments and law enforcement have released little information on the topic. This highlights again the importance of the empirical research part for this work.

However, these software-based investigative tools, while featuring similarities, will not be identical with existing malware products. Particularly, as the empirical research has

---

316 http://www.coplink.net .
317 Knowledge Computing Corporation, (2004) *The COPLINK Whitepaper*, 2004/3.
318 Ibid.

revealed,[319] there is a tendency towards in-house designed investigative tools. The above analysis has shown that these new investigative tools will likely be a combination of several related technologies and in particular autonomous agent software will also influence their design.

The important result of the analysis is that existing software products can already operate autonomously, without direct intervention by a human operator. Their actions are goal-oriented and they are capable of reacting to changing conditions.

These software tools are therefore capable of executing the actions required for an online search of ICT devices, and able to replace human officers for investigative tasks.

Hence, these new investigative technologies cannot be classed as mere software tools but rather are emerging as autonomously operating "cyber-cops" for the new cyber-policing system.

This illustrates why the existing legal framework is unable to cope with this new form of policing, and highlights why a new approach is required to regulate these cyber-cops.

[319] See p. 69.

5 MOBILE, INTELLIGENT AND AUTONOMOUS POLICING TOOLS

The previous chapter (4) has focused on the case study and specified the precise type of technology developed to undertake online searches of ICT devices. It has established that software-based investigative tools deployed for online searches share crucial attributes with existing malware, and particularly with Trojans, and autonomous agent software. The analysis of these technologies has revealed that these new investigative tools are capable of operating autonomously during cyber-investigations, and – crucially - the online search of ICT devices is technically feasible.

Moving away from the current ex-ante authorisation of new software-based investigative tools, however, requires a different approach. Instead of focusing on one specific tool and developing one specific regulatory method for this, a broader and therefore more future-proof approach is needed.

The purpose of this chapter is to identify a new wider class of software-based investigative tools – the new generation of cyber-cops. Focusing on a whole class instead of one specific technology means that deeper conceptual legal problems can be identified and a future-proof and technology-neutral regulatory approach developed. This is essential to establish legal certainty for both, the operators of these new tools and those affected by the investigations. This also ensures that the findings of this thesis can be applied to a whole class of new investigative tools, including future tools, and are therefore of wider significance.

In a first step, this chapter examines the general problems of technology regulation in section 5.1. Section 5.2 sets out the foundations for the new class of software-based investigative tools by identifying the origins of the relevant technologies and common denominators. This is followed by a brief introduction to the source domain of the relevant technologies in section 5.3. Based on these findings, a new class of investigative technologies is developed in section 5.4. Section 5.5 concludes with a summary of the main findings.

5.1 Problems of Technology Regulation

Most of the existing work on the use of autonomous agent software, Trojan software and similar technologies has exclusively focused on one specific technology.[320] While this provides the opportunity to discuss and analyse the legal and technical challenges of one specific technology in detail, this approach is of limited use to policy makers and legislators aiming to draft future-proof legislation and develop sustainable regulatory approaches for new investigative technologies. However, it mirrors the currently predominant ex-ante regulatory system of new technologies, which tends to focus on either granting authority to use specific new tools, or preventing their use. Hence, what is lacking is a more systematic analysis of related technologies to examine whether a new class of investigative technologies can be identified.

This is important, as Koops has pointed out, because technology-specific regulation is only acceptable if there is a significant difference between technologies.[321] Not only is this a sensible approach to avoid discrimination, but also does it aid to guarantee the sustainability of the law. A general principle of law making is that the law should be sustainable.[322] While it has been pointed out by many authors, and is now a generally accepted principle, that ICTs develop at a much faster rate than the law,[323] this process should be countered by drafting laws as technology neutral as possible. If a law is too technology-specific, it is not likely to cover future technological developments, and it will therefore have to be adapted sooner rather than later.[324]

One prominent example of a law that was insufficient to deal with technological changes and therefore had to be adapted soon after it had been enacted is the *1998 EC*

---

[320] See e.g. Schermer, note 309; M Bond, G Danezis, "A pact with the Devil" (2006) Technical Report 666, *University of Cambridge*, available online at http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-666.pdf; Weitzenböck, note 267.

[321] B J Koops, "Should ICT Regulation Be Technology-Neutral" in B J Koops, M Lips, C Priens, M Schellekens (eds.) *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, IT&Law Series Vol. 9, (The Hague, T.C.M. Asser Press: 2006), 77-108, 84.

[322] Ibid, at 86.

[323] See e.g. A H Easterbrook, "Cyberspace and the Law of the Horse" (1996) 207 *University of Chicago Legal Forum*, 209; T Dreier, "Law and Information Technology – An Uneasy Marriage, Or Getting Along With Each Other?" (2005) 14:3 *Information & Communications Technology Law*, 207-216; R v Fellows; R v Arnold [1997] 1 Cr App R 244; [1997] 2 All E.R. 548 illustrates that technology develops and progresses faster than the law can keep up with it.

[324] J L Koger, "You Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace As Primary Legislator Of Electronic Signatures" (2001) 11 *Transnational Law and Contemporary Problems*, 491-516, 507.

Telecommunications Framework.[325] This law had been drafted largely with the telephone in mind and covered the development of electronic communications insufficiently, hence was updated by the new *2003 e-Communications Framework*.[326]

The above arguments have been developed in the debate about technology-neutrality of legislation, which has continued to be a pervasive concept in the field of ICT regulation influencing among others debates on convergence with broadcasting, voice over IP, universal service, spectrum allocation and net neutrality.[327] The relevance and effectiveness of this concept, however, has also been critically discussed. Reed points out that one disadvantage of technology neutral legislation is that it cannot be very specific about the subject matter that it regulates, which can produce the undesirable consequence that the law, or its application in practice, is insufficiently clear.[328] An example for this is the *Regulation of the Interception of Traffic Data* in the UK,[329] which is an attempt of drafting technology neutral legislation that has resulted in regulation whose meaning is so vague that its application to the technology is often a matter of guesswork.[330]

Thus the quintessence is that legislation regulating new technologies should be applied to whole classes of related technologies, instead of one specific technology, only. This should guarantee that the balancing act between creating legislation that is general enough to be sustainable as well as future proof, and at the same time specific enough to provide sufficient legal certainty, which is one primary requirement of regulation in general,[331] is achieved.

---

[325] See http://ec.europa.eu/information_society/topics/telecoms/regulatory/98_regpack/text_en.htm.
[326] See http://ec.europa.eu/information_society/topics/telecoms/regulatory/new_rf/text_en.htm.
[327] Reed, note 91, at 264.
[328] Ibid, 280.
[329] A Escudero-Pascual, I Hosein, "The Hazards of Technology-Neutral Policy: Questioning Lawful Access to Traffic Data" (2004) 47 *Communications of the ACM* 77-82.
[330] In the House of Lords debate on the *UK Regulation of Investigatory Powers Bill 2000*, the Earl of Northesk was provoked to remark: "One of the many difficulties I have with the Bill is that, in its strident efforts to be technology neutral, it often conveys the impression that either it is ignorant of the way in which current technology operates, or pretends that there is no technology at all." Hansard, House of Lords 28th June, 2000 (Committee Stage), Column 1012.
[331] Koops, note 321, at 96.

This means for the purpose of this work that it needs to be determined in how far the technologies introduced in the previous chapter can be grouped into one, more general class. This will not only make this work more relevant for future regulatory matters, but the results can also be applied to a wider array of current and future technologies. Moreover, it will be easier to answer the research questions developed in chapter 1.2 for a group of technologies instead of developing answers for specific technologies, which might be enhanced and developed further soon after this work has been finished.

5.2 The Common Denominators

As mentioned at the beginning of this chapter, work on autonomous agent technology and software Trojans has to date, to the best knowledge of the author, exclusively focused on problems relating to one of these technologies. Thus no attempt has been made to investigate whether these (and other current or future) technologies can be grouped into one more general class.

This thesis attempts to develop such a group of related technologies in the remainder of this chapter. The methodology for doing so is to determine whether these technologies have common denominators, which allow them to be classed together into one group. This approach is similar to the successful and established approach of defining these technologies (in their singularity) illustrated in the previous chapter.[332] The focus for determining these common denominators is on characteristics that constitute the core of these technologies and, in addition, are crucial for their tasks as cyber-cops, while at the same time pose significant challenges and problems for the law, and in particular the legal framework regulating police investigations.

The previous chapter has already depicted that Trojan software and autonomous agent software are similar in design. However, it has focused on the analysis of their respective capabilities and characteristics. This analysis has shown that both technologies are used for data collection and monitoring purposes by law enforcement agencies and other governmental authorities. While this alone does not necessarily suggest that these technologies are related, it is evidence that this is the case. Thus the question is whether these technologies feature shared characteristics and capabilities,

[332] See p. 111.

which can define them in their singularity, as well as serving as key criteria of a whole class of technologies.

One of the key findings of the last chapter was that for neither of the technologies a universally agreed upon definition exists.[333] The generally accepted approach is to characterise these technologies along certain dimensions. The last chapter has discussed and analysed these dimensions in great detail and therefore serves as a base for this chapter.

The key attributes of Trojan software identified in the previous chapter were the ability to *sense the environment* and *react to this* when selecting a target computer and searching the data on this machine, *autonomously make decisions* concerning the selection of relevant data, and *travel between platforms* when targeting a computer to install itself on this machine. The key attributes of autonomous agent software identified in the previous chapter are *autonomy*, *reactivity*, the *ability to communicate* and *goal-orientation*.[334]
These key attributes indicate a similarity between these technologies. They refer to similar, if not identical abilities – such as the shared ability to communicate with their environment and reacting to this, including to changes thereof. In addition, the key abilities enable these technologies to execute similar actions.
Therefore, these technologies share crucial features, and thus appear to be related. However, the above-depicted attributes are too specific to be used as key criteria for a whole class of technologies. It is thus necessary to define more general concepts, under which these attributes can be subsumed.

When defining such concepts it is not only necessary to look at the specifics of each technology, but also to take into account their specific usage. Chapter 2 introduced the main case study of this thesis, where the specific use of the Trojan-like software tool is explained. Additionally, chapter 4 discussed a short example of the use of autonomous agent software by authorities. These examples have highlighted that the current and future use of these software tools differs from the traditional use of software. As Wooldridge explains it "traditionally, every action a piece of software does must be

[333] See chapter 3 sections 4.2.1 and 4.4.1.
[334] See chapter 4 sections 4.2.1 and 4.4 respectively for details.

explicitly anticipated, planned for, and coded by a programmer. If a piece of software ever encounters a situation that its designer did not anticipate, then the result is not usually pretty, a system crash at best, multiple loss of life at worst."[335] This is the case because traditionally software has not been very good at knowing what to do. The underlying concept of software is to create obedient and unimaginative slaves, who solely act on commands of the user. Section 4.3 has already elaborated how this traditional concept clashes with current technological progress. The main case study, as well as the example provided in chapter 4, have highlighted that the capabilities of Trojan software and autonomous agent software go beyond what has traditionally been associated with software. These tools are designed to make decisions for themselves. Their specific use during investigations requires these technologies to act without direct intervention of an operator and communicate with other software entities and humans. Thus these tools need to be able to act autonomously, hence possess a certain degree of intelligence, and move between platforms.

Therefore, the relevant key concepts defining these technologies could be *mobility*, *intelligence* and *autonomy*. This would be the case if - at least - all the above-mentioned key abilities of these technologies and the demands of the application domain can be subsumed under these concepts. Whether this is the case is determined by analysing the meaning of these concepts in more detail in the following sections.

When analysing these key concepts it is important to bear in mind that these concepts are used in a variety of disciplines. For example, human police officers are also mobile (e.g. are required to move within the boundaries of their designated operational area), act autonomously (e.g. need to make decisions independently) and show intelligence (e.g. need to apply legal concepts to new situations) as key characteristics of their profession. At first glance, this presumed similarity appears to indicate a resemblance between human officers investigating the offline world, and cyber-cops investigating the virtual living space. However, even if both human and artificial officers have the same defining characteristics in common, these do not necessarily refer to identical meanings and definitions of the terms (which in turn could pose a problem for the law).

---

[335] M Wooldridge, "Intelligent Agents: The Key Concepts" (2001) Vol. 2322 *Lecture Notes in Computer Science, Proceedings of the 9th ECCAI-ACAI/EASSS*, 3-43.

Depending on the source discipline, their meaning can therefore differ significantly, thus it is important to determine the relevant common discipline before defining these concepts further.

Traditionally, both, software agents and Trojan software have their roots in the field of artificial intelligence (AI). Hence, AI is the applicable discipline for the definition of the terms. It is important to understand the basic ideas and concepts of this field of research before further defining the key concepts.

5.3 Artificial Intelligence

AI is a relatively recently emerged field of research, which has been influenced by a variety of disciplines, for example computer sciences, philosophy and psychology. The arrival of modern computer technology prompted organised research in this area.

Kurzweil has defined AI as

> *"The art of creating machines that perform functions that require intelligence when performed by people."*[336]

Thus, AI research often aims at recreating mental capabilities of humans in machines. The *Turing Test* by Alan Turing can be regarded as the first approach to measure intelligence in machines.[337] Turing was the first researcher to pose the question whether machines (i.e., computers) can think.[338] However, he felt that to be able to actually answer this question would be too difficult due to problems with defining the term *thinking*. Turing avoided the philosophical debate on how to define *thinking* by substituting the original question with a test (an imitation game) that can be used to determine subjectively whether a machine is intelligent.[339] In the imitation game (now known as the Turing test), an interrogator has typewritten conversations with two actors he cannot see, one human, the other a machine. If after a set period of time the interrogator is unable to distinguish between man and machine on the basis of the conversation, the machine can be considered to be intelligent. Since Turing's seminal

---

[336] R Kurzweil, *The age of intelligent machines* (MIT Press, Cambridge, MA: 1990).
[337] A Turing, "Computing Machinery and Intelligence" (1950) 236 *Mind*, 433-460.
[338] Ibid, at 433.
[339] Ibid.

work in 1950, much progress has been made in areas such as theorem proving, game playing, and decision making.[340] While it has generally been doubted whether a computer passing the Turing test could really be considered intelligent,[341] software capable of passing the test has yet to be developed. The strong AI envisaged by Turing has proven to be more difficult to develop than he anticipated. Until this day, Turing's test remains relevant in so far as it incorporates most of the research streams that form AI. A computer would need the following abilities to pass the Turing test:[342]

- Natural language processing, to enable it to communicate successfully in English;
- Knowledge representation to store what it knows or hears;
- Automated reasoning to use the stored knowledge to answer questions and to draw new conclusions;
- Machine learning to adapt to new circumstances and to detect and extrapolate patterns;
- Computer vision to perceive objects and,
- Robotics to manipulate objects and move around.

Generally, two main research streams that constitute the AI research field exist, the *strong* and *weak* AI concepts. Searle has provided an adequate description of these in his work: [343]

> *"According to weak AI, the principal value of the computer in the study of the mind is that it gives us a very powerful tool. For example, it enables us to formulate and test hypotheses in a more rigorous and precise fashion. But according to strong AI, the computer is not merely a tool in the study of the mind; rather, the appropriately programmed computer really is a mind, in the sense that computers given the right programs can be literally said to understand and have other cognitive states. In strong AI, because the programmed computer has cognitive states, the programs are not mere tools that enable us to test psychological explanations; rather, the programs are themselves the explanations."*

The Turing test belongs to the field of strong AI, attempting to model human intelligence needed for a conversation. The inability to design software capable of

[340] K A Delic, U Dayal, "AI Re-Emerging as Research in Complex Systems" (2006) 7:38 *Ubiquity*.
[341] Russel/Norvig, note 279, at 947 ff.
[342] Russel/Norvig, note 279, at 2.
[343] J R Searle, "Minds Brains, and Programs" (1980) 3 *The Behavioral and Brain Science*, 417.

modeling the human intelligence required for the Turing test is rooted in the underlying concept of *strong* AI: *symbolic* AI. Symbolic AI is the branch of AI research that attempts to represent knowledge in a declarative form (i.e., symbols and rules).[344] The foundation upon which the symbolic AI paradigm rests is the *physical-symbol system hypothesis*, formulated by Newell and Simon, who state that symbols lie at the root of intelligent actions.[345]

A physical symbol system takes a set of physical patterns (symbols), combining these to form structures (expressions), and manipulating these using processes that operate on those symbols according to symbolically coded sets of instructions to produce new expressions.[346] Thus, a symbol is a mental representation of a real-world object (for example, a table, a door, or a horse) that is made up of patterns of active and inactive neurons.

In a computer, these patterns of active and inactive neurons can be substituted by sequences of zeroes and ones. Hence, according to Newell and Simon, machines can be endowed with intelligence when knowledge is being represented in the form of symbols, which these machines can understand.

However, in order for a computer to display intelligent behaviour it needs to have an internal symbolic representation of the world as a basis for its actions.[347]

Symbolic AI can be seen as a top-down approach to AI in view of the fact that the entire state of the world needs to be completely and explicitly represented.[348] While the symbolic AI approach has yielded impressive results in specialised areas where the environment can be accurately modelled, it falls short when the size and complexity of an environment increases. The reason for this is, as Luck et al. explain, that it is difficult, if not impossible, to represent a dynamic and complex environment -or even an abstraction thereof- comprehensively. This also goes for the representation of some symbolic manipulation tasks such as planning.[349] Therefore the symbolic AI approach

---

[344] Schermer, note 309, at 18.

[345] A Newell, H A Simon, "Computer Sciences as Empirical Inquiry: Symbols and Search" (1976) 19:3 *Communications of the ACM*, 113-126, 114.

[346] Wooldridge/Jennings, note 290, at 139.

[347] M Luck, R Ashri , M D'Inverno, *Agent-based Software Development* (Norwoord: ArtechHouse Inc., 2004), 14.

[348] R A Brooks, "Intelligence Without Representation" (1991) 47 *Artificial Intelligence*, 139-159, 140.

[349] Luck/Ashri/D'Inverno, note 347, at 14.

does generally not fare well within complex, real-world environments. However, the ability to deal effectively with the environment is a prerequisite for strong AI.

A new approach to AI was needed to overcome the fundamental problems symbolic AI faced. Therefore, opposed to the (somewhat flawed) notion of strong AI and the symbolic paradigm, the so-called *connectionist* paradigm was developed. This paradigm addresses the problems and dissatisfactions of the symbolic paradigm, particularly the inability to handle flexible and robust processing in an efficient manner.

The connectionist paradigm refers to a class of models that compute by way of connections among simple processing units.[350] Thus, by establishing networks of simple, and often uniform units, which mirror mental phenomena. They are large networks of extremely simple processors, massively interconnected and running in parallel.[351] Bechtel states that the understanding of how the human brain works inspired the development of this model.[352] He elaborates further that the units, like neurons, are at any given time activated to some degree. Typically, activation means that these units are electrically charged. These units are connected to other units so that, depending on their own activation, they can act to increase or decrease the activations of these other units.[353]

The most commonly known connectionist models are neural networks. A neural network consists of a large number of units joined together in a pattern of connections. Units in a net are usually segregated into three classes: input units, which receive information to be processed, output units where the results of the processing are found, and units in between called hidden units. If a neural net were to model the whole human nervous system, the input units would be analogous to the sensory neurons, the output units to the motor neurons, and the hidden units to all other neurons.[354]

---

[350] J L McClelland, "Connectionist Models and Psychological Evidence" (1988) 27 *Journal of Memory and Language*, 107-123, 108.
[351] P Smolensky, "Connectionist AI, Symbolic AI, and the Brain" (1987) 1:2 *Artificial Intelligence Review*, 95-109, 95.
[352] W Bechtel, "Connectionism and The Philosophy of the Mind: An Overview" (1987) *The Southern Journal of Philosophy*, Supplement, 17-41, 17.
[353] Bechtel, ibid, at 18.
[354] J Garson, "Connectionism" (2007) *Stanford Encyclopedia of Philosophy*, available online at: http://plato.stanford.edu/entries/connectionism/.

Connectionism systems have been inspired by biological neural networks and seem to be closer in form to biological processes. They are based on two general ideas: a) that intelligent, rational behaviour is seen as innately linked to the environment an agent occupies, and b) that intelligent behaviour emerges from the interaction of various simpler behaviours.[355]

As opposed to symbolic systems, connectionism systems are capable of dealing with incomplete, approximate and inconsistent information as well as generalisation, and are therefore believed to be a step in the direction toward capturing the intrinsic properties of the biological substrate of intelligence.[356] Brooks has argued that higher-level intelligence need not be programmed directly into a machine from the top down, but can emerge from the interaction of multiple simple modules situated within a real environment.[357] Thus through the interaction of individually limited nodes complex behaviour can emerge.

The connectionism approach has a clear advantage over the symbolic approach in that it is more flexible and adaptable. The exact details of the use (such as the exact topic and course of the conversation in a Turing test) do not need to be known in advance. Furthermore, due to the distribution of tasks,[358] these systems are more robust towards external influences and unexpected changes. These days, most of the AI research is undertaken in weak AI, applying the connectionism approach. This is particularly the case for agent-based applications and similar software, such as the Trojan-like software tool in the case study.

The purpose of this rather rudimentary description of what AI is and how AI systems are being designed is to gain a basic understanding of this domain. This is highly relevant for the analysis of the key terms in the following sections of this chapter.

---

[355] M Wooldridge, *An Introduction to Multi-agent Systems* (West Sussex: John Wiley & Sons Ltd, 2002), 89.

[356] R Sun, "Artificial Intelligence: Connectionist versus Symbolic Approaches" in N J Smelser, P B Baltes (eds.), *International Encyclopedia of the Social and Behavioral Sciences* (Pergamon/Elsevier, Oxford: 2001), 783-789, 787.

[357] R A Brooks, "How to build complete creatures rather than isolated cognitive simulators", in K VanLehn (ed) *Architectures for Intelligence* (Hillsdale, NJ: Lawrence Erlbaum Assosiates, 1991), 225-239.

[358] The distribution of tasks is a recurring notion in this thesis. It has first been described in chapter 4.4.3 when introducing multi-agent systems.

5.4 Mobile, Intelligent and Autonomous Policing Tools

As discussed above, it is relevant and necessary to develop a more general class of software-based investigative technologies. This group is defined according to shared key denominators identified based on the key characteristics of the relevant technologies. These have been identified above as potentially being *mobility*, *intelligence* and *autonomy*. These concepts could serve as the key pillars of this new class of technologies, if the relevant characteristics of the technologies can be subsumed under these concepts. Hence, in the following sections the meaning of these three concepts is analysed.

The analysis is undertaken in the context of the source domain of the relevant technologies: AI. Thus the understanding of these terms for the purpose of this work is significantly influenced by the understanding of these terms developed in the AI domain.

5.4.1 Mobility

Generally, the term mobility refers to the state of being in motion. However, as stated in the previous section, of relevance is the meaning of this term in AI and in relation to the use of AI tools by police and law enforcement agencies as depicted in chapters 2 and 4. This section therefore analyses the meaning of *mobility* in AI and determines whether this concept sufficiently incorporates some of the characteristics of the technologies defined in chapter 4, and summarised in section 5.1 of this chapter, and is thus adequate to serve as one of the key concepts for the new class of investigative technologies. This section also establishes if and how this particular concept of mobility creates problems for the law regulating police investigations and the gathering of evidence.

The rise of the commercial Internet and its many applications has led to a wealth of information that is freely available, and the transformation, and partly reinvention, of communication. Berners-Lee has stated that the main reason for designing the Internet was to create a "universe of network accessible information".[359] However, the idea of the Internet is also very much based on the mobility of this information and communication data, as well as on the distribution of computing powers and the remote connection of users with systems. The Internet itself is a rather simple

[359] T Berners-Lee, "The World Wide Web – Past, Present and Future" (1997) 1:1 *Journal of Digital Information*, available online at: https://journals.tdl.org/jodi/article/viewArticle/3/3.

application that primarily serves the purpose to transport digital information from one computer to the other. Thus the Internet can be regarded as a distributed environment.[360]

Prior to the emergence of the commercialised Internet, the term *distributed system* or *environment* was mainly used to describe a network of several computer systems with separated memory that are connected to each other by a dedicated network.[361] The computers in such networks are almost always homogeneous, which means that they have the same type of processor and operating system. Furthermore, the network is more or less static: Computers are only rarely switched off; network connections between hosts are always reliable and provide a constant bandwidth.[362] These systems are based on the client and server paradigm, where computers in a network that offer services to others are called servers, and computers that request and enjoy these services are called clients.[363] The concept of *mobility* in AI has its roots in these distributed systems. Connections between different computers or nodes are necessary for the transportation of data. However, as opposed to the pre-internet networks, the Internet as a "network of networks" mainly consists of heterogeneous computers.[364] This means that data transfer and information exchange is much more difficult, and less reliable and robust than in a network of homogeneous computers. However, the widespread client-server infrastructure was not adequate to deal with these requirements. Hence, new technologies were developed to cope with these problems. These technologies fundamentally influenced the concept of mobility in AI as it exists today. Hence, to fully understand the current concept of mobility it is necessary to analyse these technologies in more detail.

5.4.1.1 Process Migration

Process migration[365] is one of the earliest technologies that shaped the concept of mobility, as it exists today. It introduced the idea of load balancing between computers in one network.

---

[360] C Reed, *Internet Law: Texts and Materials* (Cambridge, Cambridge University Press: 2004), 7.
[361] P Braun, W Rossak, *Mobile Agents: Basic Concepts, Mobility Models, and the Tracy Toolkit* (Morgan Kaufman Publishers Inc., San Francisco, CA: 2004), 3.
[362] Braun/Rossak, ibid.
[363] See e.g. JJ Labrosse, et al., *Embedded Software* (Oxford: Elsevier, 2008) 293.
[364] Braun/Rossak, note 361, at 3.
[365] A process in computing can be defined as an instance of a computer program, consisting of one or more threads, that is being sequentially executed (i.e., a list of instructions indexed by a

Process migration can be defined as "*the transfer of a sufficient amount of a process's state from one machine to another for the process to execute on the target machine*."[366] In addition to load balancing, process migration allows for small processes to be migrated to the site of very large data files, and also offers improved reliability. If it is known that a particular machine will shortly be unavailable, active processes may be migrated so as to continue execution elsewhere.[367] This technology requires a network for a process to be able to migrate from one machine to another machine to continue its execution there. Powell and Miller specify further that these networks are part of a distributed (loosely coupled) system.[368] A loosely coupled system is one in which the same copy of a process state cannot directly be executed by both processors. Rather, a copy of the state must be moved to a processor before it can run the process.[369] Process migration is normally an involuntary operation that may be initiated without the knowledge of the running process or any processes interacting with it. Ideally, all processes continue execution with no apparent changes in their computation or communications. Process migration provides the ability to stop a process, transport its state to another processor, and restart the process, transparently.[370] However, while process migration allows an entire process to be transferred to a remote host, this mechanism does not allow an easy way to return data back to the source node without the entire process returning as well.[371] Moreover, it takes up huge amounts of bandwidth and due to inherent complexity, it is hard to introduce process migration without impacting the stability and robustness of the underlying operating system.[372] Thus mobility in process migration technology refers to the movement of a process from one machine in a loosely coupled system to another. The degree of mobility is therefore rather limited and pre-defined, and the flexibility of this procedure is very low since the whole process needs to be shifted. Thus it is impossible to transfer specific data, only. The aim

---

process-specific program-counter [G D Knott, "A proposal for certain process management and intercommunication primitives" (1974) 8:4 *ACM SIGOPS Operating Systems Review*, 7-44, 8.])

[366] J M Smith, "A Survey of Process Migration Mechanisms" (1988) 22:3 *ACM SIGOPS Operating Systems Review*, 28-40, 28.

[367] M Nuttall, "A brief survey of systems providing process or object migration facilities" (1994) 28:4 *ACM SIGOPS Operating Systems Review*, 64-80, 64.

[368] M Powell, B Miller, "Process Migration in DEMOS/MO" (1983) *Proceedings of the Ninth ACM Symposium on Operating Systems Principles* (ACM/SIGOPS: New York), 110-119, 110.

[369] Powell/Miller, ibid.

[370] Powell/Miller, ibid, at 111.

[371] D Wong, N Paciorek, D Moore, "Java-based Mobile Agents" (1999) 42:3 *Communications of the ACM*, 92-101, 92.

[372] D S Milojicic, W LaForge, D Chauhan, "Mobile Objects and Agents (MOA)" (1998) *Distributed Systems Engineering Journal*, 179-194, 185.

of this technology is to balance load between machines in one network. However, the credentials of this network and machines connected to it are previously known, thus this technology is not well suited for heterogeneous networks.

5.4.1.2 Remote Evaluation

Remote evaluation programming is another technology that facilitates the movement of data and code between different machines in a network, and has equally shaped the notion of mobility, as it exists today.

Remote evaluation can be defined as the ability to evaluate a program expression at a remote computer.[373] A computer supporting remote evaluation exports a set of procedures by making them available to other computers. A remote evaluation request occurs when one computer, which can be called the client, sends a program expression to another computer, which can be called the server. The server evaluates the program expression and returns the results (if any) to the client. The server's interface specifies the set of procedures it exports.[374] Thus, the remote computer receiving the request executes the program referenced in the request within its own local address space before returning the results to the sending computer.[375]

Remote evaluation systems are an improvement to process migration systems insofar as the remote programming can occur without having to transfer the process control data from the source to the destination host. This means that these processes are not taking up as much bandwidth as process migration systems. Furthermore, it is possible to transfer data back to the source machine much more easily. However, despite these advantages remote evaluation systems lack the ability to encapsulate more state information into the executable program at the remote host.

Thus mobility in remote evaluation refers to the movement of an operation (e.g. a procedure plus parameters) to a remote side (where it is performed entirely), and the movement of the results of this operation to the source. While the speed of the transmission has improved, the choice of the data to be moved is still pre-determined, thus the flexibility has not increased. The aim of this technology is to reduce the amount of communication within a network that is required to accomplish a given task.

---

[373] J Stamos, D Gifford, "Remote evaluation" (1990) 12:4 *ACM Transactions on Programming Languages and Systems*, 537-565, 538.
[374] Stamos/Gifford, ibid, 538.
[375] Wong/Paciorek/Moore, note 371, at 92.

5.4.1.3 Mobile Objects

Mobile object systems (based on formal object-oriented programming techniques) extended the remote evaluation by capturing more program behaviour within the mobile object.[376] A mobile object system architecture is composed of four components: (a) the host—a computer and operating system, (b) the computational environment (CE)—the run-time system, (c) mobile object systems—the computations currently running on the CE, and (d) a network or communication subsystem that interconnects CEs located on different hosts.[377]

The underlying idea of mobile objects is to create active messages, that is, messages that are able to migrate to a remote host.[378] The unit of distribution and mobility in such systems is the object. Although some objects contain processes, others contain only data: arrays, records, and single integers are all objects. [379] Thus, the unit of mobility can be much smaller than in process migration and remote evaluation systems, and therefore further reduce network traffic. Object mobility subsumes both process migration and data transfer.
However, the data portion is still dominant in this concept, whereas the active portion (i.e. the code) is more or less an add-on.[380] This means that the notion of mobility in mobile object systems is similar to the one in process migration and remote evaluation systems. It refers to the transportation of data to another specific machine in a network. The advancement here lies in the fact that the data that is transported is more specified, and it is not necessary to move entire processes or applications for the relevant data to arrive at the target machine. Thus, the concept of mobility in mobile object systems refers to the movement of objects carrying specified data from one machine in a network to another.

---

[376] Wong/Paciorek/Moore, note 371, at 93.
[377] J Vitek, M Serrano, D Thanos, "Security and Communication in Mobile Object Systems" in J Vitek, C Tschudin (eds) *Mobile Object Systems: Towards the Programmable Internet* (Springer-Verlag, LNCS 1222: 1997) 177-201, 178.
[378] Braun/Rossak, note 367, at 22.
[379] E Jul, H Levy, N Hutchinson, A Black, "Fine-Grained Mobility in the Emerald System" (1988) 6:1 *ACM Transactions on Computer Systems*, 109-133, 110.
[380] Braun/Rossak, note 361, at 22.

The three presented technologies have fundamentally shaped the concept of mobility in AI. To better understand the concept of mobility, as it exists today, it is necessary to look at the changes it has undergone due to technological progress.
The earliest concept of mobility merely referred to the movement of code in a specified network. The focus was on achieving a general transfer of data, not on the specifications of the code executing this movement. As a result, the transfer of data from one machine to another machine was possible, but to achieve this, a whole process had to be moved. Furthermore, the transfer was a one-way process only, as the return of results was very difficult. However, the successful movement of data was a very important step for the concept of mobility, as it exists today.
This concept was further extended by technological progress, which aimed at improving the executing code. Thus remote evaluation systems enabled the transfer of more specific data (programs instead of processes) and more importantly, enabled the return of results to the requesting computer. Hence, the focus for improving the concept of mobility was on enhancing the executing code. This was confirmed by the development of mobile objects, which enabled the transfer of specified data and eased the movement of this data by working on the underlying code.

This trend is crucial for the use of mobility as a key concept in this thesis. The concept of mobility underlying mobile objects is not sufficient for the purpose of this thesis. Section 5.1 has presented the key characteristics of the technologies discussed in this thesis, which are, among others, goal-orientation, reactivity, and travelling between platforms and target computers. These require a much more advanced executing code than the one present in mobile code systems. Required is, for example, the ability to transport specific code to computers selected and targeted by the executing code. Furthermore, in mobile object systems the transportation of data occurs on explicit request by the client machine to the server machine. This means that both machines are aware of the movement and have to actively collaborate in it. Thus, the movement is a transparent process. However, the technologies discussed in this thesis execute the movement of data clandestinely and without explicit approval of the target machines.

Thus in a next step the current concept of mobility in AI is examined to determine whether it has transformed sufficiently to be adequate to be used as a key concept for this thesis.

5.4.1.4 Mobile Agents

The concept of mobility has most recently been advanced in the area of software agent research. In fact, the above-depicted technologies are sometimes regarded as ancestors of mobile software agent research.[381]

Generally, mobility in agent research equally refers to code being dispatched from a client computer and transported to a remote server computer for execution.[382] However, the notion of mobility has improved and changed considerably in mobile agents as compared to the other technologies introduced above. Most importantly, mobile agents support heterogeneous architectures, operating systems, and even heterogeneous administrative domains, such as the Internet, while previous technologies tend to be much more homogenous.[383] Hence, data can be moved between machines independent of the platform of the machine (thus independent of the operating system environment, such as Microsoft Windows, Mac OS, Linux). Furthermore, the migration of the code is self-initiated.[384] This means that the agent determines dynamically where and when to travel to a particular destination node based on some embedded mobility metadata to perform some required work.[385] The migration of the code is furthermore not restricted to one machine only, but the code can be moved to many different machines in the network.[386] Moreover, mobile agents execute asynchronously, thus do not rely on the host computer being connected to the network while moving the data and executing the tasks. Mobility of data often relied on expensive or fragile network connections. However, mobile agents, after being dispatched, become independent of the process that created them and can operate asynchronously. The mobile device can reconnect at a later time to collect the agent and the results of the agent's work.[387]

---

[381] Braun/Rossak, note 361, at 17; D S Milojicic, "Trend Wars - Mobile agent applications" (1999) 7:3 *EEE Concurrency* [see also IEEE Parallel & Distributed Technology] 80-90, 81.

[382] D Chess, C Harrison, A Kershenbaum, "Mobile agents: Are they a good idea?" in J Vitek, C Tschudin (eds), *Mobile Object Systems - Towards the Programmable Internet*, Lecture Notes in Computer Science (Springer-Verlag, Berlin Germany: 1997), 25–47, 25.

[383] Milojicic, note 372, at 83.

[384] P Braun, D Trinh, R Kowalczyk, "Integrating a New Mobility Service into the Jade Agent Toolkit" in T Magedanz et al.(eds.) *Mobility aware technologies and applications: second international workshop*, Lecture Notes in Computer Science (Berlin: Springer-Verlag, 2005), 354–363, 354.

[385] Wong/Paciorek/Moore, note 371, at 93.

[386] D B Lange, M Oshima, "Seven Good Reasons for Mobile Agents" (1999) 42:3 *Communications of the ACM*, 88-89, 88.

[387] Lange/Oshima, ibid, at 88.

Additionally, mobile agents adapt dynamically to their environment. While previous technologies relied on a specific and static environment for the migration of data, mobile agents readily adapt to changes in both the program state and the network environment (such as network partitioning and disconnected hosts) to modify their routing behaviour.[388]
Lastly, mobile agents reduce network load further as opposed to the previously discussed technologies. Distributed systems often rely on communication protocols involving multiple interactions to accomplish a given task. The result is a lot of network traffic. Mobile agents allow users to package a conversation and dispatch it to a destination host where interactions take place locally. Mobile agents are also useful when reducing the flow of raw data in the network. When very large volumes of data are stored at remote hosts, that data should be processed in its locality rather than transferred over the network.[389]

As has been established, the notion of mobility has been expanded and shaped by research into software agents. The analysis of these advancements indicates that research has indeed focused on improving the executing code underlying the movement of data. While all of the research findings in relation to the concept of mobility presented in this section are technology specific, this does not mean that these findings cannot be generalised. The concept of mobility as developed for software agents can equally be applied to technologies that are architecturally similar to this technology. Generally, if specific capabilities have been developed for one technology, these can be adapted for other technologies as well. Thus it is legitimate to derive a general concept of mobility from these findings.

Hence, the concept of mobility (at the time of finishing this thesis) can be defined as the dynamical and asynchronous movement of data between one or more machines in a heterogeneous network, which can be initiated by the executing code.

Having determined the meaning of the concept of mobility in this context it needs to be analysed whether this notion could serve as a key concept for the purpose of this thesis. This would be the case if the relevant key characteristics of the technologies discussed

[388] Wong/Paciorek/Moore, note 371, at 93.
[389] Lange/Oshima, note 386, at 88.

in this thesis can be subsumed under the concept of mobility. The relevant key characteristics are goal-orientation, reactivity, and travelling between platforms and target computers. As shown above, mobility refers to code, that is capable of moving between platforms and machines in a heterogeneous network, thus capable of travelling between platforms. Furthermore, it refers to code that is dynamical, thus capable of reacting to a changing environment and making decisions based on these changes, hence featuring reactivity and goal-orientation. The executing code is capable of moving data on the Internet, which is required for the specific use of the new software-based investigative technologies, the online search of ICT devices. Furthermore, due to the decrease in bandwidth required for the movement and execution of the tasks, the target computer will not slow down to an extend recognisable by the user. The move away from a strict client-server model towards an asynchronous and dynamical self-executing model means that the migration of data can occur without explicit request and permission by the involved machines, thus the migration can occur clandestinely.

This analysis has shown that the relevant key concepts can be subsumed under the concept of mobility, and thus this notion is adequate to serve as one of the key concepts defining a new class of software-based investigative tools.

The concept of mobility raises several legal issues, which are only briefly mentioned at this stage and analysed in more detail in the following chapters. The ability to collect data from any machine connected to the Internet potentially poses a jurisdiction problem, as the target machine can be located outside of the jurisdiction of the investigating authority. Furthermore, the execution of the designated task (e.g. search for relevant data and monitoring of communication) is carried out on the target machine and the results are moved via the network to the requesting machine. This raises a problem of reliability of evidence, challenging the chain of evidence.

5.4.2 Intelligence

Having determined that mobility is suitable to serve as one of the key concepts for the new class of investigative technologies, this section analyses whether the concept of intelligence in AI is equally suited.

Intelligence stems from the Latin verb *intelligere*, which means "to understand". Intelligence is natural to every human being. Humankind is able to undertake all kinds of activities such as walking, driving a car or bike, while at the same time listening to music or engage in a conversation with another person. We can watch a movie and order books on the Internet at the same time, as well as undertake heart surgery or play a game of chess. How is this possible and how does the brain enable this? What are minds and what is thinking? What is the relationship between the mind and the brain? The fundamental nature of intelligence is only dimly understood and much will remain beyond human understanding for a long time to come. Philosophers and psychologists have attempted to answer these questions for many centuries with mixed results, and there is little agreement on what does and does not constitute intelligence and how this term can be defined.

This is reflected by the introductory comments on intelligence in the Penguin Dictionary of Psychology: "Few concepts in psychology have received more devoted attention and few have resisted clarification so thoroughly."[390] However, while the term has been defined anew by many researchers working in this field, looking at some of these definitions can be an important source for gaining a basic understanding of this debate and the concept of intelligence. Human intelligence has been defined as:

> *"A very general mental capability that, among other things, involves the ability to reason, plan, solve problems, think abstractly, comprehend complex ideas, learn quickly and learn from experience. It is not merely book learning, a narrow academic skill, or test-taking smarts. Rather, it reflects a broader and deeper capability for comprehending our surroundings—"catching on", "making sense" of things, or "figuring out" what to do."*[391]

Furthermore, it has been defined as:

> "*the ability of a system to act appropriately in an uncertain environment, where appropriate action is that which increases the probability of success, and success is the achievement of behavioral subgoals that support the system's ultimate goal*."[392]

---

[390] A S Reber, E Reber, R Allen, *The Penguin Dictionary of Psychology* (Penguin Press: New York, US, 2009), 379.

[391] L S Gottfredson, "Mainstream sciences on Intelligence: An Editorial with 52 Signatories, History, and Bibliography" (1997) 24:1 *Intelligence*, 13-25, 13.

[392] J S Albus, "Outline for a Theory of Intelligence" (1991) 21:3 *IEEE Transactions on Systems, Man, and Cybernetics*, 473-509, 474.

These definitions highlight that certain capabilities that are connected with intelligent behaviour play a crucial role in defining the concept of intelligence. While research into human intelligence has focused on what constitutes intelligence and how it can be defined and classified, the existence of human intelligence per se is not an issue. Humans are, one can say, by default endowed with at least a minimum degree of intelligence.

However, the problem of defining the concept of intelligence in AI is that computers (or more accurately the underlying software) do not naturally possess intelligence on a human level. Intelligence is embedded into software through the engineer and software designer. The focus in AI is on how to replicate and create intelligence on a human level in machines.
This requires an understanding of what constitutes human intelligence, and what the underlying principles of this concept are.
When the digital computer was invented more than half a century ago, many felt that the essence of thinking, the core of intelligence, had been found.[393] This was the case because computers were capable of simulating natural language and problem solving on a human-like level, or even excelled humans at this. A famous example for this is the victory by the IBM Deep Blue chess computer over Garry Kasparov, the world chess champion at the time, in a match in 1997.[394] However, this victory was based on the computer being capable of undertaking millions of calculations (of the various possible manoeuvres in the game and their consequences) in a very short time, and not on the fact that the computer was particularly intelligent.

However, if a computer capable of beating the world chess champion is not intelligent, the question remaining is what constitutes *artificial intelligence*? Section 5.1.1, introducing the basics of AI, states that one way of defining this domain is the art of creating machines doing tasks requiring intelligence.[395] While this definition highlights that human intelligence is a crucial benchmark for determining artificial intelligence, it does not provide more helpful information beyond this. Another definition introduced in the same section further specifies that creating such machines capable of

[393] R Pfeifer, C Scheier, *Understanding Intelligence* (MIT Press: Cambridge, MA, 1999), xi.
[394] See http://www.research.ibm.com/deepblue/
[395] See p. 127.

undertaking tasks requiring intelligence, means recreating human mental capabilities.[396] Thus this definition explains in more detail what human intelligence means, namely that it refers to mental capabilities.

While this information is not specific enough to serve as a general explanation of what the concept of intelligence refers to in AI, it can serve as a starting point for the analysis in this section. The important aspect that can be drawn from this is that knowledge of what constitutes human intelligence is required before being able to determine what precisely constitutes the concept of intelligence in AI.

5.4.2.1 Human Intelligence

As depicted in the previous section, human intelligence is still a rather unexplored and largely unknown concept.
As Albus puts it, "the definition of human intelligence remains a subject of much controversy, and so must any theory that attempts to explain what intelligence is, how it originated, or what are the fundamental processes by which it functions."[397]
One of the first attempts at creating a scientific test to determine what constitutes human intelligence was the introduction of intelligence (IQ) tests. The general idea of an IQ test is to measure a capacity that is not dependent on particular knowledge but is, in a sense, a "general intelligence capacity", or "factor g", as it is sometimes called.[398]
The heritage of the IQ test is grounded in the work of Galton, the "father" of the study of individual differences.[399]
It was Binet, who wanted to predict the school success of Paris children with this test, who invented the IQ test as is known today in 1905.[400]

There has been a huge controversy about the validity and usefulness of the IQ test and the general consensus is that this test measures general abilities that are of particular importance for learning abilities at school, but that it is difficult to reduce a highly complex phenomenon like human intelligence to a single number, and that these tests

---

[396] Ibid.
[397] Albus, note 392, at 473.
[398] Pfeifer/Scheier, note 393, at 12.
[399] R A Weinberg, "Intelligence and IQ" (1989) 44:2 *American Psychology*, 98-104, 100.
[400] Ibid.

fail to predict well the life outcomes for many people.[401] Thus the major controversy is rooted in the criticism that IQ tests are not a fair sample of a person's entire repertoire of adaptive behaviour, and are not adequate indicators of the quality and character of human functioning. Hence, intelligence is not limited to what IQ tests measure.
This was confirmed by many, but particularly Gardner in his research has found that intelligence consists of "multiple intelligences" or "multiple competences" as he has coined it.[402] According to Gardner intelligence consists not of one single factor but of multiple ones: linguistic intelligence, musical intelligence, logical-mathematical intelligence, spatial intelligence, bodily-kinesthetic intelligence, and personal intelligences (inter- and intrapersonal).[403] Thus human intelligence is more difficult to determine and understand than imagined by the founders of the IQ test.
These attempts to test intelligence have raised the issue of where intelligence and knowledge stems from: the so-called nature-nurture debate.[404] This debate is of relevance for the determination of artificial intelligence, as it could provide essential information on where intelligence stems from and how it can be developed, and therefore replicated. However, it is impossible to recite the whole debate here and the focus will therefore be on the main arguments.

The major points of view – Locke versus Descartes, empiricism versus rationalism, a "blank slate" versus a "prepared mind", and behaviorism versus ethology- represent two essentially different approaches to understanding how individuals gain knowledge.[405] Hence, those following the "nature" view argue that development is largely the expression of genetically predetermined factors, whereas those following the "nurture" view argue that most abilities are acquired during development and can be learned. The debate around these issues is long standing but no sufficient evidence proofing one view has been generated to date. However, results from scientific studies

---

[401] See e.g. D C McClelland, "Testing for Competence rather than for 'Intelligence'" (1973) 28:1 *American Psychology*, 1-14, 4.
[402] H Gardner, *Frames of Mind* (New York: Basic Books, 1983); H Gardner, T Hatch, "Multiple Intelligences Go to School: Educational Implications of the Theory of Multiple Intelligences" (1989) 18:8 *Educational Researcher* 4-10.
[403] Gardner/Hatch, ibid, at 6.
[404] See e.g. D S Moore, *The Dependent Gene: The Fallacy of the Nature versus Nurture Debate* (New York: Henry Holt, 2003).
[405] H H Spitz, *The raising of intelligence: A selected history of attempts to raise retarded intelligence* (Hillsdale, NJ: Erlbaum, 1986).

suggest that the claim that intelligence and knowledge is solely "hard-wired into the genes" and cannot be acquired and influenced by the environment is problematic.

Scarr and Weinberg conducted a study among cross-racial adopted children in 1976.[406] In this study, the IQ of black children adopted by white upper-middle-class families was compared to that of black or interracial children not raised in the specific culture of the tests and schools. The adopted children scored well above average on IQ tests and on school achievement measures, and much better than the black and interracial children with similar genetic background, who grew up in a different environment. This study showed that the environment does indeed play a role in the development of intelligence and the acquiring of knowledge. Therefore, it can be concluded that genes are not the sole determinator for behavior. Rather, they establish a range of possible reactions to the range of possible experiences that environments can provide. Environments can also affect whether the full range of gene reactivity is expressed. Thus, how people behave or what their measured IQs turn out to be or how quickly they learn depends on the nature of their environments and on their genetic endowments bestowed at conception.[407]

Having reached this conclusion, the problem then is to determine how this development works, thus how environmental and genetic factors interact in the organism to create intelligence. Understanding this is a vital step towards replicating human intelligence in machines and therefore understanding the concept of artificial intelligence. Much research has been undertaken in the fields of neuroscience and neuroinformatics to understand and recreate this process.[408] Neural networks introduced in section 5.3 are one of the research outputs of this field, attempting to replicate the human brain and creating intelligence on a human level. Thus, although much is known about the mechanisms and functions of human intelligence it is still a difficult task to understand the fundamental nature of human intelligence and define this.

---

[406] S Scarr, R A Weinberg "IQ test performance of black children adopted by white families", (1976) 31:10 *American Psychologist,* 726-739.
[407] Weinberg, note 399, at 101.
[408] See e.g. D Gardner, G M Shepherd "A gateway to the future of Neuroinformatics" (2004) 2:3 *Neuroinformatics* 271–274; M A Arbib, J S Grethe, *Computing the Brain: A Guide to Neuroinformatics* (San Diego: Academic Press, 2001).

Albus states that at a minimum level, intelligence requires the ability to sense the environment, to make decisions, and to control action. Higher levels of intelligence may include the ability to recognise objects and events, to represent knowledge in a world model, and to reason about and plan for the future. In advanced forms, intelligence provides the capacity to perceive and understand, to choose wisely, and to act successfully under a large variety of circumstances so as to survive, prosper, and reproduce in a complex and often hostile environment.[409]

It can be concluded that human intelligence is a profoundly complicated concept that is not fully understood. Research has evidenced that human intelligence cannot be measured in one number, but consists of multiple types of intelligences. Human intelligence develops through the interaction of genes and environmental influences and exists on different levels. Hence, machines that act intelligently need to be capable of achieving at least the minimum level of human intelligence. Considering the specific use of the new software-based investigative technologies, it becomes clear that the ability to sense the environment, make decisions, and control actions are key attributes of these technologies. Thus in a next step, it needs to be established whether the concept of intelligence in AI refers to such abilities.

5.4.2.2 Computational Intelligence

The introduction to AI as a research field above,[410] has already highlighted that the idea of intelligent software is old, but the realisation of this a difficult task. This section focuses solely on the analysis of the concept of artificial or computational intelligence, not the research field Artificial Intelligence in its entirety.[411] However, the above-discussed basic notions of AI are highly relevant for the analysis of what constitutes computational intelligence in this section.

The original aim of Turing to replicate human intelligence in its entirety (strong AI) has, for the time being, proven to be impossible. The aim is rather to replicate certain notions of human intelligence. The methodology for this is to design, build, and

---

[409] Albus, note 392, at 474.
[410] See p. 127.
[411] Insofar as these two can be researched in isolation. Artificial Intelligence as a research field by necessity includes the discussion of machine or artificial intelligence. However, AI as a research field encompasses a diversity of research areas as depicted above.

experiment with computational systems that perform tasks commonly viewed as intelligent.[412] The focus is therefore not on defining the concept computational intelligence (this would prove equally difficult as defining human intelligence) but rather analyse whether software possesses capabilities that can be classified as comparable to human intelligence.

As discussed above, human intelligence exists on different levels.[413] Relevant and necessary for this thesis are particularly the capabilities to sense the environment, make decisions, and control actions.

McCarthy and Hayes argue that a computer program capable of acting intelligently in the world must have a general representation of the world implemented, in light of which its inputs are interpreted.[414] The above-discussed symbolism approach to AI facilitates this approach.[415] Similar to symbolic AI, where concepts for certain objects are formalised, McCarthy and Hayes explain that concepts of causality, ability, and knowledge need to be formalised to enable a computer program to decide what to do.[416]

Their understanding of computational intelligence is that an entity that has an adequate model of the world (including the intellectual world of mathematics, understanding its own goals and other mental processes), is smart enough to answer a wide variety of questions on the basis of this model, can obtain additional information from the external world when required, and can perform such tasks in the external world as its goals demand and its phys ical abilities permit.[417]

Albus has confirmed this understanding of computational intelligence, stating that the functional elements of an intelligent system are behaviour generation, sensory perception, world modelling, and value judgment.[418]

---

[412] D Poole, A Mackworth, R Goebel, *Computational Intelligence: A Logical Approach* (New York: Oxford University Press, 1998) 2.
[413] See p. 144.
[414] J McCarthy, P J Hayes, "Some Philosophical Problems from the Standpoint of Artificial Intelligence" (1969) 4 *Machine Intelligence*, 464.
[415] See p. 129.
[416] McCarthy/Hayes, note 414, at 463.
[417] McCarthy/Hayes, note 414, at 466.
[418] J S Albus, "The Engineering of Mind" (1999) 117 *Information Science*, 3.

Russel and Norvig contribute to this that central to the approach to computational intelligence is the concept of rationality.[419]

Nilsson adds that computational intelligent behaviour involves perception, reasoning, learning, communicating, and acting in complex environments.[420]

Eberhart and Shi understand computational intelligence as computing that provides systems with an ability to learn and/or deal with new situations, such that the system is perceived to possess one or more attributes of reason, such as generalisation, discovery, association, and abstraction.[421]

These definitions of computational intelligence confirm the argument that the replication of intelligence in its entirety is impossible and indeed undesirable, but that the replication of certain human behaviour and capabilities considered to be intelligent is sufficient and constitutes computational intelligence. These definitions also confirm that the capabilities relevant and required for the software tools discussed in this thesis are an integral part of what constitutes computational intelligence. Thus the concept of (computational) intelligence as such seems well suited to serve as a key concept for this work.

However, as Poole et al. point out, there is a tension between the theoretical principles of computational intelligence, and the engineering of computational intelligence.[422] Thus the question is whether the theoretical principles developed by McCarthy and Hayes and others can technically be realised.

The engineering of computational intelligence requires the analysis of the relevant human behaviour. Steels explains that "for a long time, the natural sciences have made progress by reducing the complexity at one level by looking at the underlying components. Behaviour at a particular level is explained by clarifying the behaviour of the components at the next level down. For example, properties of chemical reactions

---

[419] Russell/Norvig, note 279, at 32.
[420] N J Nilsson, *Artificial Intelligence: A New Synthesis* (Burlington: Morgan Kaufmann Publishers, 1998) 1.
[421] R C Eberhart, Y Shi, *Computational Intelligence: Concepts to Implementation* (Burlington: Morgan Kaufmann Publishers, 2007) 3.
[422] Poole/Mackworth/Goebel, note 412, at 5.

are explained (and predicted) by the properties of the molecules engaged in the reactions. In the case of intelligence, researchers hope that an understanding of intelligence will come from understanding the behaviour underlying components. For example, most neurophysiologists believe that a theory of intelligence will result from understanding the behaviour of neural networks in the brain."[423]

Thus replicating intelligent behaviour requires identifying and analysing the scientific foundations of the equivalent human behaviour, and developing methods to engineer these.

However, cognitive tasks humans perform every day without consciously thinking about them are facilitated by the complex adaptive biological structure of human brains.[424] Research in fields such as biology and biophysics has shed some light on the construction and operation of the human brain and nervous system, which helps to understand how these tasks are performed.[425]

This research linked with the requirements in AI has led to the development of research areas that are concerned with the replication of these human brain functions, and thus enable the replication of intelligent behaviour. Hence, these research areas are essentially concerned with reverse engineering the human brain.

Albus has long assumed that brains must have very complex, explicit, hard-wired hierarchies of systems to handle a high degree of complexity in space and in time.[426] This finding was confirmed by research into the reverse engineering of the human brain, and has been a fundamental pillar for the development of research areas concerned with the replication of intelligent behaviour.[427]

Discussing these research areas and their findings in great detail would go beyond the scope of this work. However, the most relevant findings are introduced below, to establish in how far the replication of intelligent behaviour is feasible.

---

[423] L Steels, "When Are Robots Intellligent Autonomous Agents?" (1995) 15 *Robotics and Systems*, 4.

[424] Eberhart/Shi, note 421, at 4.

[425] Ibid.

[426] Albus, note 392, at 473.

[427] See e.g. P J Werbos, "ADP Design to Replicate/Understand Brain Intelligence" in L I Perlovsky, R Kozma, *Understanding Complex Systems* (Berlin, Heidelberg: Springer Verlag, 2007) 119.

5.4.2.2.1 Artificial Neural Networks

Human-level intelligence entails the capacity to handle a broad array of challenges, including logical reasoning, understanding the semantic content of language, learning, navigating around obstacles in a room, discerning the intent of other agents, and planning and decision making in situations where information is incomplete.[428] In humans, the functioning of the brain enables these capacities. Artificial neural networks, a technique to replicate this brain functioning, are one approach to creating software capable of intelligent behaviour.

Artificial neural networks are based on the biological neural networks model, which is a network or circuit of biological neurons.[429] To facilitate the replication of intelligent behaviour, and in particular the abilities to sense the environment, make decisions based on visual stimuli, and control one's actions, simplified models of artificial neural networks mimicking the neural processing in the brain have been developed. The replication of biological neural networks is particularly interesting, because the brain and its functions are so remarkably robust; it does not stop working just because a few cells die.[430]

Krogh states that "the computations of the brain are done by a highly interconnected network of neurons, which communicate by sending electric pulses through the neural wiring consisting of axons, synapses and dendrites."[431] This biological process of sensory processing by the brain inspired the creation of artificial neural networks. Simulating a network of model neurons in a computer can create an artificial neural network.[432] By applying algorithms that mimic the processes of real neurons, the artificial network can 'learn' to solve many types of problems.[433] Most current versions of artificial neural networks, often referred to as self-organising networks, learn to classify information without being taught. This is called unsupervised adaption and can frequently be used to categorise information when no known categories exist yet.[434]

---

[428] W Wallach, S Franklin, C Allen, "A Conceptual and Computational Model of Moral Decision Making in Human and Artificial Agents" (2010) 2 *Topics in Cognitive Science*, 455.
[429] J J Hoppfield, "Neural Networks and Physical Systems with Emergent Collective Computational Abilities" (1982) 79:8 *Proceedings of the National Academy of Science*, 2554.
[430] A Krogh, "What are artificial neural networks?" (2008) 26:2 *Nature Biotechnology*, 195.
[431] Ibid.
[432] Ibid.
[433] Ibid.
[434] Eberhart/Shi, note 421, at 158.

This enables the integration of software into a real-world environment, since the system is capable of dynamically behaving in unknown situations.[435]

Neural networks have highly desirable properties: just like natural brains they can adapt and learn, they are noise and fault tolerant, i.e. they continue to function even when partially damaged, and they can generalise, meaning they continue to work in similar but different situations.[436]

Salomon finds that the field of autonomous agents is an important application domain for neural networks, since they behave in the real world without any human control.[437]

The unsupervised adaption capability of neural network based systems is particularly important for autonomous agents. This is also the case for the software tools deployed during online searches of computers, which need to be capable of sensing and understanding their environment, and making decisions based on the information retrieved.

Salomon states further that the employment of neural networks to autonomous agent software should lead to intelligent behaviour of these.[438]

Thus artificial neural networks enable the replication of intelligent behaviour introduced in the previous section.

5.4.2.2.2 Fuzzy Logic

Fuzzy logic is another technique that facilitates the replication of intelligent behaviour, and implementation of this into software tools.

Fuzzy logic provides a general concept for description and measurement. Most fuzzy logic systems encode human reasoning into a program to make decisions or control a system.[439]

However, as opposed to neural networks, the biological motivation or basis for fuzzy logic does not originate at the cellular level. Rather, as Eberhart and Shi state, it is reflected at the behavioural level of the organism, that is, in the ways the organism

---

[435] R A Lucas, *Evolving Artificial Neural Network Controllers for Autonomous Agents Navigating Dynamic Environments* (University of Northern British Columbia: Thesis, 2008) 1.

[436] R Pfeifer, J Bongard, D Berry, *Designing Intelligence – Why Brains Aren't Enough* (Norderstedt: GRIN Verlag, 2011) 16.

[437] R Salomon, "Neural Networks in the Context of Autonomous Agents: Important Concepts Revisited" in C H Dagli et al. (eds) *Proceedings of the Artificial Neural Networks in Engineering (ANNIE'96)* (New York: ASME Press, 1996) 109.

[438] Ibid.

[439] Eberhart/Shi, note 421, at 269.

interacts with its environment.[440] They further explain, "while neural networks are deeply rooted in biology, fuzzy logic deals mainly with uncertainty and vagueness. We do not live in a world of ones and zeros, black and white, true and false, or other absolutes. Our observations, communications, and experiences almost always include a large measure of uncertainty."[441]

Ross elaborates further on this, stating that "our understanding of most physical processes is based largely on imprecise human reasoning. This imprecision (when compared to the precise quantities required by computers) is nonetheless a form of information that can be quite useful to humans. The ability to embed such reasoning in hitherto intractable and complex problems is the criterion by which the efficacy of fuzzy logic is judged."[442]

Zadeh can be regarded as the pioneer of fuzzy logic.[443] He defines fuzzy logic as "the precise logic of imprecision. More concretely, fuzzy logic is a system of reasoning and computation in which the objects of reasoning and computation are classes with unsharp boundaries."[444] He elaborates further that "fuzziness of human concepts is a pervasive facet of human cognition."[445]

Thus fuzzy logic can facilitate reasoning about fluid and approximate facts and circumstances, instead of fixed and exact ones usually required for computational reasoning. This enables software to reason about uncertain, unclear, or unknown facts and situations, applying a methodology similar to the reasoning of humans, which is based on past experiences and memories about similar situations.

Two main directions in fuzzy logic can be distinguished: a) Fuzzy logic in the broad sense, and b) fuzzy logic in the narrow sense.[446] Fuzzy logic in the broad sense serves predominantly as a tool for fuzzy control and analysis of vagueness in natural

---

[440] Eberhart/Shi, note 421, at 9.

[441] Ibid.

[442] T J Ross, *Fuzzy Logic with Engineering Applications* (Chichester: John Wiley & Sons, 2004, 2nd ed.) 2.

[443] See e.g. L A Zadeh, "Fuzzy Sets" (1965) 8 *Information and Control*, 338-353; L A Zadeh , "Fuzzy Logic and Approximate Reasoning" (1975) 30:3-4 *Synthese*, 407-428; L A Zadeh, "Fuzzy Sets as a Basis for a Theory of Posibility" (1978) 1:1 *Fuzzy Sets and Systems*, 3-28; L A Zadeh, "Fuzzy Logic" (1988) 21:4 *Computer*, 83-93; L A Zadeh, "Fuzzy Logic, Neural Networks, and Soft Computing" (1994) 37:3 *Communicatioins of the ACM*, 77-84; L A Zadeh, "A Summary and Update of Fuzzy Logic" (2010) *2010 IEEE International Conference on Granular Computing*, 42-44.

[444] L A Zadeh, ibid (2010), at 42.

[445] Ibid.

[446] L A Zadeh, "Preface" in R J Marks (ed) *Fuzzy Logic Technology and Applications* (New Jersey: IEEE Press, 1994) xvii.

language.[447] Fuzzy logic in the narrow sense is symbolic logic with a comparative notion of truth developed fully in the spirit of classical logic.[448]
Fuzzy logic has been applied to autonomous agent software to enable the decision-making and navigation in unknown virtual environments.[449]
Hence fuzzy logic is suitable to enable intelligent behaviour in software and situations relevant for this thesis.

Neural networks and fuzzy logic combined thus offer possibilities to enable the replication of intelligent behaviour, and in particular the sensing of the environment and the ability to make decisions based on information retrieved from the environment, as well as the ability to control its own actions and adapting these to the requirements of the environment.

It can therefore be concluded that the notion of computational intelligence differs from that of human intelligence. However, the notion of computational intelligence incorporates some of the key characteristics of software-based investigative tools, and is therefore adequate and relevant to serve as a key concept for the new class of cyber-cops. In addition, the analysis of computational intelligence has indicated that this notion is flexible and capable of dealing with technological changes, thus adequate to deal with future developments and enhancements of relevant ICT-based investigative technologies and tools.

However, the concept of intelligence raises several pertinent legal issues, which are only mentioned at this stage and analysed in more detail in the following chapters of this thesis. The abilities of software code to control its own actions, and adapt and react to its environment without the influence or control of the operator lead to legal

---

[447] See for more details on this notion e.g.: V Novak, *Fuzzy Sets and their Applications* (Bristol: Adam Hilger, 1989); H-J Zimmermann, *Fuzzy Set Theory and its Applications* (Dordrecht: Kluwer, 1991, 2nd ed); G J Klir, B Yuan (eds) *Fuzzy Sets, Fuzzy Logic and Fuzzy Systems: Selected Papers by Lotfi A Zadeh* (Singapore: World Scientific, 1996); H T Nguyen, C Noguera, *First Course in Fuzzy Logic* (Boca Raton: Chapman & Hall/CCRC Press, 1999, 2dn ed).
[448] See for more details on this notion e.g: P Hajek, *Metamathematics of Fuzzy Logic* (Dordrecht: Kluwer, 1998); E Turunen, *Mathematics Behind Fuzzy Logic (Advances in Soft Computing)* (Heidelberg: Physica Verlag, 1999); V Novak, I Perfilieva, J Mockor, *Mathematical Principles of Fuzzy Logic* (Dordrecht: Kluwer, 2000); S Gottwald, *A Treatise on Many-Valued Logic* (Baldock: Research Studies Press, 2001); R Cignoli, I D'Ottaviano, D Mundici, *Algebraic Foundations of Many-Valued Reasoning* (Dordrecht: Kluwer, 2000).
[449] See J Jaafar, E McKenzie, "Decision Making Method Using Fuzzy Logic for Autonomous Agent Navigation" (2011) 3:1 *Electronic Journal of Computer Science and Information Technology*, 8-18.

questions about the regulation of these tools, as well as the reliability of the evidence collected. During the interviews, these were the most pressing concerns in relation to these abilities voiced by the different parties interviewed.

5.4.3 Autonomy

In addition to mobility and intelligence, autonomy has been identified as a potential third key concept above.[450]

The term autonomy stems from Greek: Auto-nomos. *Auto* meaning self, and *nomos* meaning law. It refers to an entity that gives itself its own laws. Generally, the term autonomy refers to the quality or state of being self-governing.[451]

However, autonomy is a concept with a long history, and has therefore been developed and interpreted in various ways. As a result, autonomy is a concept bearing many connotations such as rationality, freedom, independence, and self-determination.[452]

Generally, autonomy in humans can be summed up to mean that to be autonomous is to be a law to oneself.[453]

Generally, all these conditions or qualities relate to the freedom from control by others. This means that autonomy requires a certain degree of intelligence. As discussed in the previous section, humans are by nature endowed with a certain degree of intelligence. The discussion of intelligence has highlighted that human and computational intelligence are not identical concepts.

The question is therefore what the concept of autonomy in AI refers to, and whether it incorporates the key attributes of the relevant investigative technologies identified above.[454]

As a first step, it is necessary to distinguish between autonomy and the concept of automatic systems, as these appear to be similar. However, as Steels discusses, the concept of automation has a different linguistic root.[455] It stems from the etymology of the term *cybernetic*, which derives from the Greek for *self-steering*. Thus automatic

---

[450] See p. 124.

[451] Merriam-Webster Dictionary, "Autonomy" available online at http://www.merriam-webster.com/dictionary/autonomy.

[452] M Schermer, *The Different Faces of Autonomy: Patient Autonomy in Ethical Theory and Hospital Practice* (Dordrecht: Kluwer, 2002) 1.

[453] Stanford Encyclopedia of Philosophy, "Personal Autonomy" 1.

[454] See p. 125.

[455] Steels, note 423, at 5.

systems are self-regulating, but they do not make the laws that their regulatory activities seek to satisfy. These are given to them, or built into them.[456] Autonomous systems on the other hand are systems that develop, for themselves, the laws and strategies according to which they regulate their behaviour: they are self-governing as well as self-regulating.[457]

Considering the specific demands for investigative tools policing the virtual living space identified above, it becomes clear that the concept of automatic systems is not sufficient. While some of the rules will be pre-defined, the software tools need to be capable of adjusting or amending these depending on the environment, collected data, and suspect behaviour.

Definitions of autonomy in the AI domain provide a better understanding of the concept autonomy.

Liu et al. divide autonomy into four sub-classes, for which they offer definitions: *entity autonomy*, *synthetic autonomy*, *emergent autonomy* and *computational system autonomy*.[458]

They define *entity autonomy* as "a condition or quality of being self-governed, self-determined, and self-directed. It guarantees that the primitive behaviour of an entity is free from the explicit control of other entities."[459]

Synthetic autonomy refers to "an abstracted equivalent of autonomy of an entity in a natural complex system. An entity with synthetic autonomy is the fundamental building block of an autonomy oriented computing system."[460]

Emergent autonomy "is an observable, self-induced condition or quality of an autonomy oriented computing system that is composed of entities with synthetic autonomy."[461]

Computational autonomy "is built from computational entities with synthetic autonomy, refers to conditions or qualities of having self-governed, self-determined, and self-directed computational entities that exhibit emergent autonomy."[462]

---

[456] Ibid.
[457] Ibid.
[458] J Liu, X Jin, K C Tsui, *Autonomy Oriented Computing: From Problem Solving to Complex Systems Modeling* (Dordrecht: Kluwer, 2005) 6.
[459] Ibid.
[460] Liu/Jin/Tsui, ibid, at 7.
[461] Ibid.
[462] Ibid.

These four different concepts of autonomy introduced by Liu et al. highlight that autonomy is a social concept. An entity's autonomy is characterised by the influence and relations to other entities. Hence, autonomy is not the same as independence.[463] In a society (natural or artificial) certain dependencies are necessary for it to function.[464] However, it also highlights that autonomy in AI, just like mobility and intelligence, refers to an abstract version of human autonomy. Thus, the question remains whether autonomy in software is relevant and suitable to serve as a key concept for the new class of investigative technologies.

Simon in his work coins the term quasi-autonomy to distinguish between the natural and the artificial worlds.[465] He regards quasi-autonomy from the outer environment as an essential characteristic of complex systems.[466] Thereby he confirms that certain dependencies are necessary and will always exist.

Colman and Han develop this thought further, identifying five levels of autonomy based on the constraints to which an entity is subject.[467]

These levels are:[468]

1. **No autonomy**: the entity is told what actions to execute, and always attempts to execute them.
2. **Process autonomy**: the entity is given a task to perform in the form of a goal state but it has some autonomy in what steps are executed in order to achieve that task.
3. **Goal-state autonomy**: the entity is given an external goal, which may be satisfied by a number of states.
4. **Intentional autonomy**: the entity has the freedom to decide whether or not to satisfy external goals – it has (or the developers ascribe to it) its own intentions.
5. **Constraint autonomy**: an entity that exhibits constraint autonomy is prepared to violate norms or even rules to achieve its goals.

These five levels highlight that the degree of autonomy is a question of design. It shows that the software tools need to be developed with the application environment and

---

[463] H Weigand, V Dignum, "I am Autonomous, You are Autonomous" in M Nickles, M Rovatsos, G Weiss (eds) *Autonomy 2003, LNAI 2969* (Berlin, Heidelberg: Springer, 2004) 228.
[464] Ibid.
[465] H A Simon, *The Sciences of the Artificial* (Cambridge: M.I.T. Press, 1969).
[466] Ibid.
[467] A Colman, J Han, "On the Autonomy of Software Entities and Modes of Organisation" (2005) *Proceedings of the 1st International Workshop on Coordination and Organisation* (CoOrg 2005), 3.
[468] Ibid.

their tasks in mind. Software tools deployed for the policing of the virtual living space (such as for the online searching of ICTs) need to possess at least intentional autonomy to accomplish the tasks adequately.
Thus the question is whether these software tools can be endowed with this level of autonomy.

The concept of autonomy has been of great importance for software agent development, as well as the development of malware and malware-like applications. D'Inverno and Luck define autonomy in software agents as "not being dependent on the goals of others, and the possession of goals that are generated from within rather than adopted from other agents. Such goals are generated from motivations, higher-level non-derivative components characterising the nature of the agent, but which are related to the goals."[469] Similarly Castelfranchi defines an autonomous agent as "a software program able to exercise a choice that is relevant in the context of goals-directed behaviour."[470] Thus he equally argues that autonomy in software agents is characterised in terms of agents having their own goals, making decisions about these goals and adopting the goals of others only when they choose to.
Jennings and Wooldridge state that autonomy reveals "when the system is able to act without the direct intervention of humans (or other agents), and has control over its own actions and internal state."[471] In other words, autonomy means that the agent is able to act continuously without interfering with its user or operator.
These definitions indicate that autonomy in software agents exists at least at the level of intentional autonomy, since the agents are capable of deciding whether or not to satisfy external goals. Arguably, software agents can possess constraint autonomy, since ignorance of external rules implies the potential violation of these.
Autonomy in malware or malware-like software is less well defined. However, Dörges finds that "autonomy is important for most malware because it means that it is able to run and execute without user intervention."[472]

---

[469] d'Inverno/Luck, note 274, at 29.
[470] C Castelfranchi, "Guarantees for Autonomy in Cognitive Agent Architecture" (1995) 890 *Intelligent Agents: Theories, Architectures, and Language*, 57.
[471] N Jennings, M Wooldridge, "Applications of Intelligent Agents" in N Jennings, M Wooldridge (eds.) *Agent Technology: Foundations, Applications, and Markets* (Berlin, Heidelberg, New York: Springer, 1998) 4.
[472] T Dörges, "Why Protection against Viruses, Bots, and Worms is so hard- Malware seen as Mobile Agents" (2007) *PRESECURE Consulting GmbH*, 2 available online at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.4657&rep=rep1&type=pdf.

Heiser discusses this in more detail, stating that autonomy is "the most significant aspect of malware behaviour within any particular life phase, affecting most of the other characteristics. Autonomy in malware means that the code operates by itself automatically without direct human intervention."[473]

Thus, while no detailed definitions and discussions about the meaning of autonomy in malware exist, those academics find that the core meaning of the concept is identical with that of software agents. Both refer to the unsupervised operation of software, and the capability of goal-oriented behaviour.

The technical realisation of these capabilities is not discussed here. Of importance for this chapter is the analysis of the concept of autonomy in AI, and the establishment of the key characteristics of this concept to determine whether it is suitable to serve as a key concept for this thesis. Generally, the technical implementation of the capabilities into software code is typically undertaken through formal logic programming.[474]

Hence, the concept of autonomy in software agents and malware is identical with the general notion of (computational) autonomy.

This means that software-based investigative tools policing the virtual living space are capable of featuring autonomous behaviour. Hence, these tools are capable of goal-directed behaviour, and autonomous decision-making.

Based on this review, it can be concluded that the concept of autonomy in AI is suitable to serve as a key concept for the new class of investigative software tools.

Autonomy in software is linked to certain risks, which are particularly prevalent if used during investigations. Most significantly, the software tool independently decides about actions, and develops own goals during the process. Local and updated information is taken into consideration during the investigative process, and this can require timely

---

[473] J G Heiser, "Understanding today's malware" (2004) 9:2 *Information Security Technical Report*, 56.

[474] See e.g. d'Inverno/Luck, note 274, at 30ff; M Nowostawski, M Purvis, "The Concecpt of Autonomy in Distributed Computation and Multi-Agent Systems" (2007) *2007/6 The Information Science Discussion Paper Series*, 3 ff; H Hexmoor, "Case Studies of Autonomy" (2000) *Proceedings of FLAIRS*, 2000; M Nickles, M Rovatsos, G Weiß, "A Schema For Specifying Computational Autonomy" (2002) *Proceedings of the Third International Worksop on Engineering Societies in the Agents World (ESAW)*; I Rejer, "A Method for Improving Agent's Autonomy" (2010) *Agent and Multi-Agent Systems: Technologies and Applications*, 52-61. Also see chapter 8 of this thesis for more details on formal language, and the implementation of rules into software code.

reactions, which the tool makes itself. The designers and operators of the tools can only to a certain degree influence these processes.
This raises several pertinent legal issues, which are only briefly introduced at this stage and analysed in more detail in the following chapters of this thesis. Most importantly, autonomy raises issues for the regulation of these tools, as well as the reliability of the evidence collected.[475]

Summarising, it can be concluded that the three concepts *mobility*, *intelligence* and *autonomy* are suitable to serve as key concepts for current and future software-based investigative tools deployed for the policing of the virtual living space (such as the online searching of ICTs). Taken together, as analysed above, the most important characteristics of the technologies relevant for this thesis can be subsumed under these concepts. In addition, all three concepts are flexible enough to deal with technological progress and future technologies utilised during investigations. As discussed above, this is important for the sustainability of regulatory attempts.

This new class of ICT-based investigative tools is termed *Mobile, Intelligent and Autonomous (MIA) Policing Tools*. It is of relevance not only for the new cyber-policing method *online search*, but also more generally for the new cyber-policing system as a whole.
Results of the empirical study presented in chapter 3 have evidenced that future software-based investigative tools will increasingly replace humans for the policing of the virtual living space. This means that these tools necessarily have to possess abilities that enable them to operate autonomously, act intelligently and move around in the virtual living space.

This is also highlighted by recent cyber-warfare and cyber-espionage cases Stuxnet and Flame, which were developed by governments to disrupt and spy on industrial infrastructures of other countries, and feature these abilities.[476]

---

[475] Further legal issues are the legal classification of these tools (can these still be regarded as mere investigative tools, or are these quasi-officer? For a discussion of this see Schafer, note 270), and the drafting of a legal basis allowing for the use of these tools. These issues, while equally relevant, cannot be discussed within the scope of this thesis. The focus is on issues that have been identified as most pressing by the different interviewees.
[476] See e.g. K Zetter, "Researchers Connect Flame to US-Israel Stuxnet Attack" (2012) *Wired*, available online at: http://www.wired.com/threatlevel/2012/06/flame-tied-to-stuxnet/; for a detailed analysis of the abilities of Stuxnet see N Falliere, L O Murchu, E Chien, "W32.Stuxnet

5.5 Conclusion

This chapter has made an important contribution towards the development of a future-proof regulatory approach of software-based investigative tools. The development of a new class of software-based investigative tools – *Mobile, Intelligent and Autonomous (MIA) Policing Tools* - enables the regulation of a group of current and future technologies, and a move away from the presently predominant ex-ante authorisation system of new investigative tools.

This new class has been developed based on key characteristics of software-based investigative tools discussed in chapters 2, 3 and 4. The concepts *mobility*, *intelligence,* and *autonomy* have proven to be suitable to serve as key concepts for this new class. Their meaning within the source domain AI is broad enough to subsume current and future tools under these concepts. In addition, these concepts refer to software abilities that are fundamental for the replacement of humans by cyber-cops for the policing of the virtual living space. It is therefore of relevance beyond the scope of this thesis.

The results of this chapter, together with those of chapter 4, form the technical foundation of this thesis. This technical research is vital for an informed legal analysis of current and future problems of the use of software-based investigative tools. Some of the current regulatory problems have arisen due to insufficient technical knowledge and, as pointed out before in this work, a lack of technical research on this topic. The research of these technical chapters clearly defines the abilities of MIA tools and therefore enables both, a detailed analysis of the most pressing legal problems and the development of a future-proof regulatory system for cyber-cops policing the virtual living space.

This newly established class is the reference point for all legal discussion in the following sections. The advantage of having identified this class is that all the legal findings of this thesis apply to a broad group of investigative tools and actions (although a focus remains on the online searching of ICTs as a confirmed investigative method) instead of one specific technology, only. This also means that the findings are

---

Dossier" (2011) *Symantec*, available online at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

of relevance for policy-makers in the longer term, instead of specifically solving one problem, only. This justifies more complex technical and legal regulatory suggestions and solutions developed in this work.

6 CROSS-JURISDICTION

The previous chapters have set the grounds for the analysis of the legal problems of MIA policing tools. The focus is on those legal problems identified as most pressing by the experts interviewed for this work in chapter 3. These legal issues result from the technical abilities of MIA tools discussed in chapters 4 and 5, and their use as cyber-cops during investigations (see chapter 2 for more details on this). The specific problem analysed in this chapter is the cross-jurisdictional policing of the virtual living space by MIA tools.

The most basic function of the Internet, to connect computers and other ICT devices all over the world and enable the exchange and storage of data, causes profound problems for questions of jurisdiction. Country borders that for centuries restricted and influenced transactions between people and acts of the judiciary, legislative and executive state powers have been blurred by ICTs and the Internet.
This undermines traditional legal concepts, like the sovereignty and territoriality principles, which have been of fundamental importance for legislators and judges. Johnson and Post, among the first scholars highlighting this problem, argue that "global computer-based communications cut across territorial borders, are creating a new realm of human activity and undermining the feasibility-and legitimacy-of laws based on geographic boundaries."[477] However, thus far the scholarly debate of this problem has predominantly focused on the question whether states can and should prescribe legislation governing online activities causing harm inside their territory but originating from outside the state borders, or originating within their state territory but causing harm in other jurisdictions.[478] This scholarly debate has been accompanied

[477] D Johnson, D Post, "Law and Borders – The Rise of Law in Cyberspace" (1996) 48 *Stanford Law Review* 1367.
[478] See for the beginnings of this debate e.g. Johnson and Post, *ibid*, arguing that states generally should not attempt to apply geographically based regulations to Internet transactions. J L Goldsmith, "The Internet and the Abiding Significance of Territorial Sovereignty" (1998) 5 *Indiana Journal of Global Legal Studies* 475, and J L Goldsmith, "Against Cyberanarchy" (1998) 65 *University of Chicago Law Review* 1199, who challenges Johnson and Post's conclusions, arguing that online activities cutting across international borders are, from jurisdictional and choice-of-law perspectives, similar to other transnational transactions that states have successfully regulated for many years. Furthermore, see H H Perritt, "Cyberspace and State Sovereignty" (1997) 3 *Journal of International Legal Studies* 155; D L Burk, "Jurisdiction in a World Without Borders" (1997) 1:3 *Virginia Journal of Law and Technology* 1522; J R

by judgments addressing the same problem of jurisdiction and the Internet. Most notably and probably best known is the case of Yahoo! Inc. being sued in France over content stored on US servers.[479] Here, the Tribunal de Grande Instance in Paris handed down a judgment in favour of the plaintiffs LICRA and UEJF (two French anti-racist organisations), which had sued Yahoo! Inc., a US cooperation, and its French subsidiaries for allowing Internet users from France to buy Nazi memorabilia via Yahoo websites.[480] The court found that Yahoo! Inc. had committed "a manifestly illegal disturbance" (comparable to a nuisance) under the *French New Code of Civil Procedure*, which in turn was based on *the French Criminal Code* and the offence of distributing Nazi memorabilia. The court rejected all Yahoo! Inc.'s arguments against the court's competence (among others, that the content was located on a server in California). The court found that harm was suffered on French territory, and therefore ordered Yahoo! Inc. to prevent access from French territory to the Nazi memorabilia, which was backed by a penalty of 1000,000 francs per day for non-compliance. This judgment was unsuccessfully challenged by Yahoo! Inc. in US courts.[481] While the details of the Yahoo! case are not relevant to this chapter, it serves to illustrate the focus of jurisprudence with regard to jurisdiction problems in relation to the Internet and other ICT technologies, and highlights the insecurities of the legislative and judicative about this matter.

Reidenberg, "Technology and Internet Jurisdiction" (2005) 153 *University of Pennsylvania Law Review* 1951; A Thierer, C W Crews (eds) *Who rules the net?: Internet governance and jurisdiction* (Massachusetts: Cato Institute, 2003); U Kohl, note 14, for an extensive overview of the discussion; J Hörnle, "The Jurisdictional Challenge of the Internet" in L Edwards, C Waelde (eds) *Law and the Internet* (3rd edition Hart publishing, 2009) 121.

[479] LICRA v *Yahoo! Inc and Yahoo France* (Tribunal de Grande Instance de Paris, 22 May 200), affirmed in LICRA and UEJF v *Yahoo! Inc and Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000).

[480] See e.g. M Reiman, "Introduction: The *Yahoo!* Case and Conflict of Laws in the Cyberage" (2003) 24 *Michigan Journal of International Law* 663; H M Watt, "Yahoo! Cyber-Collision of Cultures: Who Regulates?" (2003) 24 *Michigan Journal of International Law* 673; U Kohl, "Yahoo! – But No Hooray! for the International Online Community" (2001) 75 *Australian Law Journal* 401, for a debate of this judgment.

[481] Yahoo! Inc. v LICRA and UEJF, 433 F 3d 1199 (9th Cir. 2006); reversing Yahoo! Inc. v LICRA and UEJF, 145 F Supp 2d 1168 (ND Cal. 2001) (finding in favour of personal jurisdiction); Yahoo! Inc. v LICRA and UEJF, 169 F Supp 2d 1181 (ND Cal. 2001) (finding in favour of ripeness of the suit, and the unenforceability of the French order based on the First Amendment), Yahoo! Incc. v LICRA and UEJF, 379 F 3d 1120 (9th Cir. 2004) (personal jurisdiction reversed). The US Supreme Court declined to hear an appeal on 30 May 2006: LICRA v Yahoo! Inc., 126 S.Ct 2332 (Mem) (2006).

Relevant for this thesis, however, is a different jurisdictional problem that arises from the use of MIA tools by police and other authorities. It is not the issue of a state seeking to *regulate* extraterritorial conduct having effect within its borders, but a state seeking to *investigate* that conduct. This issue has thus far received little attention by scholars and lawmakers. However, new investigation technologies and powers make this a pressing issue.

This problem is mainly rooted in the different concepts of mobility, as analysed above in chapter 5.[482] To illustrate this problem better, a short case scenario is introduced. This scenario highlights the differences between traditional police work and investigations conducted deploying MIA technologies, and shows how this difference can raise jurisdictional problems.

Traditionally, the investigation of a suspect can involve the physical observation of the suspect to monitor his movements and investigate his network of people. Furthermore, it can involve the monitoring and interception of his telephone calls, as well as the communication in his living space, car and, under certain circumstances, working space. In addition, investigators can obtain background information about the suspect from government databases and records.

This can be followed, if certain legal pre-requisites are fulfilled, by a physical search of the living space and working space of the suspect. At this stage, investigators can seize documents and ICTs to access data and information relevant to the investigation. Such a traditional investigation is bound to the parameters of the offline world. Investigators can only follow suspects as long as they remain within the boundaries of their sovereign territory. These boundaries are clearly marked (most obviously in the case of country borders, within one country, for example, by signs announcing the beginning of a new district or city), and an unlawful crossing of these would be obvious (for example, police officers wearing a wrong uniform or featuring the wrong identity card). Furthermore, the infrastructure necessary to undertake investigations (access to workspace, ability to obtain warrants etc) does not exist outside an investigator's territory and physical distance is a constraint. Thus, traditionally investigations are shaped and restricted by the boundaries of territory and country borders.

[482] See p. 132ff.

Legislation regulating investigations has equally been shaped by these factors. Multilateral and bilateral treaties, and letters rogatory are products of the need to seek and provide assistance to investigators of other territories.

The use of MIA tools changes the nature of investigations. Cyber-cops policing the virtual living space are limited by other factors than their offline counterparts. Their activities are restricted by the encryption of files, password protection of email accounts, and the quality of the Internet connection of the target ICT device. Nation borders, however, are not a restriction for the policing activities of cyber-cops.
A suspect from Germany, for example, could use a Google Gmail email account, and therefore have his emails stored on a server in the US. Cloud computing applications enable users to work using software stored remotely on servers in a country different to the one they reside in.[483] Their own computer is merely an access portal and all data is stored remotely on different servers. Hence, investigators deploying MIA tools could - consciously or unconsciously -investigate data of a suspect located in a different sovereign territory. Factors that would prevent investigators from crossing national borders in the offline world are obsolete online, and physical distance is not a decisive factor any longer. Furthermore, the rise in portable ICT devices leads to the risk of suspects moving devices that are infiltrated by MIA software tools across national borders, thereby causing investigations to be undertaken in the foreign jurisdiction.

Hence, the advances in ICT research and the introduction of new investigative powers have led to the possibility (and need) to undertake cross-border investigations of digital data.
The question is whether existing legislation and traditional international law principles allow for, and are sufficient and satisfactory to, regulate cross-border investigations of the virtual living space given that online data can be easily and quickly deleted and amended, and rapid actions are therefore necessary.

This chapter examines the challenges for traditional concepts of sovereignty and territoriality that are caused by cross-border investigations of the virtual living space,

[483] On a most basic level, cloud computing is the delivery of computing services (computation, data access, software and storage services). For an introduction to cloud computing see e.g. M Armbrust et al., "A View of Cloud Computing" (2010) 53:4 *Communications of the ACM*, 50-58.

and establishes whether the necessary legal instruments exist to regulate these adequately and sufficiently.

In section 6.1 the foundations of the relevant international law principles are introduced. Section 6.2 examines the traditional mechanisms of cross-jurisdictional legal assistance and examines in how far these are applicable to cyber-investigations of the virtual living space by MIA tools. Section 6.3 explores the legality of cross-border investigations beyond the traditional mechanisms of legal assistance. In section 6.4 a solution for the cross-jurisdictional activities of MIA tools is outlined. Section 6.5 concludes with the main findings of this chapter.

6.1 Sovereignty and Territoriality

The decisive question of this chapter is whether cross-border activities during investigations of the virtual living space by MIA tools are consistent with international principles of jurisdiction, and other international legislation and treaties. To answer this question a closer examination of the concept of jurisdiction, and related principles is necessary. It is important to establish certain background principles of international law that highlight why the Internet and ICT technologies present difficulties for investigators in general, and why cross-jurisdictional cyber-investigations by MIA tools present a challenge for these principles in particular.

The rules of jurisdiction in international law have always been closely linked to the concept of territory.[484] The foundation for international law is grounded in geographical considerations. That is, states occupy definite portions of the earth's surface, within which their governments exercise jurisdiction over persons and property to the exclusion of other states.[485] As Steinberger finds, "the control over a state's territory is not just a consequence of statehood but also an essential attribute."[486] Thus the notion of territory is elementary to the understanding of international law principles of jurisdiction. On a most basic level, the territoriality principle dictates that states have jurisdiction over acts that occur in their territory, as

[484] U Kohl, see note 14, at 8.
[485] C C Joyner, *International Law in the 21st Century: Rules for Global Governance* (Lanham, MD: Rowman & Littlefield Publishing, 2005) 43.
[486] H Steinberger, "Sovereignty" in R Bernhardt (ed.), *Encyclopedia of Public International Law* (1987), Vol.10, 397, 413.

a corollary of their territorial sovereignty.[487] In international criminal law, "the territorial theory takes the position that criminal jurisdiction depends upon the place of perpetration. That is, the action on whose territory the crime was committed has jurisdiction of the offense."[488] Thus the weight of the territorial principle differs, depending on the different aspects of jurisdiction that are at issue.[489]

Jurisdiction is a vague term and has many different meanings, thus no definite definition of this concept exists. As Leflar, among others has cautioned, "about all that can be done about it is to try to be sure of the sense in which it is being used at any given time."[490] From a historical linguistic perspective the word jurisdiction stems from the Latin term *juris dictio*, meaning the 'administration of justice'. [491] This meaning is still valid. However, it is critical to differentiate the purely domestic meaning of this concept from the international one. In the domestic sense, it usually refers to the right of one state organ over another one, or one federal state over another one, to take actions in respect of a particular matter, as defined by constitutional law.[492] In the international context, however, this concept refers to the regulatory competence rights between different states. This chapter is only concerned with the latter meaning of the concept: competence issues over regulatory questions between states.

Generally, three types of jurisdiction can be differentiated: *prescriptive jurisdiction*, *adjudicative jurisdiction*, and *enforcement jurisdiction*.[493]

Prescriptive jurisdiction refers to the authority of a state to establish and prescribe criminal and regulatory sanctions, thus the authority to make laws. It is therefore also referred to as legislative jurisdiction.[494]

Adjudicative jurisdiction refers to the authority of states to subject persons or things to the process of its courts whether or not the state is a party to the proceedings.[495]

---

[487] M Hayashi, "The Rules of Jurisdiction in Public International Law" in M Dunn, S F Krishna-Hensel, V Mauer (eds) *The Resurgence of the State: Trends and Processes in Cyberspace Governance* (Aldershot: Ashgate Publishing Ltd, 2007) 59 (61).

[488] R M Perkins, "The Territorial Principle in Criminal Law" (1970) 22 *Hastings Law Journal* 1155.

[489] M Hayashi, note 487.

[490] R Leflar, *American Conflicts Law* (3rd edition, Indianapolis: Bobbs-Merrill, 1977) 3.

[491] I Shearer, "Jurisdiction", in S Blay, R Piotrowicz, M Tsamenyi (eds.), *Public International Law – An Australian Perspective* (2nd edition, Melbourne: Oxford University Press, 2005) 154.

[492] Kohl, see note 14, at 14; K C Randall, "Universal Jurisdiction Under International Law" (1988) 66 *Texas Law Review*, 785.

[493] B A Boczek, *International Law: A Dictionary* (Lanham, Md.: Scarecrow Press, 2005) 77.

[494] Ibid.

Enforcement jurisdiction refers to the authority of a state to induce or compel compliance with its law or to punish non-compliance through courts (in which case it constitutes an aspect of adjudication) or resort to executive action, including physical interference, seizure of property, and similar actions.[496]

Malanczuk highlights why it is important to differentiate between these three groups of powers, and particularly between the second and third: "if a man commits a murder in England and escapes to France, the English courts have jurisdiction to try him, but the English police cannot enter French territory and arrest him there; they must request the French authorities to arrest him and to surrender him for trial in England."[497]
This example underlines the argument made above, that states generally have jurisdiction over acts that occur in their own territory. Thus as a general rule, states have a duty to respect the territorial sovereignty of other states.[498]

However, international law permits in some circumstances the application of the forum state's laws to activities carried on elsewhere. Several doctrines exist under which a state can prescribe laws governing extraterritorial conduct.[499]
Of prime importance for this chapter is the principle that a state is justified in regulating conduct that has harmful *effects* within its territory (the effects doctrine).[500]

---

[495] Ibid.
[496] Ibid.
[497] P Malanczuk, *Akehurst's Modern Introduction to International Law* (London: Routledge, 1997) 109.
[498] R Jennings, A Watts (eds.), *I Oppenheim's International Law* (9th edition, Longmans, 1992) 421.
[499] For the purpose of this chapter, it is not relevant to discuss all of these principles in detail. In addition to the "effects" principle discussed in the text, states can potentially assert extraterritorial jurisdiction based on the *universality principle* (permitting states to enforce sanctions against crimes that have an independent basis in international law, such as genocide), the *nationality principle* (which permits states to regulate the conduct of its nationals wherever they are), the *protective principle* (permitting states to regulate extraterritorial activities that threaten its local security), and the *passive personality principle* (allowing states to exercise jurisdiction over any person injuring one of its nationals). See for more details e.g. R Higgins, *Problems and Process: International Law and How We Use It* (Oxford: Clarendon Press; New York: Oxford University Press, 1994) 56; J Clough, *Principles of Cybercrime* (Cambridge, UK; New York: Cambridge University Press, 2010) 407; T Hillier, *Sourcebook on Public International Law* (London ; Sydney : Cavendish, 1998) 275 ff.
[500] See e.g. J Goldsmith, "Unilateral Regulation of the Internet: A Modest Defence" (2000) 11 *European Journal of International Law*, 135, 138 (stating that it is well accepted today that international law permits a nation to regulate the harmful local effects of foreign conduct); J J Paust, "Federal Jurisdiction Over Extraterritorial Acts of Terrorism and Nonimmunity for Foreign Violators of International Law Under the FSIA and the Act of State Doctrine" (1983) 23

The rational behind this doctrine is the need to protect national economic interests. The effects doctrine was first clearly stated in the Alcoa decision (*US v Aluminium Co of America* (1945)).[501] While other states first objected to the United States's application of its economic regulations, such as antitrust laws, to extraterritorial conduct, the principle is now generally accepted.[502] Thus under certain circumstances, international law doctrines allow states to *prescribe* rules limiting certain extraterritorial conduct. However, returning to the brief example above, the enforcement of a states' law outside its territory- whether through actions of its courts or actions of its executive officials- is not permissible under international law.[503]

Despite this, there are many cases where states have claimed the right to their own law enforcement abroad,[504] such as in the case of the kidnapping of Adolf Eichmann in Argentina by Israeli agents. In 1960, Israeli Mossad agents kidnapped the Nazi criminal Adolf Eichmann in Argentina, and took him to Israel for trial, where he was later sentenced to death and executed.[505] The abduction of Eichmann was neither discussed with, nor approved by the Argentinean state. As a result, a long international dispute between Argentina and Israel evolved, with Argentina claiming that the illicit and clandestine transfer of Eichmann to Israel constituted a violation of Argentine sovereignty.[506]

Another example is the kidnapping in the Alvarez-Machain case by US agents.[507] Humberto Alvarez Machain was kidnapped in Mexico by US agents, and brought to trial in the US for allegedly being involved in the kidnapping, torture, and murder of the US

Virginia Journal of International Law, 191; O Schachter, *International Law in Theory and Practice* (Dordrecht, The Netherlands; Boston: M. Nijhoff Publishers, 1991) 264.

[501] (1945) 148 F 28 147. Here, the US Second Circuit Court of Appeals stated that any state may impose liabilities, even upon persons not within its allegiance, for conduct outside its borders that has consequences within its border which the state reprehends.

[502] T Hillier, note 499, at 277; H G Maier, "Extraterritorial Jurisdiction at a Crossroads: an Intersection Between Public and Private International Law" (1982) 76 *American Journal of International Law*, 280, 294.

[503] See generally, J A Bush, "How Did We Get Here? Foreign Abduction after Alvarez-Machain" (1993) 45:4 *Stanford Law Review*, 939.

[504] See e.g. P Malanczuk, note 497, at 110 for a listing.

[505] See e.g. R Rein, *Argentine Jews or Jewish Argentines?: Essays on Ethnicity, Identity, and Diaspora* (Leiden, Netherlands: Martinus Nijhoff, 2010) 170; M Lippman, "Genocide: The Trial of Adolf Eichmann and the Quest for Global Justice" (2002) 8 *Buffalo Human Rights Law Review*, 45.

[506] M Lippman, note ibid, at 58, also for a detailed account of the dispute.

[507] United States v Alvarez-Machain, 946 F.2d 1466 (9th Cir. 1991), rev'd, 112 S. Ct. 2188 (1992).

agent Enrique Camarena Salazar in Mexico. He was later acquitted.[508] This case equally caused an international dispute between US and Mexico over the violation of Mexico's sovereignty.

These examples demonstrate that while states sometimes try to enforce their own law on foreign territory, this generally constitutes violations of the principles of territorial integrity and non-intervention.[509]

Generally, no state has the authority to infringe the territorial integrity of another state in order to investigate a crime, or apprehend an alleged criminal.[510]

Hence, to summarise, under international law states have under certain preconditions the right to prescribe laws regulating and limiting certain extraterritorial conduct. However under no circumstances have states the power to conduct a law enforcement investigation within the territory of another state without that state's permission. Thus the territoriality principle is absolute in the case of enforcement jurisdiction, whereas it can be restricted in the case of legislative jurisdiction. Under international law, investigators are therefore limited to operate within their designated territory.

As highlighted in the brief case scenario in the introductory part of this chapter (5), traditionally the borders of this territory are obvious, and investigators are unlikely to (accidentally) cross these. However, MIA tools investigating the virtual living space are not restricted by these territorial borders and, given the infrastructure of the Internet, are likely to undertake cross-jurisdictional activities.

Hence the question is whether such cross-jurisdictional activities, for example the search and seizure of digital data during an online search of a suspect in a different jurisdiction, qualifies as an infringement of the territoriality principle, and therefore violates international law and would be improper.

---

[508] For more details on the case see e.g. J A Bush, note 503; M J Matorin, "Unchaining the Law: The Legality of Extraterritorial Abduction in Lieu of Extradition" (1992) 41:4 *Duke Law Journal*, 907.

[509] There can be, under certain circumstances, exceptions to this rule under the self-defence doctrine. Article 51 of the Charter of the United Nations, for example, recognises an "inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations." Charter of the United Nations Art 51, 59 Stat 1031, Treaty Ser No 993 (1945). See also Jennings and Watts, note 21, at 421 stating that "the justification of self-defence for action which onvolves the violation of another state's territory is an exception to the general duty of all states to respect the territorial sovereignty of other states".

[510] P Malanczuk, note 497, at 110.

This question, however, would be irrelevant if mechanisms between states have been developed to adequately deal with the gap between their ability to prescribe laws governing extraterritorial conduct and their inability to investigate this, and if such mechanisms could be applied to the extra-jurisdictional investigation of the virtual living space by MIA tools.

The following section therefore analyses whether mechanisms have been developed, and in how far these are applicable and adequate to regulate such cross-jurisdictional investigative actions.

6.2 Mechanisms of Legal Assistance

The need for monitoring suspects, or seizing evidence in other states is not novel. As a result, mechanisms have been developed addressing this need, while respecting the territoriality principal of the other state. In this section, these mechanisms are analysed, and it is examined whether these are applicable to cross-jurisdictional investigations of the virtual living space by MIA tools, and particularly online searches of ICTs.

6.2.1 Letters Rogatory

One of the traditional mechanisms developed to serve states seeking evidence from other states in both civil and criminal matters are *Letters Rogatory*. Letters Rogatory are requests for evidence issued by a court in one country, submitted through diplomatic channels and seeking the assistance of a court in another country.[511] They provide a mechanism for nations to share and request criminal information. The Letters Rogatory process involves one country's judicial authority writing a formal request to the counterpart authority in a different country for legal assistance with a single specific criminal activity. In the US, for example, the Letters Rogatory process is authorised under Title 28 USC, 1781- 82.[512]

---

[511] B Zagaris, *International White Collar Crime: Cases and Materials* (Cambridge, UK: Cambridge University Press, 2010) 275.

[512] M Goodman, "International Dimensions of Cybercrime" in S Gosh, E Turrini (eds) *Cybercrimes: A Multidisciplinary Analysis* (Berlin, Heidelberg: Springer-Verlag, 2010) 311-339, 322.

However, Letters Rogatory can be of limited use. Zagaris points out that these are executed solely on the basis of comity.[513] This means that requests can be refused, or delayed as deemed appropriate because the nation receiving the request is under no obligation to comply. The average processing time of such a request can be up to two years.[514] This long processing time is also caused by the many difficult procedural requirements necessary. Letters Rogatory must be made through the courts in both countries with the involvement of various foreign ministries, justice ministries, and in some cases embassies.[515]

Already for traditional investigations, this mechanism was only of real value if the information requested was solely to confirm already existing evidence, a fast receipt of the information was not crucial, and there was no risk of loss of the requested evidence during the processing of the letter rogatory. However, for investigations of the virtual living space, a timely recovery of the evidence is of high importance. Digital data can easily be removed, altered, or destroyed, and therefore lost for investigators.[516] Furthermore, as the time span increases, there is a growing risk of the offender finding out about the investigation against him and benefiting from the ease with which data of evidentiary value may be deleted.[517]

Thus Letters Rogatory are hardly promising for investigations of the virtual living space.

6.2.2 Mutual Legal Assistance Treaties

The limits of Letters Rogatory have led to the development of other mechanisms to ensure that states have access to extraterritorial evidence in criminal matters. Most notably among these mechanisms are treaties on mutual legal assistance in criminal matters. These treaties regulate that contracting parties shall provide assistance in both criminal investigations and proceedings. These agreements exist in form of

---

[513] B Zagaris, "United States Treaties on Mutual Assistance in Criminal Matters" in M C Bassiouni (ed) *International Criminal Law: Multilateral and Bilateral Enforcement Mechanisms* ((Leiden, Netherlands: Martinus Nijhoff, 2008), 385.

[514] N Seitz, "Transborder Search: A new Perspective in Law Enforcement?" (2005) 23 *Yale Journal of Law and Technology*, 23, 28.

[515] B Zagaris, note 513, at 386.

[516] Y Uzunay, D Incebacak, K Bicakci, "Towards Trustable Digital Evidence with PKIDEV: PKI Based Digital Evidence Verification Model" in A Blyth, I Sutherland (eds.) *EC2ND 2006: Proceedings of the Second European Conference on Computer Network Defense, in conjunction with the First Workshop on Digital Forensics and Incident Analysis* (London: Springer, 2007), 105.

[517] W Bär, *Der Zugriff auf Computerdaten im Strafverfahren* (Köln: Heymanns Verlag, 1992) 41.

bilateral treaties between two states, and multilateral treaties between a number of states.

A good example for the latter category, which is also most relevant for this chapter and will therefore serve as the prime example of multilateral treaties here,[518] is the *European Convention on Mutual Assistance in Criminal Matters* of the Council of Europe and its two additional protocols, which also includes non EU-member States.[519]

The states party to this Convention have agreed to grant each other the widest possible assistance in criminal matters.[520] While the treaty considers letters rogatory as one of the main tools to seek assistance, with some exceptions it obligates the parties to carry out such requests.[521] States have retained the right to make declarations and reservations to the treaty, and most states have made use of this right. Such declarations are, for example, made in relation to the specification of Article 3 of the Convention, which states that a request for mutual legal assistance must be made by a judicial authority. Most countries have made declarations to the effect that they recognise members of the judiciary, as well as officers from public prosecutor's department as judicial authorities.[522] Thus the content and extent of these declarations does not limit the general scope and aim of the Convention. Generally, the Convention is not limited by an exclusive list of types of assistance, however, some examples, such as the search and seizure of evidence, questioning of witnesses, and the exchange of information from judicial records are given. This means that the Convention is relatively neutral as to what type of assistance can be sought and provided.

---

[518] For a full account and discussion of other multilateral treaties see e.g. C Joubert, *Judicial Control of Foreign Evidence in Comparative Perspective* (Amsterdam, Netherlands: Rozenberg Publishers, 2005).

[519] *European Convention on Mutual Assistance in Criminal Matters* (hereafter the Convention), entered into force June 12, 1962, European Treaty Series No. 30. This convention is presently in force between Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom (as of 29/09/2010), see Council of Europe, Chart showing Signatures and Ratifications of Council of Europe Conventions and Agreements, at http://conventions.coe.int/treaty/Commun/ListeParGroupe.asp?GR=1&MA=20&CM=15&CL=ENG; *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters* of 17.03.1978 (ETS No. 99); *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters* of 08.11.2001 (ETS No. 182).

[520] Article 1.1 of the Convention.

[521] Article 3.1 of the Convention.

[522] C Joubert, note 518, at 89.

This treaty has recently been updated by the *2000 EU Convention on Mutual Assistance in Criminal Matters* and its two protocols between the member states of the European Union.[523] These documents supplement and build on the *1959 Council of Europe Convention on Mutual Assistance in Criminal Matters* by developing and modernising existing provisions governing mutual assistance. An example for such a modernisation is the introduction of provisions with regard to the interception of telecommunications.[524] However, the Convention is still not implemented in all EU Member States.

In addition to these multilateral treaties, bilateral treaties between two states exist, containing similar obligations like the above-discussed Convention. These are manifold and there is neither space nor necessity to discuss any of these in great detail here. Instead one example of a bilateral agreement is discussed here, to provide an overview of the scope of these agreements. This enables an evaluation of their effectiveness and suitability to be applied to mutual assistance matters relating to the virtual living space and digital data.

The US is not party to the Council of Europe Convention, and thus one bilateral agreement between the US and another state is depicted here to include this jurisdiction into the analysis.

The US was particularly interested in establishing agreements containing similar obligations to those included in the Council of Europe Convention with other states, after this was ratified in 1962. As a result, the US entered into negotiations with Switzerland that culminated the signing of the first bilateral mutual legal assistance treaty in 1973.[525] The two states signatory to this treaty therein agreed to afford each other mutual assistance during investigations or court proceedings, the return of any objects, articles, or other property or assets belonging to the requesting state, and proceedings concerning compensation for damages suffered by a person through unjustified detention as a result of actions taken pursuant to the treaty.[526] Thus the scope of the mutual assistance in this case is not as broad as the one of the European

[523] OJ C197, 12 July 2000. One protocol provides for mutual assistance in relation to bank accounts and banking transactions; the other improves and supplements the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters and its additional Protocol.
[524] See Articles 18-22 of the Convention.
[525] See Treaty with the Swiss Confederation on Mutual Assistance in Criminal Matters, Senate Executive Report 94-29, 94th Cong, 2d Sess 1 (1976); Treaty on Mutual Assistance in Criminal Matters, US-Switzerland, 27 UST 2019, TIAS No 8302 (1977).
[526] US-Switzerland Treaty, note 532, Article 1.

Convention. The treaty equally defines, though is not limited to, certain types of assistance. These are, for example, the ascertaining of the whereabouts and addresses of persons, the taking of a testimony or statement of persons, and the authentication of documents. In addition, the treaty specifies that states are requested to designate a central authority to expeditiously process assistance requests, and that requests must be executed in a manner consistent with their own laws.[527] While the Swiss-US treaty is the longest and most complicated of any of the mutual assistance treaties presently negotiated by the US, all provide for a similar range of assistance in criminal matters.[528]

Thus both, bilateral and multilateral treaties are an improvement to letters rogatory because they better specify the duties and responsibilities of signatory states. Furthermore, they are binding, thus assistance has to be provided upon request. However, the procedural process that needs to be undergone to request assistance is cumbersome and time-consuming. Formal requests for specified information, and oftentimes judicial authorisation are required.[529] These mutual assistance mechanisms are thus ill suited to deal with requests of Internet related investigations, where timely assistance and responses are crucial. In particular for investigations by MIA tools, where the software tool itself makes the decisions about accessing data and monitoring communications.

6.2.3 International Police Cooperation

In addition to the mutual legal assistance treaties, mechanisms are in place for cooperation between states at police level. Of greatest importance for this chapter are two associations of police forces: the *International Criminal Police Organization* (Interpol) on international level, and the *European Police Office* (Europol) on European level. The aim of both organisations is to provide and promote cross-border cooperation between criminal police authorities, and establish procedures to facilitate assistance during criminal investigations.

---

[527] This means, for example, if Switzerland requests the US to conduct a search within their territory, this must meet the requirements of the Fourth Amendment and other applicable US law.

[528] A Ellis, R L Pisani, "The United States Treaties on Mutual Assistance in Criminal Matters: A Conparative Analysis" (1985) 19 *International Lawyer*, 189, 198.

[529] I Brown, D Korff, "Terrorism and the Proportionality of Internet Surveillance" (2009) 6:2 *European Journal of Criminology*, 119, 124.

Interpol was originally formed in Vienna in 1923, and has steadily grown in membership but never substantially changed in form or objectives.[530]
Interpol is not a supranational police agency with investigative powers or an organisation sanctioned by an international governing body such as the United Nations. Rather, it is a cooperative network formed independently among police agencies to foster collaboration and provide assistance in police work across nations.[531] To achieve this, Interpol has established a central headquarters, located in Lyon, France, with specialised bureaus, so-called National Central Bureaus (NCB), in the countries of participating police agencies.[532] At present, Interpol counts 188 member countries.[533] Interpol's primary challenge has been to develop a system that allows for the sharing and dissemination of information among the member countries. To achieve this, Interpol has set up a variety of databases (for example, the Interpol weapons and electronic tracking system [IWETS]), which member countries can access, as well as introduced the communication system I-24/7, which enables police officers a secure communication channel with other police forces all over the world at any time.[534]

Europol is the criminal police agency of the European Union. The establishment of Europol was agreed in the *1992 Treaty on European Union*, also referred to as the *Maastricht Treaty*. However, the *Europol Convention*, which officially formed the organisation, was not ratified by all member states until 1998. Europol commenced its full activities on 1 July 1999.[535] The Convention is still the instrument governing the constitution of Europol, but has been significantly amended since its establishment.[536] Europol has its headquarters in The Hague, where it allocates its resources. The aim of Europol is to assist law enforcement authorities of Member States in their fight against serious forms of organised crime.[537] Its objectives are to improve the effectiveness of

---

[530] M Deflem, "Bureaucratization and Social Control: Historical Foundations of International Police Cooperation" (2000) 34:3 *Law & Society Review*, 739-778.
[531] M Deflem, "Global Rule of Law or Global Rule of Law Enforcement? International Police Cooperation and Counterterrorism" (2006) 603 *Law, Society, and Democracy: Comparative Perspectives*, 240-251.
[532] Ibid.
[533] See http://www.interpol.int/public/icpo/default.asp.
[534] Interpol, "General Secretariat 2002 Activity Report", available online at http://www.interpol.int/content/download/773/6131/version/5/file/agn72r01.pdf.
[535] House of Lords, European Union Committee, *Europol: Coordinating the Fight Against Serious and Organised Crime*, 29th Report of Session 2007-2008, 12.
[536] Ibid.
[537] See http://www.europol.europa.eu/index.asp?page=ataglance&language=.

and cooperation among the police authorities of the EU member states. Similar to the structure of Interpol, Europol is not an executive police force with autonomous investigative powers.[538] Deflem lists its core activities as: (a) the facilitation of information exchange among the so-called Europol Liaison Officers, who are seconded to the Europol headquarters in The Hague by the member states to act as representatives of their national police; (b) the supply of operational analysis in support of relevant police operations conducted by the member states; (c) the drawing up of strategic reports, such as threat assessments, and crime analyses on the basis of information supplied by police of the member states or generated at Europol headquarters; and (d) the offering of technical support for police investigations conducted in the EU member states.[539]

Comparably with Interpol, Europol's most important instruments are databases and communication systems. The Europol Computer System facilitates the exchange and analysis of data. This is supplemented by two databases: the EU Customs Information System that provides customs agencies with the ability to exchange information on smuggling, and the FIDE, which provides information on subjects involved in a criminal investigation.[540]

Both associations have significantly improved mutual assistance during criminal investigations. However, both Interpol and Europol suffer from the lack of enforcement power and the fact that neither of these associations is a supranational force. The cooperation of the member states with the associations is voluntary, which means that crucial information is oftentimes not shared.

An indication of a lack of cooperation among European member states was revealed after the Madrid bombings, when French police officials were outraged over the fact that their Spanish counterparts refused to share information on the types of explosives that had been used.[541]

As with other mutual assistance measures discussed above, the mechanisms in place to facilitate cross-jurisdictional cooperation at police level are of somewhat limited

---

[538] M Deflem, "Europol and the Policing of International Terrorism: Counter-Terrorism in a Global Perspective" (2006) 23:3 *Justice Quarterly*, 336-359.

[539] Ibid, at 342.

[540] Ibid.

[541] R Kupchinsky, "Intelligence and Police Coordination in the EU" (2004) 4:11 *RFE/RL Organized Crime and Terrorism Watch*.

benefit to investigations involving the Internet, and in particular where MIA tools are used. The main focus of cooperation of existing measures is on the collective accumulation of data. However, data relevant for cross-jurisdictional investigations of the virtual living space, and particularly online searches, is usually fluctuant and pertains to one specific person, who has not necessarily been a suspect previously. Thus data is unlikely to be stored in any of the databases, and rapid assistance in form of searches and seizures is not part of the activities supported by either Interpol or Europol. In addition, as indicated above, cooperation is not mandatory, which poses the same problems discussed above for Letters Rogatory.

The analysis of existing mechanisms of legal assistance has shown that mechanisms obligating states to assist one another in extraterritorial investigations are in place. However, it has also highlighted that traditional mechanisms, governing the mutual assistance in criminal matters while respecting the territorial sovereignty of other states are ill suited for the regulation of mutual assistance requests for cross-jurisdictional investigations by MIA tools. The technological advancements, and the development of the Internet and related ICT technologies significantly change the nature of mutual assistance requests. The searching and seizing of digital data requires speedy actions, which are in stark contrast to the formal and lengthy procedures required for the mutual assistance requests under existing mechanisms.
While the number of transnational crimes has historically been rising, cases where the relevant evidence is primarily located abroad were still the exception rather than the rule. Thus traditional mechanisms of mutual assistance were sufficient to deal with these requests. However, during investigations of the virtual living space and of ICT devices, investigators will often find that crucial evidence is located in a different jurisdiction. This might even be the case when a crime has no other international element, as described in the brief example at the beginning of this chapter. The use of free email accounts and cloud computing applications means that relevant data is stored on servers outside of the jurisdiction of the investigating country. Thus the physical location of digital evidence depends upon the fortuity of network architecture, rather then the focus of the crime.

Particularly those working for law enforcement units have also confirmed the problem of mutual assistance requests for digital evidence. Here, it was pointed out that existing mechanisms governing such requests are unapt to govern cooperation among states.

The interviewees highlighted two aspects. Firstly, it was pointed out that traditional channels (mechanisms described above) for obtaining evidence abroad are not flexible and fast enough in cases of Internet investigations. Secondly, it was stated that from a technical point of view, cross-jurisdictional searches and the seizure of digital evidence abroad could be undertaken without any problems. Thus a dichotomy exists between what is technically possible and legally allowed. It was also said that the legal uncertainty negatively impacts the work of officers, and sometimes halts the development of new investigation technologies.

Therefore, the widespread of the Internet and the increased relevance of digital data for investigations creates new legal challenges for cooperation among law enforcement agents from different jurisdictions. Thus the question posed in section 6.1 of this chapter, whether cross-border searches using MIA tools qualify as an infringement of the territoriality principle, and therefore violate international law and would be improper needs to be addressed.

6.3 Beyond Traditional Legal Assistance Mechanisms

The question whether cross-jurisdictional investigations are legal is far from straightforward. Most countries do not have any specific legislation regulating the issue of cybercrime jurisdiction, and therefore rely on the traditional mechanisms described above, which leads to unsatisfying results as has been highlighted in the previous part of this chapter. Those countries that do have cybercrime jurisdiction legislation in place can often be placed at the other extreme end. Malaysia, for example, has provisions stating that it can theoretically claim jurisdiction for any cybercrime committed anywhere.[542]

To answer the question whether cross-jurisdictional investigations of the virtual living space are permissible under international law, a closer analysis of the nature of these investigations needs to be undertaken.

Generally, a cross-jurisdictional investigation of the virtual living space refers to the searching and seizure of digital data located in a jurisdiction other than the one of the acting state. These activities are usually carried out remotely from the home

[542] B-J Koops, S Brenner, "Cybercrime Jurisdiction – An Introduction" in B-J Koops, S Brenner (eds.) *Cybercrime and Jursidiction – An International Survey* (The Hague: Asser Press, 2006) 3.

jurisdiction of the investigating authority. This is true for both cases, investigations conducted by human officers and those by MIA tools.
However, the type of data to be investigated can differ. Two different types need to be distinguished: a) freely accessible data, and b) non-freely accessible data.
In the first case, this can, for example, be data located on openly accessible websites, or on online fora that can be accessed with guest accounts, as well as communication data that is openly accessible, such as open chat rooms.
The latter case is data that is located on private accounts (such as email accounts), or on the hard drive of private computers, as well as communication data solely intended for one or more specified persons, such as conversations on Voice-over-IP (VOIP) applications.

The following analysis of the legality of cross-jurisdictional investigations differentiates between these two types of data. This is important because the potential impact on the person to be investigated differs significantly whether freely accessible data, or non-freely accessible data about him is investigated. In the latter case, the potential privacy and data protection implications can be much more significant, and thus states have a higher interest to protect their citizens and therefore claim jurisdiction over any investigative acts. Additionally, the technical steps required for the accessing of protected data are considerably more complex, which means the investigative actions required are more intrusive.

6.3.1 Cross-Jurisdictional Investigations of Freely Accessible Data

6.3.1.1 Literature Debate

Those authors who have written on the subject have discussed cross-jurisdictional investigations of freely accessible digital data controversially.
A large number of scholars find that a cross-border search of openly accessible data is compatible with international principles of territory and sovereignty.[543] The reasoning for this stance, however, varies significantly.

[543] See e.g. P de Hert, "Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace – Whose Sovereignty is At Stake?" in B-J Koops, S Brenner (eds) *Cybercrime and Jurisdiction – An International Survey* (The Hague: Asser Press, 2006) 107, who states that he cannot see international law prohibiting police to consult foreign publicly-accessible files, newsgroups, or websites; N Seitz, note 514, at 33; M Germann, *Gefahrenabwehr und Strafverfolgung im Internet* (Berlin: Duncker & Humblot, 2000) 652.

Maybe the most forthright, de Hert, states without further explanation that the consultation of publicly available data on the Internet by police stored on foreign servers is uncontroversial and not problematic.[544]

Similarly, Goldsmith reasons that cross-jurisdictional investigations of freely accessible digital data are consistent with international principles of enforcement jurisdiction.[545] However, he supports his position by arguing that states have always exercised a certain amount of extraterritorial regulation, by exercising territorial power in ways that changed behaviour in other nations, which he refers to as indirect extraterritorial regulation.[546] Indirect extraterritorial regulation works through force (or threat of force) that states impose nationally, but which has also an effect on behaviour in another state's jurisdiction. For example, if an offshore person or firm causes local harm from abroad, the local government can indirectly regulate the harmful foreign activity by threatening to seize the offshore firm's local assets.

Technological advancements, as Goldsmith argues, have merely expanded indirect extraterritorial regulatory activities but not introduced them. Thus his argument is that such activities have always existed, and are therefore commonly accepted and customary. He compares cross-jurisdictional searches with the use of orbital reconnaissance satellites.[547] However, he also cautions that such cross-border searches can negatively impact on privacy and free speech rights of the target person.[548] For the case of freely accessible data these concerns can be neglected because only data the target person voluntarily reveals is accessed.

Coming to the same conclusion, but with a different argumentation, Graf, the then-senior prosecutor at the German Federal Court of Justice (BGH) argues that cross-jurisdictional searches of freely accessible digital data need to be allowed for reasons of practicability.[549] He believes that a reliable conclusion about the location of the computer cannot be drawn based on the Uniform Resource Locator (URL). Thus he reasons that cross-jurisdictional investigations of freely accessible data are a necessity to conduct any kind of Internet related investigations, and therefore must be allowed.

---

[544] De Hert, ibid, at 107.

[545] J L Goldsmith, "The Internet and the Legitimacy of Remote Cross-Border Searches" (2001) *The University of Chicago Legal Forum* 103-118, 104.

[546] Ibid, at 110.

[547] Ibid, at 114.

[548] Ibid, at 105.

[549] J P Graf, "Befugnisse und Grenzen der Ermittlungsbehörden" *Deutsches Polizeiblatt* 4/2001, 6, 9.

Jofer, who also agrees that cross-jurisdictional searches of freely accessible data should be allowed, argues that the traditional concept for defining an infringement of the territoriality principle is unsuitable here.[550]
Traditionally, the territoriality principle is violated if a law enforcement agent enters the territory of another state to conduct investigative measures.
However, as Jofer argues, in the case of cross-jurisdictional investigations of freely accessible digital data this is not the case. Law enforcement officers are conducting the investigative measures from their own territory. Jofer finds that by tolerating the Internet as an institution, the state has permitted data traffic in its national territory, which includes the retrieval of data from abroad.[551]

Jofer's argument that tolerating the Internet as an institution necessarily means that all data traffic within a state's territory needs to be accepted is difficult, particularly because often data traffic is prompted from a different jurisdiction. This would mean that any form of data traffic, whether malicious or harmful, would have to be accepted.

A better approach in the author's opinion is to focus on the intensity of the violation. The relevant criterion is not where the violation occurs, but only the intensity of the violation of the legal framework of the country where the data is retrieved. The degree of intensity depends on whether the rights of a foreign citizen are breached by the acts. In case of openly accessible data, the acting agents are not breaching any rights of citizens, because no acts of deception, or other coercive measures are necessary to access the data. This approach equally acknowledges how the Internet has changed policing, but avoids the potentially difficult generalisation of Jofer's approach.

Some scholars disagree and, discussing cross-jurisdictional searches, reject the permissibility of the measure, even in the case of freely accessible digital data.
Gercke states that the territoriality principle prohibits any form of extraterritorial activity by law enforcement agents in foreign territory, regardless of whether or not it is a measure that requires the physical intrusion of an agent.[552] Due to this absolute

---

[550] R Jofer, *Strafverfolgung im Internet: Phänomenologie und Bekämpfung kriminellen Verhaltens in internationalen Computernetzen* (Frankfurt am Main: Lang, 1999) 193.
[551] Ibid.
[552] M Gercke, *Rechtswidrige Inhalte im Internet: eine Diskussion ausgewählter Problemfelder des Internet-Strafrechts unter Berücksichtigung strafprozessualer Aspekte* (Aachen: Hochschulschrift, 2000) 171.

interpretation of the territoriality principle, he comes to the conclusion that also the mere accessing of publicly accessible websites constitutes a violation, even though it does not establish an intrusion due to the lack of intensity of the measure.[553] This is because the territoriality and sovereignty principles are violated by any kind of extraterritorial actions, not only those establishing an intrusion.[554]

Coming to the same conclusion, Bär argues that the new possibilities the networked environment of the Internet offers for extraterritorial data processing would be used as an "extended arm" by law enforcement agencies in the case of cross-jurisdictional searches, and the intensity of such actions would therefore be comparable to the physical presence of agents in foreign territory.[555]

Similarly, Spatscheck reasons that the right of the state to independently decide whether or not investigations shall be undertaken in its sovereign territory must not be circumvented with the help of advanced communication technologies.[556]

One central question in the above-depicted debate whether cross-jurisdictional searches of freely accessible data constitute a violation of the territoriality principle is in how far such actions are comparable to traditional investigative and monitoring measures, such as the use of satellites. The opposing authors all refer to the fact that new technologies should not offer ways to circumvent existing legal concepts, such as the territoriality concept, and agree that cross-jurisdictional searches go beyond the possibilities existing investigation measures offer. Whereas according to conventional wisdom the mere accessing of publicly accessible extraterritorial data on the Internet is not an action significantly different from traditional measures, such as the consulting of foreign newspapers, or the monitoring of foreign territory from a domestic position, such as by border police or by satellite.

6.3.1.2 Legislation

Hardly any international legislation dealing with matters of Internet regulation, and in particular questions of jurisdiction exists. Nevertheless, the potential issue of cross-jurisdictional cyber-investigations and the resulting jurisdiction problem has been

---

[553] Ibid.

[554] U Sieber, in T Hoeren, U Sieber (eds) *Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs* (München: Beck, 2000) Nr. 19 RN 736.

[555] Bär, note 517, at 235.

[556] R Spatscheck, "Steuerhinterziehung im Internet" (2000) 28 *Strafverteidiger Forum*, 1, 6.

discussed at the European level as early as 1995. The Council of Europe engaged in discussions about this topic under the working title of 'transborder network search' as part of the preparation for *Recommendation R (95) 13 on Problems of Criminal Procedure Law connected with Information Technology*.[557] In the absence of any concrete national or international case law, it remained undecided whether a state whose law enforcement agents would access digital data on the territory of another state, would interfere with the internal affairs of the latter state.[558] It was recommended at the time that states should enter into mutual agreements as to what extent cross- jurisdictional investigations could be authorised. However, as Kaspersen reports, two states involved in the negotiations of the *Recommendation (95) 13* attempted to conclude such a bilateral agreement, but failed because of the sensitivity and complexity of the issue.[559]

Due to the importance of the topic, the Council of Europe recommended at the time that generally access to data stored on international networks should be permitted in cases where immediate action is necessary.[560]

Thus the discussions of this topic surrounding the negotiations of the *Recommendation (95) 13* did not deliver any concrete results at the time.

The topic was also discussed at a ministerial conference of the G-8 countries on combating transnational organised crime.[561] Here, recommendations and principles in relation to cross- jurisdictional investigations of publicly accessible data, similar to those of the Council of Europe, were developed. It was stated that the accessing of publicly available (open source) data, regardless of where the data is geographically located, could be undertaken without the consent of the affected state.[562]

---

[557] Council of Europe, Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law connected with Information Technology (adopted 11 September 1995).

[558] H W K Kaspersen, "Jurisdiction in the Cybercrime Convention" in B-J Koops, S Brenner (eds) *Cybercrime and Jursidiction – An International Survey* (The Hague: Asser Press, 2006) 19.

[559] Ibid, at footnote 24.

[560] Council of Europe, at 565, Appendix § VII (17): The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.

[561] Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow, October 1999, at http://www.g7.utoronto.ca/adhoc/crime99.htm.

[562] Ibid, Annex 1 (6a).).

The issue was debated again during the discussions of the 2001 *Council of Europe Convention on Cybercrime* (CoC).[563] The CoC was developed in response to a growing concern about the adequacy of legislation criminalising certain activities occurring over computer networks.[564] It has thus far been signed by 46 countries, including the US, Canada and Japan, and was ratified by 30 countries. The CoC contains a number of rules dealing with questions of jurisdiction (Article 22 CoC), which reflect the application of a number of different jurisdiction principles. The aim of Article 22 is to ensure that parties to the CoC establish the required level of extraterritorial jurisdiction.[565] However, these jurisdictional rules do not regulate extraterritorial investigative actions. During the discussions of the CoC the importance as well as difficulties of cross-jurisdictional investigations were highlighted again. It was stated that extraterritorial investigations had to be considered a violation of international law and could only be permissible if a specific regulation would be drafted and included in the CoC.[566] As a result of these discussions, Article 32 was drafted and included into the CoC.[567] According to Article 32 (a) CoC, a state may access publicly accessible data that is in the 'open source'. This is the case if data can be accessed without the need for further procedures, such as logins with passwords. States are allowed to retrieve this data independently of the geographical location of its storage medium.[568]

The CoC therefore establishes a legal basis explicitly allowing the extraterritorial investigation of openly accessible data. While not all states have ratified the CoC (Germany and the UK are examples), it provides at the very least a model that states should adapt.

---

[563] Council of Europe, *Convention on Cybercrime*, Budapest, 23 November 2001 (CETS 185), http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.
[564] Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime (Final Draft, released June 29, 2001), A2, at http://www.justice.gov/criminal/cybercrime/COEFAQs.htm.
[565] Kaspersen, note 558, at 10, see also here for a more detailed analysis of the background and meaning of Article 22 CoC.
[566] Ibid, at 20.
[567] Article 32 is the result of lengthy and controversial discussions, which will be further discussed in the next section of this thesis, where these are of more relevance.
[568] Article 32 (a) of the CoC reads "A Party may, without the authorization of another Party, (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically."

In addition, given the fact that consent about the legality of cross-jurisdictional investigations of openly accessible data was reached during the discussions of the CoC it appears a valid option that this could be recognised and legit under customary international law.

Customary international law is binding even for nations that have not formally accepted law regulating the matter in question.[569] Customary international law is regarded as a primary form of international law.[570] It is defined as "the collection of international behavioural regularities that nations over time come to view as binding as a matter of law."[571] Kelly defines customary law as "a set of norms derived from practice that is invested with binding authority by the relevant community." He goes on to add that customary law "is not mere practice or habitual behaviour, rather it is a normative order consisting of rights and duties abstracted from practice."[572] Arend and Beck note that customary international law is developed as a result of state behaviour. They state that "if, over a period of time, states begin to act in a certain way and come to regard that behaviour as being required by law, a norm of customary law has been developed."[573]

There are two central pre-requisites for the development of customary law: state practice and *opinio juris*. According to Roberts, "state practice refers to general and consistent practice by states, while *opinio juris* means that the practice is followed out of a belief of legal obligation."[574]

Doehring finds that the central pre-requisite is that "a behaviour is practiced over a certain period of time and be considered justifiable by all involved parties."[575]

The examination of openly accessible extraterritorial websites for investigative purposes has been and is being practiced daily without states taking offense at this

---

[569] J W Dellapenna, "The Internet and Public International Law: Law in a Shrinking World: The Interaction of Science and Technology with International Law" (1999-2000) 88:4 *Kentucky Law Journal*, 809, 841.

[570] See e.g. J L Goldsmith, E A Posner, "A Theory of Customary International Law" (1999) 66:4 *The University of Chicago Law Review*, 1113, 1116.

[571] Ibid.

[572] J P Kelly, "The Twilight of Customary International Law" (2000) 40:2 *Virginia Journal of International Law*, 449, 461.

[573] A C Arend, R J Beck, *International Law and the Use of Force: Beyond the UN charter Paradigm* (London: Routledge, 1993), 6-7.

[574] A E Roberts, "Traditional and Modern Approaches to Customary International Law: A Reconciliation" (2001) 95:4 *The American Journal of International Law*, 757.

[575] K Doehring, *Völkerrecht* (Heidelberg: C.F. Müller, 2004) §4, 286.

practice.[576] Thus this behaviour has and is being practiced regularly and by different states. This implies that the cross-jurisdictional searching and monitoring of openly accessible websites is not only tolerated but also considered lawful. Cross-jurisdictional investigations of openly accessible data are therefore permissible under customary international law.

No case law that could confirm this has, to the best knowledge of the author, been generated.

Therefore, it can be summarised as a first result that cross-jurisdictional investigations of openly accessible data are permissible. On this specific issue, relative consent exists between conventional wisdom in literature and existing international regulations. As indicated above, the author agrees that the examination of extraterritorial openly accessible data should be permissible. The very nature of the Internet supports the accessibility of websites from any place in the world. The geographical location of the server storing the data is irrelevant. Thus, the accessing of freely accessible data on the Internet by law enforcement agencies should not be determined by this factor.

6.3.2 Cross-Jurisdictional Investigations of Protected Data

Generally, information relevant for criminal investigations is seldom published on openly accessible websites. In most cases, relevant data is stored on hard disks of personal computers, distributed via emails, or published on access-restricted websites and in online fora. Chapter 2 has highlighted that the main interest of (German) law enforcement authorities lies indeed in the use of MIA tools for the investigation and monitoring of protected data, since online searches primarily target data stored on ICTs, and thus protected from public access.

More important is therefore the question whether searches of extraterritorial, protected data are permissible under international law.

---

[576] See for a recent example the UK police monitoring websites for threats against the Pope during his UK visit, A Arco, "Police Monitor Internet for Threats Against the Pope During his Visit" (2010) *Catholic Herald*, available online at http://www.catholicherald.co.uk/news/2010/07/21/police-are-monitoring-internet-for-threats-against-the-pope/; Switzerland is monitoring the Inernet, N Luethi, "Cybercops nehmen Dienst wieder auf" (2003) *Telepolis*, http://www.heise.de/tp/r4/artikel/13/13911/1.html.

6.3.2.1 Literature Debate

The opinions in the literature are considerably more univocal on this topic than in the case of openly accessible data. The strongly prevalent view holds that cross-border searches of protected data are impermissible.[577] While again the argumentation of the authors differs slightly as will be highlighted below, the reason for most of the authors coming to the same conclusion is that extraterritorial investigations of access-restricted and private data fundamentally differ from those of openly accessible data. The investigation and retrieval of such data requires, as illustrated in chapters 4 and 5 of this thesis, intrusive acts that can significantly influence and alter the network and server where the data is stored, as well as the computer or other ICT device that is being infiltrated. Such actions have a much higher potential to interfere with the sovereignty of a state, and therefore violate international law.

De Hert finds that "the accessing of foreign secured files and data amounts to plain judicial hacking, and is therefore impermissible."[578]
Wilske and Schiller note that "especially concerning measures in aid of enforcement of criminal law, a state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the state, given by duly authorised officials of that state."[579] From this they conclude that "as a consequence for any 'cybersearch' measure targeting a hard drive or other restricted data in the course of a law enforcement investigation the consent of the territorial sovereign in which the target is located is required. Otherwise, the action violates the territoriality principle and other international law principles."[580]
Ringel agrees with this, stating that most states would regard such actions as a violation of their sovereignty in a transnational investigation that has not been permitted.[581]

---

[577] A selection of opinions is provided here, however, this is by no means the entire literature debate on the topic.
[578] De Hert, note 543, at 107.
[579] S Wilske, T Schiller, "International Jurisdiction in Cyberspace: Which States May Regulate the Internet?" (1997) 50 *Federal Communications Law Journal*, 171.
[580] Ibid, at 174.
[581] K Ringel, "Rechtsprobleme beim Zugriff auf EDV-Beweismittel" (1998) 3 *Deutsches Polizeiblatt*, 14, 17.

Bellia argues along the same lines, stating "remote cross-border searches conducted without the permission of the state in which the searched data is stored generally will violate customary international law."[582]

The reasoning behind these arguments is, as analysed above under 6.1, that no state has enforcement jurisdiction over another country. Thus no law enforcement officer has the right to conduct activities in another states territory.

A smaller number of authors argue that cross-border investigations are permissible under international law even in the case of protected data.

The most drastic are von Briehl and Ehlscheid, who argue that extraterritorial cross-border searches of private and access-restricted data should generally be allowed, because the intensity of the intrusion is so low, given the fact that no law enforcement agent enters the foreign territory, that the cross-border search cannot be considered an infringement of foreign sovereignty.[583] This view completely ignores that access to private, protected data *per se* constitutes a violation of a person's data protection rights, no matter whether access occurs from within or outside of a state's territory. Such actions are therefore reserved to the nation's law enforcement and thus violate sovereignty rights if conducted by other nations.

Similarly, Sofaer et al. in their proposal for an international convention on cybercrime and terrorism suggest "state parties shall be free to engage in reasonable, electronic methods of investigation, even if such conduct results in transfer of electronic signals into the territory of other states."[584] However, they add that affected states should be informed of such actions as soon as practicable.
Sussman, who is more cautious about the permissibility of such actions, reasons that extraterritorial cross-border searches of non-openly accessible data are likely to occur, and should therefore be permissible under exigent circumstances.[585]

---

[582] P L Bellia, "Chasing Bits Across Borders" (2001) 35 *University of Chicago Legal Forum*, 80.
[583] O G von Briel, D Ehlscheid, *Steuerstrafrecht* (Bonn: Deutscher Anwaltverlag, 2001) 451.
[584] A Sofaer et al., "A Proposal for an International Convention on Cybercrime and Terrorism" (2000) *Centre for International Security and Cooperation, Stanford University*, Article 6 (5), available online at http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf .
[585] M Sussmann, "The Critical Challenges from International High-Tech and Computer-related Crime at the Millenium" (1999) 9 *Duke Journal of Computer & International Law*, 451, 471.

Goldsmith argues along the same lines. He reasons that technological developments will make cross-border searches of access-restricted data necessary, however, sensible limits to such actions will emerge in form of customary international law principles.[586] He states further that states will limit their actions because aggressive cross-border searches can easily be reciprocated. He also suggests that this will be an incentive for states to develop cooperative principles.[587]

The problem with these arguments of the minority opinion is that all authors fail to recognise that cross-jurisdictional investigations of protected digital data are highly intrusive measures, comparable to the search of a living space in the physical world.[588] This, however, according to prevailing opinion, violates international law if it is conducted by a foreign agent.

6.3.2.2 Legislation

As noted above in the discussion of the permissibility of cross-border searches of openly accessible data (6.3.1), this measure has been discussed among legislators, and some international legislation regulating cross-border searches exists. The question is, however, whether existing legislation permits cross-border searches of non-publicly accessible data.

The Council of Europe's *1995 Recommendation R (95) 13* on Problems of Criminal Procedural Law Connected with Information Technology (*Recommendation*) indicates that such searches should be permitted in emergency cases.[589] However, the *Recommendation* does not provide a legal basis for such measures. On the contrary, the Recommendation highlights the need for the establishment of an *unambiguous* legal basis, to avoid violations of state sovereignty or international law. The use of the term unambiguous highlights the fact that cross-border searches of access restricted data are considered to be a problematic issue, and require a unified approach and sound legal basis to be permissible under international law. This is emphasised by the fact that at the time, this measure was seen as the *ultima ratio* and envisaged to be only applicable in cases of emergency. In the discussions preceding the *Recommendation*,

[586] Goldsmith, note 570, at 116.
[587] Goldsmith, note 570, at 117.
[588] See chapter 2, p. 34 for a discussion of this.
[589] Council of Europe, *Recommendation No. R (95) 13* of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law connected with Information Technology (adopted 11 September 1995); Appendix § VII (17) see for details text of note 565.

however, no unity could be established, and hence no legal basis was integrated into the *Recommendations*.[590]

As analysed above, the *2001 Council of Europe Convention on Cybercrime* (CoC) includes provisions on the permissibility of cross-border searches. Article 32 (a) determines that parties to the Convention may access publicly accessible data.[591] The drafters of the CoC discussed the issue whether a country is permitted to access private and access-restricted data stored in another country without seeking mutual assistance at length.[592]

However, in again consulting the CoC, it becomes clear that contrary to the issue of access to freely accessible data, the access to protected data remains unregulated in the CoC. Article 32 (b) CoC only establishes that in cases where consent of the legally authorised person exists, law enforcement agencies are permitted to access stored data.[593] Thus for this alternative, it is irrelevant whether the data is secured by access codes or security measures, as long as the person referred to has the right of lawful access, irrespective of the fact that other persons also may have access rights. Remarkably, neither the COC, nor the explanatory report provide a legal definition of "authorised person". The explanatory report generally states that the authorised person must be defined according to the circumstances and the applicable law of each individual case.[594] Further, the person in question must have the right to disclose the data, which means that the operation cannot be undertaken if the person is bound by a duty of secrecy.[595] The explanatory report provides an example, illustrating that an ISP could possibly be regarded as such an authorised person, if the data is stored in another country by this body.[596]

---

[590] Kaspersen, note 558.

[591] See note 555.

[592] Council of Europe, Explanatory Report, http://conventions.coe.int/treaty/en/reports/html/185.htm, at para. 293.

[593] Article 32 (b) of the CoC reads "A Party may, without the authorization of another Party, [...] (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

[594] Council of Europe, note 599, at 294.

[595] Kaspersen, note 558, at 21.

[596] Council of Europe, note 599, para. 294 reads: "Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article."

The term 'authorised person' is therefore not restricted to the person directly affected by the measure. It may be a third person in cases where the decision to store data abroad stems from another person or body other than the affected person, and this third person has *de facto* access to the data. However, importantly, Article 32 (b) is not a means for coercion to demand the retrieval of data from a third person, such as an ISP.

During the negotiations of the CoC a third alternative to Article 32 (a,b) was discussed but not included in the final text of the Convention. This alternative provided that a cross-border search should be permissible in cases of emergencies, such as in matters of life and death concerning law enforcement officers, undercover agents, and witnesses.[597] However, during the course of the negotiations no common understanding of emergency cases could be established, and participating states felt unable to commit to binding provisions.[598] It was also felt that further experiences should be gained and further discussions held before other alternatives could be introduced.[599] Thus no further provision was included into the CoC.

Consequently, Article 32 CoC constitutes the lowest common denominator on which states involved in the establishment of the Convention could agree. Thus the logical conclusion is that cross-jurisdictional are impermissible under international law. However, this conclusion is averted by Article 39 CoC, which states that none of the provisions laid down in the Convention shall affect or impair other rights.[600] Therefore, neither the permissibility, nor the impermissibility of cross-jurisdictional investigations of protected data can be concluded from Article 32 CoC. However, what can be concluded is that the CoC does not explicitly allow the cross-jurisdictional investigations of protected data.

The G-8, during its conference on combating transnational organised crime developed similar recommendations, finding that accessing, searching, copying, or seizing data stored on a computer system located in another state is permissible and can be conducted without the consent of the affected state, if acting in accordance with the

---

[597] Kaspersen, note 558, at 21.

[598] Seitz, note 514, at 47.

[599] de Hert, note 543, at 107.

[600] Article 39(3) CoC reads "Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party." See also Council of Europe, note 571, para. 293, ("stating that Article 39, paragraph 3 provides that other situations are neither authorized, nor precluded").

lawful and voluntary consent of a person who has the lawful authority to disclose the data.[601]

Thus under written international law cross-jurisdictional investigations of protected data are impermissible.

The focus is therefore on existing case law to establish whether such measures are permissible under customary international law. The incident that has become know as the *Gorshkov-Ivanov case*, constitutes a case in point.[602]Around the end of 1999, the FBI identified Russians Vasiliy Gorshkov and Alexey Ivanov as the hackers who had been breaking unauthorised into US businesses, including banks, credit card institutions, and internet service providers.[603] The offenders gained access to credit card numbers and other information about financial transactions and used these to commit fraud. The FBI created a bogus company called "Invita" located in Washington, allegedly specialising in security consultation for Internet firms. Invita offered jobs to both of the suspects, but demanded proof of their qualifications. To demonstrate their skills, and "interview" for the jobs, the FBI brought the hackers to Seattle. As part of the "interview" and to demonstrate their skills, they were asked to hack into a network set up by the FBI. [604] In doing so, they used laptops provided by the FBI to access Russian computers, where they kept hacking tools.[605] The FBI had installed a keylogger program on each of the laptops and the program recorded the usernames and passwords the hackers used to access their Russian computers.[606] Ivanov and Gorshov were arrested the same day. The FBI agents used the information retrieved by the keylogger program to access the Russian computers and download files they contained, including stolen credit card numbers and other evidence.[607] All this was done without obtaining a warrant. The two

---

[601] G-8, see note 561, Annex 1 (6b).

[602] See the resulting judgments of the incident: United States v Gorshkov, 2001 WL 1024026 (W.D. Wash. 2001); United States v Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001); For a summary of the case, and a detailed analysis of the technical aspects see, P Attfield, "United States v Gorshkov: Detailed Forensics and Case Study; Expert Witness Perspsective" (2005) *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering* (SSADFE'05), 3.

[603] United States v Gorshkov, 2001 WL 1024026 (W.D. Wash. 2001).

[604] Ibid.

[605] Ibid.

[606] Ibid.

[607] Ibid.

Russians were charged with multiple misdemeanours, and with the help of the data downloaded from Russia, both were convicted to fines and prison sentences.[608]

This is, to the best knowledge of the author, to date the only reported case where a court had to deal with the issue of cross-jurisdictional investigations of protected data. Primarily, the court focused in its judgment on the charges against the two Russian citizens. However, in connection with an attempt by Gorshkov to suppress the evidence obtained from the Russian computers, the court reasoned about the permissibility of cross-jurisdictional investigations of protected data. Gorshkov argued that the evidence obtained from Russian computers was the product of a search and seizure that (a) violated the Fourth Amendment and/or (b) violated Russian law.[609] However, the court denied the notion, arguing that the Fourth Amendment did not apply because it does not encompass extraterritorial searches directed at non-US citizens.[610] The court further held that the agents' actions did not violate Russian law and even if they did, it was no basis for suppressing evidence in a US proceeding.[611]

Russia felt that the FBI agents violated Russian sovereignty by conducting the cross-border search, and subsequently charged the agent primarily responsible for the intrusion with hacking and asked that he be turned over for trial. The US authorities did not comply with this request.

The conclusion that can be drawn from this judgment is that US authorities and the respective judges consider a cross-jurisdictional investigations of protected data to be permissible under international law in exceptional cases, such as the one on hand, where there was a perceived risk that the evidence might be deleted quickly. The United States Department of Justice (USDOJ) confirms this, stating that cross-jurisdictional investigations of computers (thus access-restricted data) can generally only be conducted with the consent of the foreign state,[612] however, in cases of

---

608 Ibid.

609 Ibid.

610 See S Brenner, "'Our'" Fourth Amendment", *CYB3RCRIM3*, 11.03.2006, available online at http://cyb3rcrim3.blogspot.com/2006/03/our-fourth-amendment.html, for a critical discussion of this argument.

611 United States v Gorshkov, 2001 WL 1024026 (W.D. Wash. 2001).

612 United States Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3rd edition, OLE Litigation series, 2009), 56, available online at http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.

emergency, such as a terrorist attack, a non- or pre-consensual cross-border search can be permissible.[613]

It can, however, also be concluded from this judgment that Russia does not agree with this. Russia considered the cross-border search conducted by US agents as a violation of their territorial sovereignty. This is demonstrated by Russia's lawsuit against the FBI agent. Thus Russia regards cross-jurisdictional investigations of protected data as impermissible under international law.

These conclusions are important for the question whether cross-jurisdictional investigations of protected data are permissible under customary international law. As established above under 6.3.1, for customary international law to develop, state practice and *opinio juris* are required, thus general and consistent practice by states, which is followed out of a belief of legal obligation.[614] These pre-requisites are not fulfilled, with Russia objecting to the measure. Therefore, even though no further case law exists on this matter, given Russias clear objection on the matter and also the consent of several states on this topic during the legislative discussions, it can be concluded that cross-border searches of restricted data are also impermissible under customary international law.

6.3.3 Cross-Jurisdictional Investigations of Protected Data by MIA Tools

The above arguments and discussions all assume that human officers conduct these cross-jurisdictional investigations of protected data. As discussed above,[615] MIA tools increasingly replace human officers for these cyber-investigations. Their abilities allow these tools to conduct the required actions without human intervention and supervision.

Thus, the question is whether it makes a difference under international law if cross-jurisdictional investigations of protected data are undertaken by pieces of software instead of human officers. Could these investigative actions be lawful because no human officer is directly involved in the cross-jurisdictional investigative activities?

As discussed above under 6.3.1.1, a violation of the territoriality principle can be determined according to the impact that the action has on the affected state's sovereign

[613] Ibid, at 58.
[614] Roberts, note 574.
[615] See chapters 1 and 2 for a discussion of this.

interests. Principally, the search of a hard disk or other protected data by foreign law enforcement has in essence the same effect as a traditional search of premises.[616] It is highly intrusive and potentially infringes privacy and data protection rights of the person concerned. Hence, this is a measure reserved to the sovereign law enforcement. Territorial sovereignty serves, inter alia, to protect the residents from physical persecution by other states.[617]

Thus in this case, the question is whether a cross-jurisdictional investigation of protected data by MIA tools converts the affront to sovereignty that a human police officer would cause when conducting these investigative actions from an intentional performance of sovereign functions on another state's territory into mere interference with the goals of a regulatory scheme, here the regulatory scheme designed to protect persons or property within its territory?

It could be argued that this is the case if a cross-jurisdictional investigation by MIA tools would be less invasive than one by a human officer.

As discussed in chapter 4, [618] MIA tools are more complex than common software products, which are heavily reliant on human input to function. MIA tools operate autonomously, without direct intervention by human operators.[619] They independently select computers and other ICTs, and the relevant data to search. Hence, no human officer necessarily knows of the cross-jurisdictional nature of the investigation. The question is whether this makes the act less invasive, and thus lawful.

As discussed above,[620] MIA tools can be regarded as quasi-officers, whose role goes beyond that of a mere tool (such as the keylogger in the case example above) assisting human officers in their work. However, thus far no legal status has been ascribed to these tools. This causes difficulties when it comes to classifying their acts in the context of legal concepts, such as sovereignty.

---

[616] See note 591.
[617] S T Bernardez, "Territorial Sovereignty" in R Bernhardt (ed) *Encyclopedia of Public International Law* (4th ed., North-Holland Publishing Co.: Amsterdam, 2000) 823, 827.
[618] See p. 104ff.
[619] See chapters 4 and 5 for a discussion of their abilities.
[620] See p. 9ff.

Their actions, however, mirror those of human officers. Just because software tools conduct the relevant investigative actions does not make these less invasive for the affected person. Ultimately, the aim is to collect protected data to use as evidence against the suspect. The potential for rights violations in the course of such an investigation is equally high if MIA tools conduct these investigations.

Thus the question is whether the fact that human officers do not make the decision to investigate cross-jurisdictional data and also do not know about this influences the permissibility of these actions. This could be the case if actions by MIA tools could not be attributed to authorities.

The question of liability of actions of intelligent technologies is one that has also arisen in related research areas, such as robotics, however, without a definitive result thus far.[621] The problem is again that the legal status of these tools has yet to be defined. However, as a principle, in criminal investigations a state should not be able to divert liability for actions because intelligent tools are deployed instead of human officers. Two analogies can assist to clarify this situation. Firstly, if human officers use technologies, such as bugs or keyloggers to assist their work all actions are attributed to the acting authority, even if the technology has, unwanted by the operator, caused harm.
Secondly, if authorities enter into public-private partnerships with private companies and these conduct certain acts normally executed by police officers (such as private security companies) their actions are attributable to the authority.[622]
These examples highlight that actions of MIA tools, as quasi-police officers acting on behalf of the authority, are in any case attributable to the authority deploying these tools. This is also the case if human operators do not know about the cross-jurisdictional nature of the investigation.
International legislation cannot be circumvented by deploying new technologies that are capable of replacing human officers for intrusive actions.

---

[621] See e.g. for a discussion of this E Schaerer, "Robots As Animals: A Framework for Liability and Responsibility in Human-Robot Interactions" (2009) *18th IEEE International Symposium on Robot and Human Interactive Communication*, 72-77; U Pagallo, "Killers, Fridges, and Slaves: A Legal Journey in Robotics" (2011) 26:4 *AI & Society*, 347-354.
[622] J Becker, "Rechtsrahmen für Public Private Partnerships" (2002) *Zeitschrift für Rechtspolitik*, 303-308.

Cross-jurisdictional investigations of digital data by MIA tools are therefore comparable to actions of human officers entering the territory of another state, and therefore violate the territorial sovereignty of the affected state, unless the state has agreed to the action.

It can therefore be concluded that under international law and existing jurisprudence, cross-jurisdictional investigations of digital data are impermissible (with the exception of those cases where consent is granted). Thus, international legislation confirms the views of conventional wisdom on this issue.

6.4 Cross-Border MIA Searches: An Outlook

The above analysis and discussion of the permissibility of cross-jurisdictional investigations has shown that these are under the existing international legal framework only permissible under certain circumstances.

The below figure visualises the different options.

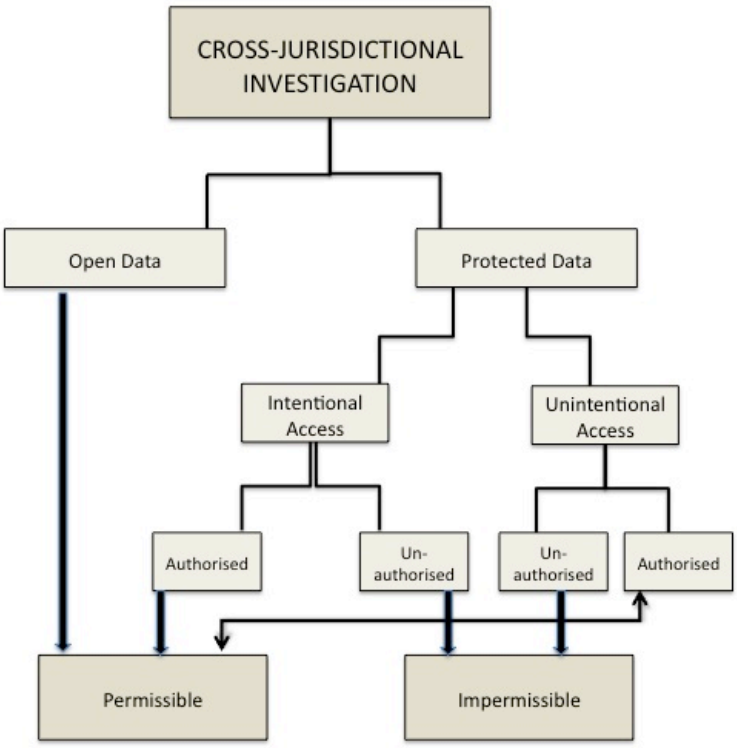

Figure 1: Permissibility of Cross-Jurisdictional Investigations

As shown, cross-jurisdictional investigations are permissible where investigators access data in the open domain, or have the explicit consent of an authorised person. However, previous chapters have shown that MIA tools are likely to be used for investigations of private and protected data, located on personal ICTs of suspects. Currently, states are not permitted to undertake such investigative actions of data located in other sovereign territories, even if they are acting in "good faith". In addition to the violation of international law principles, investigators could also violate national laws regulating access to computer systems,[623] and therefore make themselves liable for legal prosecution in the affected country.

Generally speaking, this is a favourable outcome. Using advanced technology instead of traditional methods should not circumvent existing legal practice. This could lead to far-reaching consequences, such as the Gorshkov and Ivanov case, where the US ignored international law principles, and thereby accepted that cross-border searches of restricted data are permissible in cases of emergency, and thus made itself liable to become a target for such actions by other nations. The recent Stuxnet case is another example that highlights the negative impact of circumventing existing legal practice and legislation.[624]

However, as highlighted above, digital data has a pronounced tendency to cross national borders, and is by nature evanescent. Additionally, the use of MIA tools by law enforcement will increase as highlighted in chapters 2 and 3, particularly because international bodies recommend the introduction of new software-based investigative powers, such as the online searching of computers.[625] Traditional methods of mutual legal assistance are, as discussed above, not adequate to assist law enforcement agents in cases of access to extraterritorial digital data. It is essential, therefore, to establish legal certainty, and define circumstances and conditions under which cross-jurisdictional investigations are permissible.

---

[623] Such as the *UK Computer Misuse Act 1990*.

[624] Falliere/Murchu/Chien, note 476.

[625] Council of the European Union, "Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime", 2987th Justice and Home Affairs Council meeting, 27 – 28 November 2008, available at http://www.ue2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf

The European Commission has announced in September 2010, that it wants to harmonise the laws of EU member states dealing with cyber attacks.[626] One of the action points outlined in the proposal is the improvement of European criminal justice/police cooperation by strengthening the existing structure of 24/7 contact points, including an obligation to answer within 8 hours to urgent requests. While the exact details of the proposed Directive, and in particular the extend to which matters of jurisdiction will be addressed, are at this point still very much unclear, this would be a great opportunity to address the problems surrounding cross-jurisdictional investigations of data by MIA tools.

However, the general question is how cross-jurisdictional investigations of protected data should be regulated, and whether these should be allowed at all. As has been discussed above, such acts are significantly infringing privacy and data protection rights of the targeted person, as well as sovereign rights of the affected state. The approach must be an outweighing of the interests and needs of the acting state (taking into consideration that the use of MIA tools will be much more common in the future) against the interests and rights of the affected state.

One key requirement that was mentioned by all the different views in literature, and during policy debates is the need for obtaining consent to cross-border searches of the affected state. Informing the affected state before any actions are undertaken is necessary and important to minimize the violation of international law. However, as discussed under 6.2, with regard to digital data and Internet investigations the process of gaining consent needs to be remodelled and more adequately tailored to cross-jurisdictional investigations by MIA tools. If a satisfying solution could be found for this issue, many of the doubts raised by the different countries would be resolved, and consent of policymakers on this topic achieved. This would enable the development of international legislation regulating such actions.
The unique abilities of MIA tools (as analysed and illustrated in chapters 4 and 5 of this thesis) could pose a solution to this issue. The advantage of software code is that

[626] European Commission, "Proposal for a Directive on Attacks against Information Systems, repealing the Framework Decision 2005/222/JHA, 30 September 2010, available online at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463&format=HTML&aged=0&language=EN&guiLanguage=en.

specific rules and commands can be implemented into the tool.[627] This approach, regulation through code, is analysed and discussed in detail in chapter 8. However, a brief outlook of how this approach could solve the issue in question is provided here. MIA tools could, for example, be designed to detect whether data is located within or outside of the territory of the operating country. This could, for example, be achieved by designing the tool to check IP addresses. Thus in cases where data, or the target ICT tool is identified by the MIA tool to be located in a different sovereign territory, a pre-defined procedure is set into motion. The MIA tool can initiate communication with a virtual police station, designed for this purpose.[628] At this point of contact, the MIA tool can communicate the request and specific details of the planned search. The software installed to reply to these requests can verify that such a search would be in line with existing legislation in the state, and allow or reject the request. Such a communication would take very little time, and no human officers would be required at this stage. In case of a rejection of the request, human officers could take over negotiations.

This, still somewhat futuristic scenario, would require all states to develop legislation regulating investigations of the virtual living space, such as the online search of computers, and define under which circumstances other states would be allowed to conduct such measures on their territory. Given the recent recommendation of the Council of Europe that member states should facilitate clandestine remote searches of computers of suspects, is a first indicator that more countries will consider introducing legislation dealing with this matter in the near future.[629]

6.5 Conclusion

Concluding, it can be summarised that cross-jurisdictional investigations of the virtual living space are only permissible under international law if freely accessible data is searched. The investigation of protected data located in a different jurisdiction violates international law, unless an authorised person approves the action. This is the case for both; investigations conducted by human officers and MIA tools.

---

[627] See e.g. Lessig, note 24; and the updated version L Lessig, *Code Version 2.0* (New York: Basic Books, 2006). for a detailed discussion on how laws could be implemented into software.
[628] See e.g. M Valeri, "Europe's first 'Online Police Station'", (2006) presented at *6th Computer Law World Conference*, Edinburgh, for a discussion of a simpler version of such an institution.
[629] See note 627.

However, increasingly data located in the virtual living space is crucial for the success of investigations. The relevant data is mainly protected data stored on hard drives of suspects and exchanged during communications.[630]

MIA tools targeting such data are oblivious to where the data is stored. As highlighted by the short case scenario under 6 above, country borders no longer restrict the actions of these tools. Given the fluctuant nature of online data and the networked environment of the Internet, this is necessary. However, as shown in this chapter, this causes significant problems for the law.

The specific abilities of the new class of investigative technologies therefore profoundly challenge existing legal frameworks regulating investigations. The empirical research in chapter 3 suggested that this is the case, and this chapter has highlighted that the existing legal framework is inapt to adequately regulate actions of MIA tools for the specific case of cross-jurisdictional investigations of the virtual living space.

However, the unique abilities of the software code of MIA tools could constitute a solution for this problem. Just like human officers, MIA cyber-cops should obey to existing legislation and rules when conducting their investigative actions. The concept of regulation through code, as introduced in section 6.4 could enable tools to act accordingly. Chapters 8 and 9 explore this approach further.

[630] See chapter 2 for a discussion of the online searching method.

7 DOUBLE DIGITALITY

The previous chapters have highlighted that digital data is increasingly important for investigations, and particularly private and protected data stored on ICTs. For the investigation of this data and the policing of the virtual living space more frequently novel MIA tools are deployed.

The previous chapter has analysed how this challenges international laws regulating cross-jurisdictional investigations. Another pertinent problem identified by the interviewed experts is the use of the evidence collected by MIA tools for criminal proceedings.[631] This chapter focuses on this issue and analyses the particular problems of protected data seized from ICTs and the virtual living space by MIA tools.

This evidence collected by MIA tools is in digital format. This type of evidence is also referred to as 'digital evidence', 'electronic evidence', or 'computer evidence'.[632] The mere existence of these different concepts describing this type of evidence indicates that this class of evidence is significantly different from traditional evidence, and therefore raises particular problems and issues.

In addition, digital evidence seized by MIA tools raises another problem: the "double digital paradigm". This concept developed in this thesis refers to digital data that is seized by (digital) software from live systems.

A short case scenario is again introduced here, to better illustrate the differences between traditional physical and documentary evidence and digital evidence, and in particular digital evidence collected by MIA tools.

This case scenario highlights that existing legislation governing the collection and preservation of evidence during criminal investigations and procedures is challenged by digital evidence, and particularly if seized by MIA tools.

---

[631] See chapter 3, p. 79 ff.

[632] For the purpose of this chapter, the author chooses to refer to this type of evidence as 'digital evidence'.

Traditionally, if investigators gain a warrant to search the premises of a suspect and seize relevant documents and other items of (potentially) evidentiary value, this includes the physical entering of human officers of the suspect's flat or other relevant premises (such as his work place). These officers are trained to undertake search and seizure procedures in compliance with existing legislation regulating these actions. In addition, these officers can serve as eyewitnesses during court proceedings, testifying that certain circumstances were as stated in reports. The evidence that is traditionally seized during such procedures is documentary and physical evidence. Hence, depending on the crime the suspect is accused of, this could be documents, weapons, clothing, or other relevant items.

Photographs of the premises and the location of the seized items may be taken, and the evidence is catalogued and taken away. These procedures ensure that during court proceedings, it can be proven beyond reasonable doubt that the seized evidence was indeed found at the suspect's premises, and has not been tampered with after the seizure. To ensure this, the original pieces of documentary and physical evidence are presented and examined during the court proceedings.

Additionally, documentary and physical evidence can help to connect a crime to a suspect beyond a reasonable doubt. For example, documents with distinctive handwriting, a specific weapon, or clothing with traces of DNA can create a powerful tangible connection between a suspect and a crime. Thus physical evidence has an important probative value, and is of significant value to investigations.

What then is the difference between documentary and physical evidence, and digital evidence, and in particular the search and seizure of digital evidence by MIA tools?

The brief scenario on digital evidence is divided into two parts. Firstly, a scenario is described that highlights the problems and differences between digital and physical evidence a). This is followed by a variation to this scenario, highlighting the specific problems with digital evidence collected by MIA tools b).

a) The widespread use of ICTs means that investigators are frequently faced with evidence in digital form. Thus, when investigators gain a warrant to search a suspect's premises and seize evidence (potentially) relevant to a crime, upon entering the premises of the suspect they are frequently faced with the problem that documents and data of potential importance are stored on computers and other ICTs, as well as the

virtual living space. These devices have replaced traditional files and personal calendars as means for producing and storing documents. In addition, the increase in online communication means that emails have largely replaced traditional letters as the mainstream communication means. Thus, emails of evidentiary value could be stored on the email account of the suspect.

This means that relevant documents are stored in digital format on ICTs and the virtual living space and do not exist as physical documents. The search of a premise therefore requires the investigators to seize computers and other ICTs to search these for relevant documents and data. However, as opposed to documentary and physical evidence, digital evidence stored on ICTs cannot be inspected and catalogued at the premise. Relevant documents stored on ICTs in digital format are essentially consisting of zeros and ones in electronic format. Therefore, these documents are not readable by a human unless decoded by a program (such as Microsoft Word). This means that officers present during the search cannot testify in court that certain evidence was found at the scene, and therefore likely belonged to the suspect. The evidence is not the computer itself, but the data stored on its hard drive or on online accounts of the suspect.

To retrieve digital evidence from ICTs, these devices are seized and then inspected by forensic analysts.

Computer forensic experts have developed a detailed set of procedures that forensic analysts ordinarily follow when they seize and analyse ICTs.[633]

While the technical details are not important at this stage, the general structure of this analysis is relevant to show the differences between seizing digital evidence and physical evidence. As a first step, ICTs are seized by investigators at the scene, and returned to a government forensic laboratory for analysis.[634] At the forensic laboratory, as a first step a "bit-stream" or "mirror image" of the hard drive is generated.[635] The bit-stream copy is an exact duplicate, not just of the files, but of every single bit and byte stored on the drive.[636] The forensic analyst then performs his work on the copy rather than the original to ensure that the original is not be damaged or altered by the

---

[633] See generally B Nelson et al., *Guide to Computer Forensics and Investigations* (Boston, MA: Cengage Learning, 2009), surveying and explaining current computer forensics practices.

[634] Computer Crime and Intellectual Property Section, US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Office of Legal Education Executive Office for United States Attorneys, 2009), 76.

[635] M Meyers, M Rogers, "Computer Forensics: The Need for Standardization and Certification" (2004) 3:2 *International Journal of Digital Evidence*, 6.

[636] Ibid.

analyst's investigation. Thus, the original ICT device remains intact for court proceedings, should the need to compare the copy with the original occur.
A deviation of this procedure might be necessary if one of the ICT devices is still switched on during the seizure. Many modern computers have large amounts of Random Access Memory (RAM) where process context information, network state information, and much more are maintained. Once a system is powered down the immediate contents of that memory is lost and can never be completely recovered. So, when dealing with a crime or incident involving digital evidence, it may be necessary to perform operations on a system that contains evidence, especially in a networked environment.[637]
Therefore, one significant difference between the seizure of documentary and physical evidence, and the seizure of digital evidence that becomes obvious is that in the traditional investigative context, seizure implies the 'confiscation' or 'taking possession' of physical material for later inspection, which in itself constitutes the evidence. Whereas in the digital realm, seizure implies the 'confiscation' or 'taking possession' of a data storage medium, that may contain the evidence. The relevant (digital) evidence is very volatile, and can therefore be lost or altered almost immediately upon seizure. However, similarities exist in that specifically trained experts, who document every step of their activities and can testify in court what they have detected and where, undertake the procedures.

b) Search and seizure of digital data conducted by MIA tools, significantly changes the scenario. In this case, the first important difference to a traditional search and seizure of documentary and physical evidence is that no physical premise of a suspect is searched. The place of interest is the virtual living sphere of the suspect.[638] In addition, the operation is not conducted by a human officer, but rather by a piece of software programmed to execute certain actions. The search and seizure of the virtual living space of a suspect by MIA tools therefore entails the remote infiltration of an ICT tool to gain access to the data stored on it. Once this has been accomplished, the MIA tool searches for relevant data, copies this and returns it to the investigators. The entire process occurs without direct supervision or participation of a human officer, or forensic analyst. The tool operates autonomously.

---

[637] E Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and The Internet* (Amsterdam: Elsevier Academic Press, 3rd edition, 2011) 245.
[638] See chapter 2, p. 53 for a detailed discussion of this notion.

The search and seizure of data with MIA tools raises several issues as opposed to the traditional search of a premise. In addition to those identified above for the digital realm, no human officers are present, who could act as eyewitnesses after the operation. In addition, the data is seized from live systems. The ICT device (such as the computer) itself is not seized and examined by a forensic specialist according to widely recognised procedures. Thus no original system exists to verify the authenticity of the seized data. Even if the ICT tool is seized after the MIA tool has retrieved relevant data, the system will not be in the identical state it was in at the time of the search and seizure of the data.

This means that no physical source exists for later comparison with the admitted evidence. In other words, "a live image (or copy) can only be verified against itself from the point when acquisition occurred, whereas images of 'dead' machines can be verified against the original media".[639] More problematically, data can be manipulated. For example, as Nikkel points out, 'IP and MAC addresses can be spoofed, various protocol headers can be faked, and the content transmitted can be fabricated. Network traffic can be intercepted and modified during transit'.[640] Significantly, MIA tools are not primarily designed with evidence preservation in mind.[641]

The case of *R v Aaron Caffrey* highlights in particular how difficult it can be to prove the reliability of MIA tools and therefore the authenticity of the seized data.[642]

Caffrey was acquitted of a section 3(1) *Computer Misuse Act 1990* offence of causing unauthorised modifications of computer material, allegedly having gained unauthorised administrator rights to Web services on the Port of Houston computer by using a known exploit within Microsoft software. He claimed in his defence that hackers had used a Trojan virus to gain control over his computer and launch programs to hack into the Port of Houston computer. Although no traces of a Trojan virus were found on his computer and it was therefore highly unlikely that hackers had gained control over his computer, he was acquitted of the crime on the basis that the possibility that a Trojan virus had been installed on the computer and had destroyed itself, leaving no traces, could not be excluded. Since MIA tools are very similar in

---

[639] E E Kenneally, "Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection" (2005) 9:2 *UCLA Journal of Law and Technology*, 3.
[640] B J Nikkel, "Improving Evidence Acquisition from Live Network Sources" (2006) 3 *Digital Investigation*, 89.
[641] E Casey, A Stanley, "Tool Review – Remote Forensic Preservation and Examination Tools" (2004) 1 *Digital Investigation*, 284.
[642] E George, "UK Computer Misuse Act – The Trojan Virus Defence Regina v Aaron Caffrey, Southwark Crown Court, 17 October 2003" (2004) 1:2 *Digital Investigation*, 89.

nature to Trojan software,[643] this highlights the difficulties of proving that the MIA tool operated faultlessly during an investigation and, hence, that the evidence collected is reliable.

If a person is acquitted because of the mere possibility that a Trojan infected his computer, *a fortiori* an acquittal could be expected if it is known that a Trojan, albeit under police control, was operative – first because the police Trojan itself might have compromised the crime scene, second because it proves that the suspect's computer was vulnerable to attacks in principle. If the police were able to gain access, it is highly likely that the computer was vulnerable and, indeed, that some malware will have exploited this vulnerability.

These case scenarios have highlighted the fundamental differences between documentary and physical, and digital evidence. While a weapon on a physical crime scene remains the same after collection by police and inspection by experts and jury, and can at any time during the proceedings be used as an objective comparator for the claims made by either side, digital evidence potentially changes every time it is opened and viewed on a computer. In some sense, there is no 'enduring original' that can serve as an objective comparator.

The "double digital paradigm" pertinent to evidence seized by MIA tools challenges existing legislation regulating the search and seizure of evidence even further. Software code seizing software code from live systems stands in grave contrast to traditional procedures of physical objects by human officers.

Therefore, the question arises whether digital evidence seized by MIA tools would stand in court.

As mentioned elsewhere in this thesis,[644] the author has been a partner on two European projects dealing with this question.[645]

The first project in particular focused on determining whether digital evidence is admissible, and whether specific regulations dealing with this type of evidence exist. The project was comparative and empirical in nature. Experts from 16 member states

[643] See chapter 4 p. 93ff.

[644] See generally pp. 24 and 31, and p.77ff for a detailed discussion of the project.

[645] 1. "Admissibility of Electronic Evidence (A.E.E.C.)" project, and 2. "European Certificate on Cybercrime and Electronic Evidence (ECCE)" project. Both projects were financed by the European Commission under the Framework Program.

carried out an analysis of existing procedural legislation in their jurisdiction dealing with matters of (digital) evidence, and undertook interviews with legal professionals directly involved in the process of obtaining, analysing and presenting digital evidence in court (e.g. police officers, computer forensic analysts, lawyers, judges). The main findings of the project with regards to digital evidence were that no country had introduced specific legislation dealing with digital evidence at the time of the study (2005-2006). The interviewees indicated that existing legislation was applied analogously to the new type of evidence at the time of the interviews.
About half of the interviewees, however, indicated that the introduction of new legislation (or the amendment of existing) to specifically regulate digital evidence would be beneficial. Generally, all interviewees agreed that the current situation was unsatisfactory, and could lead to much confusion and legal uncertainty. Most of the interviewees also stressed that there was a significant lack of technical knowledge among the legal experts.[646]

The second project was a continuation of the first, focusing on addressing the issues highlighted by the experts interviewed for the first project. These were in particular the lack of knowledge about legal and technical issues relating to cybercrime and digital evidence among members of the judiciary and lawyers. Thus the project aimed at developing the first European Certificate on Cybercrime and Electronic Evidence. The first stage of the project consisted of developing a training program on cybercrime and electronic evidence, which incorporated knowledge about the technical and legal issues pertaining to these topics. The second stage of the project consisted of training seminars in 11 European and 3 Latin American countries for judges, prosecutors and lawyers, who could gain the certificate at the end of the course. The development of the teaching material, and particularly the teaching experiences highlighted again the significant lack of technical knowledge about digital evidence among legal professionals in all countries, and the insecurity about the regulation of this type of evidence.

The findings of the empirical results presented in chapter 3 are remarkably similar to those of the two European projects. This highlights that little research and law and policy making has occurred on this topic. The interviewees stated that no legislation exists explicitly regulating the use of digital evidence, and in particular digital evidence

[646] See for a summary of the project and the main findings Insa, note 179.

seized by software tools from live systems ("double digital paradigm"). They also highlighted that a significant lack of knowledge about the technical aspects of this type of evidence exists, which can lead to problems with admitting and interpreting the evidence. It was stated that legal analytical work is required to establish legal certainty.

This chapter introduces in paragraph 7.1 the notion of digital evidence. It attempts to define the notion in section 7.1.1, and highlights the most pertinent technical characteristics of this evidence class in section 7.1.2. The convergence of science and law, and the influence of forensic science on the law of evidence are examined in section 7.1.3. In section 7.2 the admissibility of digital evidence in England and Wales, and Germany is analysed, and the particular problems with digital evidence collected by MIA tools highlighted. Section 7.4 examines potential solutions for the admissibility of digital evidence collected with MIA tools.

7.1 Digital Evidence

The term digital evidence (as well as the synonyms electronic and computer evidence) indicates that this type of evidence differs from documentary and physical evidence, if only by explicitly making a differentiation through the additional term "digital". The short case scenarios presented in section 7 have indicated that this type of evidence has some distinguishing features that set it apart from physical, and therefore the traditional notion of evidence. A thorough understanding of what digital evidence is, is necessary for the evaluation of the legal problems it triggers.

7.1.1 Definition

No generally accepted definition of the term digital evidence exists. The reason for this is that the relevance of this type of evidence for criminal investigations is only a very recent phenomenon that is rooted in the advent of the Internet and widespread of ICT devices.[647] The technological development and its simultaneous integration into societies occur at such speed that legal concepts based on these technologies are difficult to develop. As Mason and Schafer put it, "any definition that is too narrowly tailored to the current state of technology faces the risk of becoming obsolete within

[647] M Pollitt, R Bianchi, "Digital Evidence" in A Mozayani, C Noziglia (eds) *The Forensic Laboratory Handbook Procedures and Practice* (New York, Dordrecht, Heidelberg, London: Springer, 2011 2nd ed), 213.

years if not months. Definitions that are suitably future proof by contrast tend to focus on the most abstract aspects of the technology, and will therefore cut across traditional divisions and categories in the law of evidence that have historically grown."[648] In addition, digital evidence can be found in an ever-increasing number of places and in a great number of formats.

Several authors have attempted to define the term digital evidence, and these definitions should not be dismissed upfront for either being too technology specific or neutral. These are important sources for a better understanding of the concept and both, the technical and legal issues attached to it. Thus some of these definitions are introduced here, and a working definition of the term for the purpose of this thesis determined.

Digital evidence has been defined as "any information of probative value that is either stored or transmitted in a digital form."[649] A slight modification of this definition is "digital evidence is information stored or transmitted in binary form that may be relied on in court".[650]

The problem with these definitions is that they focus too heavily on the evidentiary value of the data, and neglect data that may further an investigation. In addition, as Casey points out, "the term binary in the latter definition is inexact, describing just one of many common representations of computerised data."[651]

Casey therefore goes on to define digital evidence as "any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi".[652]

This definition is much broader, because it refers to data as information of various kinds, including text images, audio and video. The focus is clearly on data collected during and for criminal investigations. However, the use of the term computer is potentially misleading, as it could be read to exclude other ICT devices transmitting or

---

[648] S Mason, B Schafer, "The Characteristics of Electronic Evidence" in S Mason (ed) *Electronic Evidence* (London: Lexis Nexis Butterworths, 2010), 22.

[649] Scientific Working Group on Digital Evidence (SWGDE), "Digital Evidence: Standards and Principles" (2000) 2:2 *Forensic Science Communications*, available online at: http://www.fbi.gov/about-us/lab/forensic-science-communications/forensic-science-communications-april-2010.

[650] J R Vacca, *Computer Forensics: Computer Crime Scene Investigation* (Hingham, MA: Charles River Media, 2nd edition, 2005), 700.

[651] Casey, note 637, at 7.

[652] Ibid.

storing data. In addition, this definition requires that the data must be directly linked to the course of a crime, and that it is reliable and therefore admissible in court.
Mason and Schafer define digital evidence[653] as "data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence".[654]
This definition is much wider with respect to the storage device. It intends, as Schafer and Mason point out, to include all forms of devices that can, in its widest meaning, be considered a computer (thereby explicitly excluding the human brain), store or transmit data, including analogue devices producing an output.[655] The relevant data is also further specified. Here, the focus is not so much on crime investigations, but more on legal disputes in general, implying that the data must be relevant for the process of deciding a dispute between different parties.

The conclusions that can be drawn from analysing existing definitions of digital evidence is that the state-of-the-art of technology, as well as the technical meaning of terms used is of high relevance for the validity of the definition. Equally important is the context setting to which the definition applies.
It also highlights just how much technical progress affects legal concepts regulating technologies. While initially computers were the main and only source of digital evidence, this changed with the development of other ICTs, such as wearable (e.g. smart phones) and even implantable (brain-computer interaction chips) ICTs.
Thus before developing a working definition of digital evidence, these above identified issues need to be addressed and taken into account.
As analysed in chapters 2 to 5, MIA tools are used to infiltrate a variety of data processing and storing devices. However, one condition is that the devices are connected to the Internet. Without an Internet connection the infiltration is impossible. This is an important difference to more traditional search and seizure procedures of digital evidence conducted by human officers (see case variation a above).

---

[653] However, choosing the term electronic evidence.
[654] Mason/Schafer, note 648, at 25.
[655] Ibid.

The definition should be a guideline and provide a common understanding of the term for those parties involved in the handling of digital data collected by MIA tools. The working definition for this thesis is therefore:

Digital evidence is data stored, processed, or transmitted by any information and communication (ICT) device that has the potential to support or refute a theory about unlawful behaviour occurred or to occur in the future.

This definition has two aspects that set it apart from other definitions of this concept, but are relevant for the fact that the evidence is collected by MIA tools. Firstly, the use of the term ICT instead of computer indicates that any data that is processed, stored or transmitted by devices that can be connected to the Internet is included in this definition. This takes into account the rapid advancements in technology, not limiting the definition span to now outdated concepts of computers in the form of a PC or laptop. This guarantees that also smart phones, navigation systems, and even smart implantable microchips are included in the definition. However, it excludes devices that are not connected to the Internet, and therefore cannot be infiltrated by MIA tools. Secondly, the definition restricts the data to information that is relevant to the claim of a party that a breach of law has occurred, or that an initial suspicion exists that this will occur in the near future. Thus, the data needs to be relevant to the claim. However, as opposed to the two early and Casey's definition but in accordance with Mason and Schafer's interpretation, admissibility of the evidence is not a decisive aspect here. Hence this working definition tries to sufficiently address the conclusions drawn from existing definitions above.

Mason and Schafer make an important statement with regard to the use of the term data that is also of relevance for this thesis' working definition. The term data is used here in a non-technical sense meaning roughly 'a gathered body of facts'.[656] Computer scientists often distinguish between 'data' and 'programs', and the distinction is indeed constitutive for the definition of computer. For the purpose of this thesis, however, this distinction is unhelpful. In a copyright case, if the defendant has allegedly installed an unauthorised operating system, the 'presence of the system on the computer' is digital data for this purpose.[657]

[656] Mason/Schafer, note 648, at 25.
[657] Mason/Schafer, note 648, at 25.

Summarising, it can be concluded that no one widely accepted definition of digital evidence exists. The reason for this is that the validity of such a definition greatly depends on the context, and the state of the art of technology. However, the existence of a definition applicable to digital evidence collected by MIA tools is relevant for the common understanding of this type of evidence among the different parties involved in the process of seizing, examining, analysing, and assessing the data. Therefore, a working definition of digital data has been developed for this thesis, which is sufficiently technology neutral to ensure it remains valid in case of technological progress. The analysis of the various definitions facilitated the development of this definition.

7.1.2 Characteristics of Digital Evidence

The above definition in conjunction with the short scenarios in part 7 have already indicated the most pertinent characteristic of digital evidence: It is latent to the human observer, unless made visible by a computer process or program. However, a forensic expert is required to find and evaluate all "hidden" data relevant to the investigation. Thus the virtual living space fundamentally differs from the physical world, in which the laws of physics uniquely render objects.

If the police found a gun with an alleged perpetrator's fingerprints on it, the prosecutor could argue that the gun should be accepted as circumstantial evidence. Because various physical and chemical investigations are possible, it would be almost pointless for the defendant to claim that the object is not a gun, the fingerprints belong to somebody else, and so forth. A defendant could, of course, challenge the validity of a specific fingerprint identification, among other things, but the general facts are indisputable.

Digital world objects on the contrary are bits and bitstrings, exhibiting no measurable intrinsic physical properties (weight, size, age, and so forth). Furthermore, as Oppliger and Rytz point out, deciding whether a bitstring is genuine or synthetically generated is difficult.[658] In addition, digital evidence stored on an ICT device cannot be compared to similar documentary and physical evidence.

[658] R Oppliger, R Rytz, "Digital Evidence: Dream and Reality" (2003) 1:5 *IEEE Security and Privacy*, 44, 45.

For example, an electronic document, even if it looks remarkably like a traditional piece of paper containing handwritten information on a screen of an ICT device is nothing like the physical counterpart.

Mason and Schafer explain that it is not an object that exists somewhere on the device, in the same way as a paper document is filed in a physical file. Instead, the digital document is better understood as a process by which otherwise unintelligible pieces of data that are distributed over the storage medium are assembled, processed and rendered legible for a human user. In this sense, the document is nowhere; it does not exist independently from the process that recreates it every time a user opens it on screen.[659]

This means that digital evidence is generally an abstraction of some event or digital object. When a person instructs a computer to perform a task such as compiling a document, the resulting activities generate data remnants that give only a partial view of what occurred.[660] Thus the human user never sees the actual data but only a representation, and each layer of abstraction can introduce errors.[661]

Hence, digital data is a messy and slippery form of evidence that can be very difficult to handle. For instance, a hard drive platter contains a messy amalgam of data – pieces of information mixed together and layered on top of each other over time. [662] Only a small portion of this amalgam might be relevant to a case, making it necessary to extract useful pieces, fit them together, and translate them into a form that can be interpreted by a human.[663]

In addition, unlike documentary and physical evidence encountered during investigations, digital evidence can be very fragile. Its very existence may not be obvious until an expert has further examined the hardware containing the digital data. However, it also means that digital evidence, by its fragile nature can easily be disrupted, changed or replaced.[664] Physical and documentary evidence tends to obey

---

[659] Mason/Schafer, note 648, at 28.

[660] D Farmer, W Venema, "Forensic Computing Analysis: An Introduction" (2000) *Dr.Dobb's*, available online at: http://www.drdobbs.com/184404242;jsessionid=UUDPHDMG32RETQE1GHPSKH4ATMY32JVN.

[661] B Carrier, "Defining Digital Forensic Examination and Analysis Tool Using Abstraction Layers" (2003) 1:4 *International Journal of Digital Evidence*, 4.

[662] Casey, note 637, at 25.

[663] Ibid.

[664] Uzunay/Incebacak/Bicakci, note 515, at 105.

the "Dead Body Theorem", meaning, "it is not going anywhere".[665] Digital evidence can be altered maliciously by offenders or accidentally during collection without leaving any obvious signs of distortion.

It can, for example, be tainted or destroyed by performing a simple action like turning off the power of the ICT device. In addition, the exact same data can easily be recreated by any person who has access to the ICT device.[666] If the ICT device is connected to a network (such as the Internet or an Intranet), data can maliciously be tainted or deleted if the ICT device is accessed through another device connected to the same network.

However, digital evidence possesses several features that mitigate the problem of its fragility. The fact that digital evidence can be duplicated exactly means that a copy can be examined as if it was the original, therefore avoiding the risk of damaging the original.[667] Furthermore, with the right tools it is relatively easy to determine whether digital evidence has been modified or tampered with by comparing it with an original copy.[668] In addition, digital evidence is difficult to destroy. Even when a file is deleted, or a hard drive is formatted, digital evidence can be recovered.[669] Moreover, when suspects attempt to destroy digital evidence, copies and associated remnants can remain in places that they were not aware of.[670]

However, these advantages do not always apply to digital evidence seized using MIA tools. The reason is that MIA tools seize evidence from ICT tools and live networks without confiscating the tool itself. Hence, the suspect continues to use the ICT tool and therefore modifies the data and the system itself, and thus no possibility exists to create a duplicate of the seized data. This means, no later comparison of the copied data with the original is possible to determine whether the data has been modified or tampered with.

Another problem during investigations of the virtual living space is that digital evidence can exist in large volumes, as opposed to physical evidence. Data storage needs and data storage capacities are ever increasing. Last century, it was common to

---

[665] J Kornblum, "Preservation of Fragile Digital Evidence by First Responders" (2002) *Digital Forensics Research Workshop*, 1, available online at: http://dfrws.org/2002/papers/Papers/Jesse_Kornblum.pdf.

[666] Uzunay/Incebacak/Bicakci, note 515, at 106.

[667] Casey, note 637, at 26.

[668] Ibid.

[669] Ibid.

[670] Ibid.

acquire hard disks in 700 MB image segments in order to burn an entire image to a handful of CD-ROMs. Now, "small" cases often involve several hundred gigabytes of data, and multi-terabyte corporate cases are commonplace. In 2007, for example, the size of Wal-Mart's data warehouse exceeded the petabyte mark.[671]

In addition, the advent of computer networks, the most well known of which is the Internet, has also contributed to the increase of data potentially relevant for investigations. Networked ICTs enable users to create and transmit large volumes of data, a phenomenon described as networked communication.[672] For example, one word-processing document can be sent to any number of people across the globe. If the creator of the document sends the file to 20 people, the number of copies will far exceed 20 when each person copies the file to another drive on their computer, and the organisation backs up the email database each day, then backs up the main database each week, and copies are burnt on to CD-ROMs or copied on to external storage devices.[673] As a result of this, investigators are faced with large volumes of data that need to be identified to obtain relevant documents pertaining to the investigation of a suspect.

The above analysis of the most pertinent characteristics of digital evidence has shown that this type of evidence fundamentally differs from traditional documentary and physical evidence, and therefore challenges existing legislation regulating the seizing and use of evidence during criminal investigations. However, the question arises whether digital evidence and its characteristics and challenges for the law and law enforcement are unique, and therefore unprecedented.

7.1.3 Digital Evidence – An Entirely New Challenge?

The previous sections have shown that digital evidence is a distinctive new class of evidence that differs significantly from traditional evidence types that are commonly seized and used during criminal investigations. The conclusion appears to be that digital evidence is unlike any other existing evidence type, and therefore requires entirely new procedures and legislation regulating its seizure and use.

---

[671] M Hayes Weier, "Hewlett-Packard Data Warehouse Lands In Wal-Mart's Shopping Cart" *InformationWeek*, 4 August 2007, available online at: http://www.informationweek.com/news/storage/showArticle.jhtml?articleID=201203024.

[672] Mason/Schafer, note 648, at 31.

[673] Ibid.

Legal professionals expressed this opinion and supported this theory, particularly when digital evidence first gained relevance for investigations and court proceedings. General apprehension towards digital evidence by legal practitioners was uniformly found across jurisdictions.[674]

However, science has provided a foundation for legal proceedings for more than 100 years.[675] During this time, the science practiced in the legal system has differed from traditional scientific endeavours in its form and application, though not in its content.[676] While traditional science deploys the "scientific method" to drive methods of proof, the legal system has demanded additional approaches to ensure the reliability of evidence, the scientific methods applied and the resulting testimony. These requirements are the result of judicial decisions rather than scientific research and discourse.[677]

Thus the question arises whether this confluence and convergence of disciplines (which resulted in the establishment of the domain that is commonly referred to as forensic science)[678] has resulted in general principles and procedures applicable to the handling of digital evidence.

Kirk finds that "with all the progress that has been made in the field of forensic science, on a wide front, careful examination shows that for the most part, progress has been technical rather than fundamental, practical rather than theoretical, transient rather than permanent."[679] He states further "many persons can identify the particular weapon that fired a bullet, but few if any can state a single fundamental principle of identification of firearms. Document examiners constantly identify handwriting, but a

---

[674] Ibid, at 23.

[675] The introduction of DNA evidence, for example, was also met with great skepticism, however, scientific results and principles influenced the law and enabled the use of DNA evidence in court proceedings.

[676] M Pollitt, "Applying Traditional Forensic Taxonomy to Digital Forensics" in I Ray, S Shenoi (eds)IFIP International Federation for Information Processing, Volume 285; *Advances in Digital Forensics IV* (Boston: Springer, 2008) 17-26, 18.

[677] C H Welch, "Flexible Standards, Deferential Review: Daubert's Legacy of Confusion" (2006) 29:3 *Harvard Journal of Law and Public Policy*, 1085.

[678] Forensic Science can be referred to as "the application of a broad spectrum of sciences to answer questions of interest to a legal system that may be in relation to a crime or a civil action; A Pushpalatha, B Mukunthan, "Automation of DNA Finger Printing for Precise Pattern Identification using Neural-fuzzy Mapping Approach" (2011) 13:3 *International Journal of Computer Applications*, 16, 17.

[679] P L Kirk, "The Ontogeny of Criminalistics" (1963) 54:2 *The Journal of Criminal Law, Criminology, and Political Science*, 235-238, 235.

class of beginners studying under these same persons, would find it difficult indeed to distinguish the basic principles used. In short, there exists in the field of criminalistics a serious deficiency in basic theory and principles, as contrasted with the large assortment of effective technical procedures."[680]

However, having identified the lack of comprehensive fundamental principles in forensic science, Kirk fails to develop a set of these in his work. This does not, however, render the importance of his ascertainment.

Following Kirk's criticism (though not necessarily as a direct result of this), a theoretical framework defining fundamental concepts for the application of scientific knowledge to the legal forensic domain has evolved. These concepts are pillars guiding the forensic analysis in a logical progression, starting with understanding the origin of evidence, culminating in a statement of the significance of an analytical result.[681] As the most important concepts for the work of traditional forensic practitioners can be identified two principles and four processes:[682]

1. *Divisibility of Matter*: This principle refers to the ability to impute characteristics to the whole from a separated piece.[683] It is built on the fact that matter must divide before it can be transferred.[684] Inman and Rudin explain this further stating that "matter divides into smaller component parts when sufficient force is applied. The component parts will acquire characteristics created by the process of division itself and retain physico-chemical properties of the larger piece."[685]

2. *Transfer*: This principle is derived from Locard's exchange principle, which states, "with contact between two items, there will be an exchange of material."[686] Locard is considered to be the pioneer of modern forensic science,[687] and while his exchange principle may appear obvious in retrospective, it is the fundament of the existing corpus of forensic scientific

---

[680] Ibid.
[681] K Inman, N Rudin, "The Origin of Evidence" (2002) 126 *Forensic Science International*, 11.
[682] Pollitt, note 676, at 21ff.
[683] Ibid, at 12.
[684] Ibid.
[685] Ibid.
[686] E Locard, L'Enqueˆte criminelle et les Methodes scientifiques, Flammarion, Paris, 1920.
[687] Pollitt, note 676, at 19.

knowledge. Such exchanges can include for example fingerprints and footprints, hair, fibres of clothes, scratches, wounds, or oil stains. These examples show that transfer should not only be reduced to transfer on a microscopic scale.[688]

3. *Identification*: This process refers to the categorisation of evidence into a class. Saferstein, who can be credited with defining this principle, refers to it as "the physiochemical nature of the evidence."[689] Inman and Rudin note that being able to accurately describe an item or its composition may be sufficient for a given forensic purpose. For example, when the mere presence of illicit drugs is an important element of a crime being investigated, the identification of a white powder as containing cocaine, dextrose and talc may be all that is required.[690]

4. *Individualisation*: This process is based on the physical and logical paradigm that any individual object is unique. Its aim is to uniquely identify a specimen using a set of characteristics.[691] This process answers the questions: "which one is it?" or "whose is it?" depending on whether the item is animate or inanimate by inferring a common source or origin.[692] The notion can be clarified using an example. A video surveillance camera captures the shooting death of a victim. The perpetrator cannot be identified from the video, but the image is clear enough to identify the type of firearm. A bullet is recovered from the victim and submitted for examination. Based on the bullet's weight and composition, and the size and twist of the rifling marks, the examiner may be able to identify an ammunition manufacturer, the caliber of the weapon and, potentially, its manufacturer. These are all class characteristics, which, on their own, do not link the suspect to the weapon or the weapon to the bullet. After a suspect is identified, a search reveals a box of unused ammunition and a weapon consistent with the one in the surveillance video. The characteristics of the

---

[688] R Böhme et al., "Multimedia Forensics Is Not Computer Forensics" in Z J M H Geradts, K Y Franke, C J Veenman (eds.) *Computational Forensics: Third International Workshop*, *IWCF 2009* (Berlin, Heidelberg: Springer, 2009) 90-103, 92.
[689] R Saferstein, *Forensic Science Handbook, Volume II* (Englewood Cliffs, New Jersey: Prentice-Hall, 1988).
[690] K Inman, N Rudin, *Principles and Practices of Criminalistics: The Profession of Forensic Science* (Boca Raton, Florida: CRC Press, 2001).
[691] Kirk, note 679, at 237; P DeForest, R Gaensslen, H Lee, *Forensic Science: An Introduction to Criminalistics* (New York: McGraw Hill: 1983) 7.
[692] Inman/Rudin (2002), note 681, at 15.

seized ammunition are identical to the bullet obtained from the victim. As a result, it can be determined that the bullets have a common origin and are therefore "class evidence." The recovered weapon is test-fired and the resulting bullet and the bullet recovered from the victim are microscopically examined. Matching the micro-striations on the bullets allows the examiner to identify the two bullets as coming from the recovered weapon, to the exclusion of all others. This is the process of identification, which yields what is referred to as "individual evidence."

5. *Association*: This process refers to the linking of a person with a crime scene. It can be defined as "an inference of contact between the source of the evidence and a target".[693] Such an inference is based on the detection of transferred evidence. The source and the target are relative operational definitions defined by the structure of the case; if transfer is detected in both directions, for instance, each item is both a source and a target of evidence. An example can, again, clarify the notion. Consider a fiber collected from the body of a deceased individual. The evidence fiber from the body and the reference fibers from the van carpet are found to be the same type and to contain indistinguishable dye components. These physico-chemical similarities are expected if the van carpet is the source of the evidence fiber, if the fiber was transferred during the crime, and if it persisted on the body until collected. Next, an evaluation is made of all other possible sources of fibers indistinguishable from the evidence fiber, including all carpets made from such fibers and any other items manufactured from indistinguishable fibers. From this information, the probability of finding the fiber on the deceased if it derived from some other source can be estimated.

6. *Reconstruction*: This process refers to the understanding of the sequence of past events.[694] This principle attempts to answer the questions: "where, how, and when". It can also be referred to as "the ordering of associations in space and time."[695]

---

[693] Inman/Rudin (2002), note 681, at 15.
[694] P DeForest, R Gaensslen, H Lee, see note 691, at 8.
[695] Inman/Rudin (2002) note 681, at 16.

This framework of principles and processes has evolved as the underlying paradigm of forensic science. It is the guideline for forensic examinations, and has stood the tests of time and the courts. It facilitates the formulation of an accepted practice that adds to the efficiency, effectiveness and reliability of the practitioner's work. Figure 1 is a pictorial representation of this framework, which serves to better illustrate the significance and role of each of the principles and processes for a traditional forensic examination.

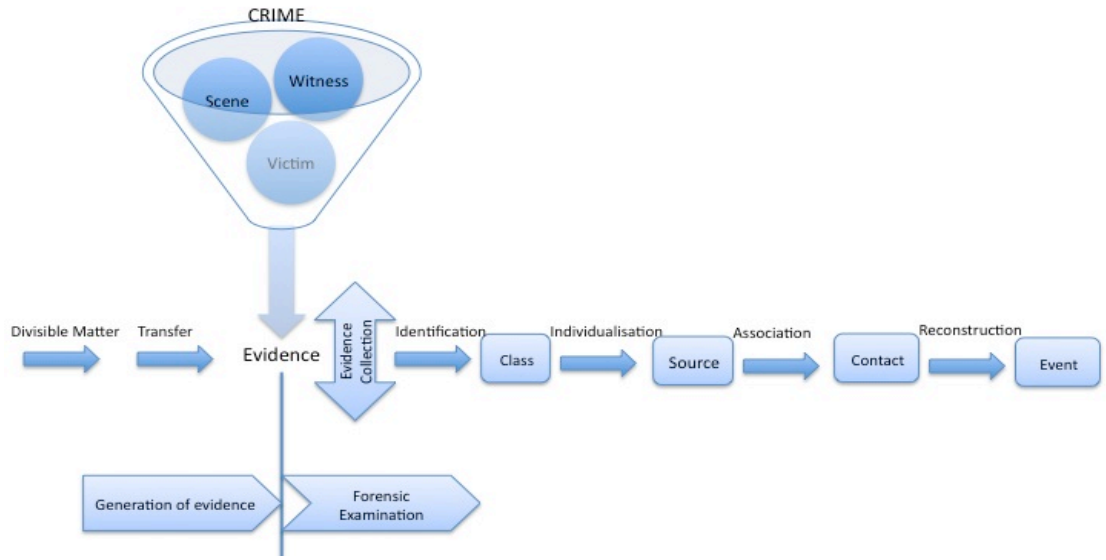

Figure1: Evidence Principles and Processes

This figure illustrates that the two principles (*divisibility of matter* and *transfer*) generate the evidence, and are the two fundamental principles upon which the forensic analysis of physical evidence is based. The processes (*identification, individualisation, association, and reconstruction*) serve to reconstruct the origins of the evidence and the event that led to the creation of the evidence, and therefore form the infrastructure for the practice of forensic science.

The question is now, whether this fundamental paradigm of forensic science developed for the handling of physical evidence is applicable (if only in parts) to digital evidence.

Looking at Figure 1 above, it is easy to see how the two principles *divisibility of matter* and *transfer* underlie many of the biological, physical and chemical examinations conducted by traditional forensic scientist. However, it is questionable whether this also applies to the handling of digital evidence, which differs significantly from traditional evidence as discussed above in section 7.1.1 and 7.1.2. However, as shown above, one characteristic of digital evidence is the fact that it can be duplicated easily.[696] Thus digital evidence exhibits divisibility of matter when duplicates are created. This is the case because electronic duplicates are representatives of the original evidentiary items. The content of an electronic document is identical with the original content,[697] however, in the process of duplicating the original, the new document acquires its own characteristics. The force required for the division of physical evidence,[698] can be seen in the act of instructing the ICT device to produce the duplicate, and the execution of this order by the tool.

Transference can be detected in digital evidence in its interactions. As analysed in section 7.1.2, digital evidence is fragile, and easily modified.[699] Any modification, even the turning on of the ICT device, can modify data, and therefore digital evidence. Any new application or process will leave a digital fingerprint behind.

Thus the two principles of *divisibility of matter* and *transfer* can also be applied to digital evidence. However, as Pollitt remarks, these principles do not have a great deal to offer in terms of developing guidelines for the examination process of digital evidence.[700] This is also highlighted by Figure 1 above, which shows that the two principles are relevant for the generation of the evidence, not, however, for the examination process. The examination process is of high relevance for the question of reliability of evidence, and the applicability of existing paradigms to digital evidence therefore potentially valuable for the handling of this new type of evidence.

---

[696] See p. 216.
[697] See p. 216.
[698] Inman/Rudin (2002) note 681, at 12.
[699] See p. 217.
[700] Pollitt, note 676, at 20.

The process of *identification* is of equal importance for digital evidence handling as it is for documentary and physical. However, here it is a two-fold process.[701] First the hardware (for example, computers, PDA, memory stick, network cable) that contains digital evidence needs to be recognised. Second, digital data stored on the hardware, and the distinction between irrelevant data and information linked to the investigation needs to be recognised and distinguished. In traditional forensic science, the identification process leads to the classification of the evidence into classes. As Pollitt states, in the discipline of digital forensics, the identification process helps describe and class digital evidence in terms of its context – physically (a particular brand of hard drive), structurally (the number of cylinders, heads and sectors), logically (a FAT32 partition), location (directory and file) or content (a memo, spreadsheet, email or photograph).[702] The presence of metadata or the existence of a particular letter (not necessarily their content) may be probative in an investigation. The process of identification involves classifying digital objects based on similar characteristics, called class characteristics.[703]

For example, there are different types of graphic files (e.g. JPEG, GIF, TIFF) making it possible to be specific when classifying them. Such class characteristics are useful for locating fragments of digital objects on a disk. For instance, searching an entire hard drive for all occurrences of class characteristics like "JFIF" is a more thorough way to search for JPEG images than simply looking at the file system level for files with a ".jpg" file extension. In addition to finding fragments of deleted images in unallocated space, searching for class characteristics will identify JPEG files that have been renamed with a ".doc" extension to hide them from forensic examiners. Evaluating the source of a piece of digital evidence essentially means to compare items to determine if they are the same as each other or if they came from the same source.[704] The aim in this process is to compare the items, characteristic by characteristic, until the examiner is satisfied that they are sufficiently alike to conclude that they are related to one another. Constellations of similar characteristics are relevant in evaluating the relationships between digital evidence and its source. The more characteristics an item and potential source have in common, the more likely it is that they are related.

---

[701] Casey, note 637, at 468.
[702] Pollitt, note 676, at 20.
[703] Casey, note 637, at 488.
[704] Casey, note 637, at 492.

The relevance of the process of *individualisation* for digital evidence is relatively apparent. File systems, partitions and individual files have characteristics that uniquely set them apart from others. Thus the concept of a significant difference is important because it can be just such a difference that distinguishes an object from all other similar objects, that is, it may be an individual characteristic.[705] Although such characteristics are rarer than class characteristics, it is important to keep in mind that digital evidence may contain unique characteristics that individualise it, that is, link it to a particular source with a high degree of probability. An example is a Microsoft Word file, which has a well-documented internal structure. It would be accurate to describe the origin of such a file as being produced by Microsoft Word. All of these are class characteristics. Conversely, a file may be positively identified based on its mathematical signature (i.e. hash value), which corresponds to the process of identification.

The process of *association* is slightly more abstract in digital forensics, albeit relevant. The physical transfer of evidence is uncommon in digital evidence cases. In digital forensics, it is necessary to identify the items (files, data structures and code) that need to be associated and to determine where they might be located and the tools that could be used to locate the items.[706]

The process of *reconstruction* however, is more common and easier in the case of digital evidence than physical evidence. Digital evidence is a rich and often unexplored source of information because of the dates and times stamped on metadata pertaining to data, files, file systems and network communications. It can establish action, position, origin, association, function, sequence and more, enabling an investigator to create an incredibly detailed picture of events surrounding the crime.

The above analysis of the forensic science paradigm has highlighted, that scientific research has greatly impacted and influenced the legal concept of evidence. The evolvement of forensic science has allowed for a better understanding of the principles underlying physical evidence, and therefore enabled the development of generally accepted guidelines for the adequate and proper examination of evidence. This has

[705] Casey, note 637, at 495.
[706] Pollitt, note 676, at 22.

facilitated the efficiency, effectiveness and reliability of legal forensic examiner's work.[707]

The analysis of the application of the existing forensic paradigm to digital evidence has shown, that digital evidence, despite its unique characteristics identified in section 7.1.2, can be subsumed under the existing forensic science principles and processes. One important lesson can be drawn from this finding: from a scientific perspective, digital evidence shares fundamental features with traditional types of evidence.

This finding is of importance for the following analysis of the conceptual problems digital evidence generates for the law. The reliability of digital evidence, and therefore admissibility of this evidence for court proceedings has been questioned by legal professionals from the time of the introduction of this new evidence class.[708] However, the fact that traditional forensic science has developed an effective and relatively efficient process for the proper examination of evidence that has stood the tests of time and the courts,[709] which is applicable to digital evidence, means that scientific findings can be used to overcome legal insecurities and problems.

7.2 Use As Evidence

The above analysis of the concept of digital evidence has shown that fundamental differences between physical and digital evidence exist. As shown, these problems have led to scepticism about digital evidence among legal practitioners. This was also highlighted by the empirical research conducted for the European projects.[710]

This difference also impacts on the use of digital evidence in court proceedings, and in particular on the use of digital evidence collected by MIA tools. However, the previous chapters of this thesis have proven, that the deployment of MIA tools is already well underway, and will likely occur more frequently in the future. Therefore, it is crucial to assess the usability of digital evidence in court proceedings.

If data collected by MIA tools cannot be used during court proceedings, the practical relevance of this class of investigative technologies would be minor. To evaluate the

---

[707] Pollitt, note 676, at 19.

[708] See for a discussion of this e.g. E van Buskirk, V T Liu, "Digital Evidence: Challenging the Presumption of Reliability" (2006) 1:1 *Journal of Digital Forensic Practice*, 19-26.

[709] Pollitt, note 676, at 25.

[710] See p. 77.

usability of this type of evidence for legal proceedings, an analysis of the relevant evidence law principles is undertaken in this section.

This exercise is comparative in nature, examining the situation in two jurisdictions: England & Wales, and Germany. There are two reasons for this: firstly, these two jurisdictions have been the prime focus of this thesis, with case studies from both discussed. The focus on these two jurisdictions in this chapter ensures that the legal evaluation of this type of evidence in common law, as well as civil law jurisdictions occurs. This is also relevant for the second reason, namely the cross-jurisdiction nature of MIA tools, as discussed in chapter 6. The introduction of MIA technologies for law enforcement authorities is an international development,[711] and it is therefore important to establish whether different jurisdictions are apt to handle digital evidence collected by MIA tools.

7.2.1 Background

Evidence in legal proceedings[712] is information with which the matters of requiring proof in a trial are proved.[713] Conceptually, the admissibility requirements for digital evidence are the same as those imposed on any type of evidence: the evidence must be both reliable and relevant. This is the case for both jurisdictions in question.[714]

The previous paragraph (7.1.3) has concluded, that science can play an important role in assisting the law in overcoming conceptual insecurities. For the application of scientific findings to the law and legal proceedings, it is, however, important to ascertain the validity of the scientific results.

It is inherent that the process of "fact-finding" in both the law and in science is a probabilistic quest, (though this is not always recognised in the case of science).[715] Legal proceedings typically include standards allocating a burden of proof: beyond a reasonable doubt is the standard for guilt in criminal matters.

---

[711] See p. 55ff.

[712] This is true for both criminal and civil law proceedings. However, for the purpose of this thesis the focus will be solely on criminal proceedings.

[713] A L-T Choo, *Evidence* (Oxford: Oxford University Press, 2006) 1.

[714] For a general overview of evidence law and its principles in England & Wales see H M Malek (ed), *Phipson on Evidence* (London: Sweet & Maxwell, 17th ed, 2010). For Germany see U Eisenberg, *Beweisrecht der StPO* (München: C.H. Beck Verlag, 2011).

[715] R M Wheate, A Jamieson, "A Tale of Two Approaches – The NAS Report and the Law Commission Consultation Paper on Forensic Science" (2009) 7:2 *International Commentary on Evidence*, 3.

The law does not pronounce culpability based on absolute certainty, but in accord with legally required degrees of belief.[716] Similarly, science, though perhaps a search for "the truth", is nevertheless still probabilistic: the only certainty in science, particularly in a forensic context, is exclusion. Scientific laws are typically developed during a long process of attempting to disprove a certain hypothesis, in addition to testing and retesting alternative hypotheses.[717] This accords with the Popperian view of science[718] (although a number of authors consider that falsifiability may not be the touchstone claimed by Popper's adherents[719]).

Therefore, it is important that scientific results applied to the law, and in particular criminal legal proceedings are soundly scientific based, and are not raised above their supportable scientific value.

7.2.2 The Admissibility of Digital Evidence – England & Wales

The aim of this section is to set out the main principles of the admissibility of evidence in digital format in criminal proceedings in England & Wales, to determine whether the existing legal framework is appropriate and sufficient to deal with this type of evidence. This is by no means an account of the existing evidence law in its entirety in England and Wales, nor meant to be.[720] It serves to highlight the challenging and problematic aspects of this type of evidence.

As a start, it is important to identify the considerations upon which the law of criminal evidence is premised. Essentially, it can be said that underlying the principles of criminal evidence are considerations of both intrinsic policy and extrinsic policy.[721]

---

[716] See *R v Stevens* [2002] All ER (D) 34 (Jun) for example, in which the Court of Appeal (Criminal Division) reiterated, in response to jury questions about the definition of a reasonable doubt, that it was not helpful for a judge to direct a jury to distinguish between being sure and being certain and a judge should avoid doing so".

[717] Wheate/Jamieson, note 715, at 3.

[718] See generally, K Popper, *The Logic of Scientific Discovery* (New York: Basic Books, 1959). Popper noted that corroboration of a theory is a matter of its past performance only, and "says nothing whatever about future performance, or about the "reliability" of a theory.' K Popper, *Objective Knowledge: An Evolutionary Approach* (Oxford: Clarendon Press, 1982), 18.

[719] See works by T Kuhn (eg *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 1962)), C Hempel (eg *The Philosophy of Carl G.Hempel: Studies in Science, Explanation and Rationality* (Oxford: Oxford University Press, 2001)) and P Feyerabend (eg *Against Method* (London: Verso, 1993)) for the ongoing debate as to the definition of "science" and the "scientific method".

[720] For this see e.g. Malek, note 714.

[721] L-T Choo, note 713, at 19.

The concern of intrinsic policy is with the promotion of accurate fact-finding or truth[722] discovery, or, in other words, with what Bentham referred to as "rectitude of decision."[723] It is important to ensure that evidence is as reliable as possible. Dworkin states that 'people have a profound right not to be convicted of crimes of which they are innocent."[724]

This intrinsic consideration is the basis for evidence principals regulating the admissibility of evidence (such as the hearsay principle). It is also relevant for the discussed value and reliability of scientific findings applied to evidence law.[725]

The concept of extrinsic policy, as explained by Wigmore, "has no relation to the scientific principles of proof. Rather it excludes good evidence on other grounds of policy, which are supposed to override the policy of obtaining all possible useful evidence. They seek to preserve unharmed the extrinsic interests that would be injured by using the evidence, and at the same time to let justice be done by establishing the truth in the case in hand."[726] Galligan states that extrinsic policy "refers to the exclusion of evidence for reasons other than reasons of evidentiary value. The issue is whether certain kinds of evidence, which are likely of probative value, should be excluded, in order to advance other values of policies."[727]

The concept of extrinsic policy therefore regulates the case of improperly obtained evidence.[728]

From this, it can be derived that for digital evidence to be admissible, it must be reliable, and not otherwise be excluded.

---

[722] For a critical discussion of the concept of 'truth' see generally K D Killback, M D Tochor, "Searching for Truth but Missing the Point" (2002) 40 *Alberta Law Journal Review*, 333.

[723] J Bentham, *Rationale of Judicial Evidence, Specially Applied to English Practice*, Vol 1 (London: Hunt and Clarke, 1827) 1.

[724] R Dworkin, *A Matter of Principle* (Havard: Havard University Press, 1985) 72.

[725] See p. 216ff.

[726] J H Wigmore, *The Science of Judicial Proof, as given by Logic, Psychology, and General Experience, and Illustrated in Judicial Trials* (Boston: Little Brown and Co, 3rd ed, 1937) 945.

[727] D J Galligan, "More Scepticism About Scepticism" (1988) 8 *Oxford Journal of Legal Studies,* 249, 255.

[728] See for a general discussion of improperly obtained evidence for example J Allan, "To Exclude or Not to Exclude Improperly Obtained Evidence: Is a Humean Approach More Helpful?" (1999) 18 *University of Tasmania Law Review,* 263; C J W Allen, "Discretion and Security: Excluding Evidence Under Section 78(1) of the Police and Criminal Evidence Act 1984" (1990) *Cambridge Law Journal,* 80; A J Ashworth, "Excluding Evidence As Protecting Rights" (1977) *Criminal Law Review,* 723; B Fitzpatrick, N Taylor, "Human Rights and the Discretionary Exclusion of Evidence" (2001) 65 *Journal of Criminal Law,* 349.

However, another admissibility criteria exists: *relevance*. Relevance[729] is the fundamental condition of admissibility of evidence.[730] The question whether evidence is relevant depends not on abstract legal theory but on the individual circumstances of each particular case.[731] Stephen has defined relevance as "The word 'relevant' means that any two facts to which it is applied are so related to each other that according to the common course of events, one either taken by itself or in connection with other facts proves or renders probable the past, present or future existence or non-existence of the other."[732] Thus, an item of evidence is relevant as long as it has probative value or probative force,[733] however little.[734] Lord Simon of Glaisdale explained in *DPP v Kilbourne*, that "evidence is relevant if it is logically probative or disprobative of some matter which requires proof. […] It is sufficient to say, even at the risk of etymological tautology, that relevant (ie, logically probative or disprobative) evidence is evidence which makes the matter which requires proof more or less probable."[735]

The requirement of relevance of evidence is not further discussed here.[736] It was depicted for sake of completeness, but does not in itself raise problems for digital evidence. However, implicitly, it contains an interesting issue: the question of what constitutes an admissible type of evidence. Given the unique characteristics of digital evidence as described above,[737] the question arises whether digital data, given its unique nature, can be regarded as an admissible type of evidence.

---

[729] For a general discussion of relevance see Law Commission (Consultation Paper No 141), *Criminal Law-Evidence in Criminal Proceedings: Previous Misconduct of a Defendant-A Consultation Paper* (1996) [6.7]-[6.9], available at http://www.lawcom.gov.uk/docs/cp141.pdf.

[730] For a more detailed discussion of this concept see: I Dennis, *The Law of Evidence* (London: Sweet & Maxwell, 2010), 40ff.

[731] *R v Guney* [1998] 2 Cr App R 242, 265.

[732] J F Stephen, *A Digest of the Law of Evidence*, ed. by H L Stephen, L F Sturge (London: Macmillan, 1948), Art. 1.

[733] *R v Hartz* [1967] AC 760, 785 per Thesiger J: 'the word "relevant" is to all intents and purposes synonymous with the phrase "of probative value".

[734] 'It is enough if the item could reasonably show that a fact is slightly more probable than it would appear without that evidence': E W Cleary (ed), *McCormick on Evidence*, 3rd ed. (St. Paul: West, 1984) 542.

[735] [1973] AC 729, 756.

[736] See for a detailed discussion, note 728; L-T Choo, note 713, at 3, also depicting the controversly debated Wigmore approach to relevance.

[737] See p. 214ff.

7.2.2.1. Types of Evidence

Generally, the types of evidence admissible during criminal procedures fit into two categories: direct and indirect (or circumstantial) evidence.[738]

Direct evidence is evidence that proves a fact or proposition directly rather than by secondary deduction or inference.[739] Examples of direct evidence include eyewitness testimony, the oral confession of a defendant, or a victim's first-hand account of a criminal assault. In addition, the existence of a physical object constitutes direct evidence.[740] Its existence can be proven by its production, or by the testimony or declaration (which must be admissible) of a person who actually perceived the object. Considering these characteristics of direct evidence it appears doubtful whether digital evidence, given its volatile nature, can be direct evidence.

Casey remarks, "it is a common misconception that digital evidence cannot be direct evidence because of its separation from the events it represents."[741] However, digital evidence can prove facts just like physical evidence can. The human perception of a screen printout is admissible as direct evidence.[742] Further examples of digital data admitted as direct evidence are records of the product of mechanical devices and automatic recordings, including photographs,[743] video recordings,[744] and computer printouts.[745] Furthermore, system data, such as the computer logon record is direct evidence that a given account was used to log into a system at a given time.

Indirect or circumstantial evidence is evidence from which a fact in issue may be inferred.[746] Thus, indirect evidence is evidence of a relevant fact as opposed to evidence of a fact in issue.

---

[738] Malek, note 714, paras 1 – 10 to 1 – 16.

[739] C P Nemeth, *Law and Evidence: A Primer for Criminal Justice, Criminology and Legal Studies*, 2nd ed (Sudburry: Jones and Bartlett, 2011) 16.

[740] S Mason, "England & Wales" in S Mason (ed) *Electronic Evidence* (London: Lexis Nexis Butterworths, 2010), 301.

[741] Casey, note 637, at 72.

[742] In *R v Gilham* [2009] EWCA Crim 2293, 173 CL&J 749, the image on a screen was considered to constitute sufficient evidence of data copied on to the RAM of a computer used to play counterfeit games to establish an offence of breach of copyright.

[743] *R v Tolson* (1864) 4 F & F 103, 176 ER 488, where a photograph was admitted in a case of alleged bigamy to illustrate oral testimony; E Goldstein, "Photographic and Videotape Evidence in the Criminal Courts of England and Canada" (1987) *Criminal Law Review* 384.

[744] *Kajala v Noble* [1982] 75 Cr App R 149; R V Grimer [1982] Crim LR 674, 126 SJ 641; R v Thomas (Stephen) [1986] Crim LR 682.

[745] *R v Wood* [1983] 76 Cr App R 23.

[746] L-T Choo, note 713, at 7.

Most of the digital evidence that can be admitted as direct evidence also comprises indirect evidence. The computer logon record example above comprises indirect evidence that the individual who owns the account logged into the system, and therefore was responsible. However, someone else may have used the individual's account and other evidence would be required to prove that the suspect actually logged into the system.

Thus it can be concluded that digital data can generally be admitted as direct or indirect evidence in criminal court proceedings. The unique nature of this type of evidence does not exclude it from falling into one of the existing admissible evidence classes. However, other evidence principles could preclude the admissibility of digital evidence.

7.2.2.2 Best Evidence

Best evidence is a concept that can best be described as "the nature of the fact admitted, or the best evidence that the circumstances would allow, or the best evidence the party could produce.[747] Originally, the concept was relevant when dealing with the contents of a writing, recording, or photograph, where the original evidence was sometimes required to prevent a witness testimony from misrepresenting such materials.[748] Mason notes that this rule is no longer as relevant as it used to be, and now confined to written documents in the strictest sense.[749] Essentially, as Casey states, "with the advent of photocopiers, scanners, computers and other technology that can create effectively identical duplicates, copies became acceptable in place of the original, unless a genuine question is raised as to the authenticity of the original or the accuracy of the copy or under circumstances it would be unfair to admit the copy in lieu of the original."[750]

Generally, an exact copy of digital evidence can be created, and the presentation of the copy might even be preferable, because the original stored on the ICT device will not accidentally be altered.[751]

---

[747] Malek, note 714, para 7 – 40.
[748] Casey, note 637, at 64.
[749] Mason, note 740, at 309.
[750] Casey, note 637, at 64.
[751] See p. 215, for a discussion of the volatile nature of digital evidence.

However, this is not as straightforward if MIA tools collect the digital evidence. As discussed above in the short case scenario,[752] MIA tools seize the data from live systems, and therefore, the ICT device from which the data stems might not be available for a cross-checking. Even if it was seized after the search, the data in question might be lost.

Thus the best evidence rule might require that the target system be taken offline at the time of evidence collection. This would contradict the envisaged use of MIA tools, where the fact that the evidence is collected from live-systems is one of the key aspects of these tools. Hence, the question is whether the best evidence rule precludes the admissibility of digital evidence collected by MIA tools.

In *Bobo v State*, the judge decided that printouts of emails that no longer existed on the computer of the suspect because they had been deleted "were the best evidence of the emails originally exchanged."[753] This case is a strong indicator that evidence seized from live systems might still be regarded as the *best evidence* if certain technical standards are obeyed.[754]

No case similar to this has to date been decided on in England or Wales. However, given the current understanding of the best evidence rule, it seems likely that a similar decision would be reached.[755] Looking at the historical change of the best evidence rule also leads to this assumption. This rule has been amended and thereby lost in significance synchronously with technical advancements, which made the historical meaning of the rule obsolete (perfect copies could be produced). Thus under the condition that the authenticity of evidence seized from a live system can be verified, it can be assumed that the best evidence principle would not contradict the admissibility of digital evidence collected by MIA tools in court.

Thus it can be concluded that generally digital evidence is an admissible type of evidence in court proceedings in England and Wales.

---

[752] See p. 204f.

[753] *Bobo v State*, 2008 WL 2191159.

[754] See section 7.3, and chapters 8 and 9 for an introduction and discussion of a technical solution to this.

[755] See e.g. *Masquerade Music Ltd v Springsteen*; *Springsteen v Flute International Ldt*; sub nom. *Springsteen v Masquerade Music Ltd* [2001] EWCA Civ 563; [2001] C.P. Rep. 85; [2001] C.P.L.R. 369; [2001] E.M.L.R. 25, CA (Civ Div), where some of the relevant documents to prove a title to copyrights were missing, but the judge ruled that the best evidence rule has expired, and the presentation of the original documents was not necessary.

7.2.2.3 Exclusionary Principles – Improperly Obtained Evidence

However, evidence can be ruled inadmissible based on a number of exclusionary principles.[756]

Particularly relevant for digital evidence, and especially digital evidence seized by MIA tools is the principle of improperly obtained evidence.

Evidence can be excluded, as a matter of law or discretion, on the grounds that it was obtained illegally, improperly or unfairly.[757] Evidence can be obtained improperly, for example, by trickery, deception bribes, threats or inducements, or in violation of a person's human rights guaranteed by the *European Convention of Human Rights (ECHR)*. Particularly Article 8 ECHR, which guarantees the right to privacy, could be of relevance for digital evidence obtained remotely from ICTs and computer networks after infiltrating these.

As shown in chapter 2, this potentially violates privacy and data protection rights of affected persons, and hence would be obtained improperly.[758] Additionally, digital evidence obtained by MIA tools could be in breach of international legislation as shown in chapter 6 and therefore be obtained improperly on those grounds.

Principally, there is no automatic exclusion of improperly obtained evidence in England and Wales.[759] Courts have discretion whether to admit evidence that is improperly obtained in criminal cases, subject to the provision of s 78 of the *Police and Criminal*

---

[756] For the purpose of this thesis, the focus is solely on the principle of improperly obtained evidence. The use of MIA tools makes this the potentially most immediately relevant principle. For an overview of all exclusionary principles, see e.g. H L Ho, *A Philosophy of Evidence Law* (Oxford: Oxford University Press, 2008) 48-9, for discussion of all existing exclusionary principles.
While the hearsay principle is probably the most commonly known, this principal is no longer seen as problematic. It is based on the perceived unreliability of hearsay evidence (Teper v R [1952] AC 480, 486 per Lord Normand). However, the Criminal Justice Act 2003 repealed the provisions relating to hearsay in the Criminal Justice Act 1988 (Criminal Justice Act 2003, s.115). In any case, computer self-generated output is not hearsay but real evidence (R v Saward [2005] EWCA Crim 318 at 44). This category has two sub-divisions: firstly output that contains no input from human thought, such as that created by a web camera, or automated screen capture (R v Skinner [2005] EWCA Crim 1439 at 21). Secondly, computer self-generated output that draws directly or indirectly on information fed into the device by a person. The first category is admissible if legally relevant. The second is inadmissible unless it is proven to the judge's satisfaction that the information supplied was accurate (R Pattenden, "Authenticating 'things' in English law: Principles for adducing tangible evidence in common law jury trials" (2009) 12 The International Journal of Evidence & Proof, 273, 275).

[757] A Keane, *The Modern Law of Evidence* (Oxford, New York: Oxford University Press, 7th edition, 2008) 53.

[758] See the discussion of the BVerfG judgment in chapter 2.

[759] *R v P* [2002] 1 AC 146; *Attorney-General's Reference (No. 3 of 1999)* [20011 2 AC 91.

Evidence Act 1984.[760] Courts may refuse to admit evidence on which the prosecution propose to rely if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it under s 78.[761] It is, of course, impossible to list all the kinds of impropriety, which will be treated as having an adverse effect on the fairness of the proceedings here.[762]

However, principally this does not mean that in every case of a significant or even substantial breach the evidence in question will be excluded.[763] The task of the court is not merely to consider whether there will be an adverse effect on the fairness of the proceedings, but such an adverse effect that justice requires the evidence to be excluded.[764]

No case law exists, to the best knowledge of the author, on the exclusion of digital evidence (and particularly not digital evidence seized remotely) on the grounds that it was obtained improperly. However, cases of intercepted (and electronically recorded) communication improperly obtained can serve as a comparison here. Evidence of intercepted communications recorded electronically was not automatically inadmissible, even if the recording device had been placed by an illegal act, and on the premises of a third party,[765] and if the opportunity to plant it had been secured by deception.[766]

This can be compared to the investigation of the vitual living space by MIA tools. Even if the tools are planted illegally and communication data and other evidence is seized, this does not necessarily mean that the evidence is excluded from court proceedings. Intercepted communications data was excluded under the s 78 discretion when the police had, in bad faith, manipulated facilities for prisoners to be interviewed by their legal advisers so that these conversations could be overheard.[767] Thus only if and when confidential communication data was intercepted did courts in the past decide that this should be excluded as evidence.

---

[760] Mason, note 740, at 405.
[761] A Samuels, "Illegally Obtained Evidence: In or Out?" (2003) 67 *Journal of Criminal Law* 411-414.
[762] See e.g. Keane, note 757, at 57 ff; Allen, note 728, for more details on this.
[763] Keane, note 757, at 64.
[764] *R v Walsh* (1989) 91 Cr App R 161 at 163, CA and *R v Ryan* [1992] Crim LR 187, CA.
[765] *R v Khan* [1994] 4 All ER 426.
[766] *R v Chalkley* [1998] QB 848, [1998] 2 All ER 155.
[767] *R v Grant* [2005] EWCA Crim 1089, [2006] QB 60.

Applying these results to digital data, and particularly data seized by MIA tools, it can be concluded that such data is likely only excluded under the s 78 discretion if it was improperly seized confidential data.

7.2.2.4 Authentication of Digital Evidence

The previous sections have shown, that digital evidence is admissible in criminal proceedings, if it is relevant, can be considered an admissible evidence type, and is not otherwise excluded.

However, in addition documents and all other forms of tangible evidence must be authenticated, to establish the reliability of the evidence in question and show that they are what they purport to be. The term *authentic* is used to describe whether a document or data is genuine, or that the document (in the case of digital data) "matches the claims made about it".[768]

Authentication means satisfying the court (a) that the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate.[769]

To prove the aforementioned requirements, the identity, provenance, continuity, integrity, and originality of the evidence need to be established.[770]

Identity attempts to proof that two 'things' are the same.[771] *Provenance* refers to the mechanical or physical origin of the evidence.[772] *Continuity* is the chain of custody or transmission between seizure and examination by an expert or use in court.[773] *Integrity* determines whether deterioration, interference and contamination between seizure and examination has been avoided.[774] *Originality* refers to the original 'thing' in its initial state.[775]

---

[768] Pattenden, see note 756, at 275.
[769] C Reed, "The Admissibility and Authentication of Computer Evidence – A Confusion of Issues" (2005) 5th *BILETA Conference British and Irish Legal Technology Association*, 5.
[770] Pattenden, note 756, at 277.
[771] Wigmore, *Wigmore on Evidence*, 3rd ed., Vol. 7 (Boston: Chardbourn, 1940) §2129; *Boyle v Wiseman* (1855) 11 Ex. 360 at 367-8.
[772] *Trimcoll Pty Ltd v Deputy Commissioner of Taxation* [2007] NSWCA 307 at 30.
[773] *R v Stubbs* [2002] EWCA Crim 2254 at 16; *R v Early* [2002] EWCA Crim 1904 at 21; *R v Emu* [2004] EWCA Crim 2296 at 26.
[774] *R v Hoey* [2007] NICC 49 at 46.
[775] *R v Robson* [1972] 1 WLR 651 at 653, 655.

As established above,[776] digital evidence is a particularly volatile and fragile type of evidence. It can easily be tainted and altered in many ways. Thus proving the integrity of this type of evidence is much more difficult than doing so with a piece of physical evidence, such as a knife. This can be photographed at the crime scene, to establish identity and provenance, placed in a clean bag to avoid contamination, and therefore establish integrity and originality. The chain of custody is established by documentation of the people coming in contact with the piece.[777]

For digital data, the establishment of authenticity, and therefore of the above-mentioned criteria, incorporates a technical process of a protocol of checks and balances to demonstrate the history of how the digital data has been managed since its seizure.[778] It can be argued that the process of demonstrating the authenticity of a digital object is "a process of examining and assigning confidence to a collection of claims."[779] Proving the authenticity of a digital object means providing sufficient evidence to convince an adjudicator that the object that has been retrieved is a faithful representation of the object that was relied upon by the originator.[780]

The technical process required for seizing and analysing digital evidence in a way that allows later authentication during court proceedings needs to be undertaken by a forensic expert.[781] As shown above in the short case example, digital evidence is latent to the human eye, and it requires an expert to make it visible and ensure that it remains in its original state.[782] This process is complex and very technical, and only the basic structure will be depicted in this thesis.[783]

Generally, whether examining digital data acquired from a desktop drive, mobile phone memory, or network trace, a forensic examiner must ensure the integrity of the entire

---

[776] See p. 214ff.

[777] Casey, note 637, at 470.

[778] S Mason, "Authenticating Digital Data" in S Mason (ed) *Electronic Evidence* (London: Lexis Nexis Butterworths, 2010), 89.

[779] C Lynch, Authenticity and integrity in the digital environment: An exploratory analysis of the central role of trust" in *Authenticity in a Digital Environment* (2000), Council on Library Information Resource, 40.

[780] Mason, note 778, at 90.

[781] Casey, note 637, at 471.

[782] See p. 204ff.

[783] For a detailed analysis and discussion of this process see e.g. Casey, note 637, at 227 ff.

investigation.[784] At the most basic level, digital forensics has three major phases: 1) acquisition, 2) analysis, and 3) presentation.[785] The entire process is based on the forensic science paradigm depicted above in section 7.1.3.[786]

The acquisition phase saves the state of a digital system, so that it can be analysed later.[787] To ensure that the digital evidence remains intact, the evidence containing ICT system is taken offline and a bit-stream image of the entire original evidence disk is created.[788] This process, known as "bit-stream imaging", involves copying all data from the original disk, sector-by-sector, to a target working disk or image file.[789] Forensic tools are used to accomplish this.[790] These tools must modify the suspect device as little as possible and copy all data.[791]

The analysis phase takes the acquired data and examines it to identify relevant pieces of evidence.[792] The examination of the data is carried out on the created copy to ensure that the original is kept intact. Again, forensic tools are used to analyse and examine the relevant data. Throughout this process, the chain of custody of the digital evidence is ensured by properly marking and identifying the hardware seized, tracking and maintaining all the required signatures, secure storage, and properly time-stamping digital documents, and archiving system logs.[793]

Thus the process heavily relies on the validity of the methods, and the forensic soundness and verification of the specific tools that are used.

To ensure the methods are valid and consistent, general guidelines on good practice for computer-based electronic evidence have been introduced in the UK[794] by the

---

[784] B N Levine, M Liberatore, "DEX: Digital Evidence Provenance Supporting Reproducibility and Comparison" (2009) *DFRWS Annual Conference*, 1.

[785] B Carrier, "Open Source Digital Forensics Tools: The Legal Argument" (2002) *@stake Research Report*, 2.

[786] See p. 222.

[787] Carrier, note 785, at 2.

[788] Kenneally, note 639, at 12.

[789] Ibid.

[790] An example for such a forensic tool is EnCase, http://www.guidancesoftware.com/forensic.htm.

[791] Carrier, note 785, at 2.

[792] Ibid.

[793] P Turner, "Digital provenance – interpretation, verificaton and corroboration" (2005) 2 *Digital Investigation*, 45, 48.

[794] While the focus of this chapter is on England and Wales only, these guidelines are drafted to include Scotland and Northern Ireland (see p. 2).

Association of Chief Police Officers' (ACPO).[795] While some authors have doubted the validity of such guidelines, and of existing methods,[796] these are generally accepted in the literature as a sound basis.[797]

The verification of the reliability of the tools used, and the reliability of the evidence collected with these is a somewhat different matter. Evaluating them as scientific evidence has challenged these tools and the techniques used to process digital evidence. Because of the power of science to persuade, courts are careful to assess the validity of a scientific process before accepting its results.

In the United States, scientific evidence is evaluated based on the principles developed in *Daubert v Merrell Dow Pharmaceuticals, Inc., 1993*,[798] and the Federal Rule 702.[799]

At present, no legislated equivalent to the Daubert test, or the Federal Rule 702 exists in England and Wales (or other parts of the UK). The position is that where the court needs assistance, a reliable body of relevant knowledge exists, and a suitably qualified expert[800] can render an opinion on the issue at hand, the court will call such evidence.[801] Thus the common law in England and Wales requires the court to be satisfied that the scientific evidence is "sufficiently reliable" in order for it to be admitted.[802]

The Law Commission (LC) in its report on admissibility of expert evidence in criminal proceedings[803] proposed that a Daubert-like test, enshrined in legislation alongside a list of guidelines for the court to consider (namely, the admission of expert evidence

---

[795] ACPO, "Guide for Computer-Based Electronic Evidence" available online at http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

[796] See e.g. M Reith, C Carr, G Gunsch, "An Examination of Digital Forensic Models" (2002) 1:3 *International Journal of Digital Evidence*, for a discussion of existing guidelines.

[797] See e.g. Casey, note 637, at 230.

[798] *Daubert v Merrell Dow Pharmaceuticals* 509 US 579 (1993).

[799] The Daubert decision (replacing the Frye test, which relied on scientific acceptance as the sole criteria; *Frye v United States* 293 F 1013 (1923)) and Rule 702 of the Federal Rules of Evidence altered and expanded the indicia that judges should consider in ruling on the admissibility of expert evidence. The Court looked not only to acceptance by the scientific community, but also considered whether the theory/technique had been tested, subject to peer review and publication, had a known or potential error rate, and was the subject of standards as to its application and operation.

[800] By study or experience (*R v Hodges* [2003] EWCA Crim 290) although in some fields qualifications may be of increased importance (*R v Robb* [1991] 93 Cr App R 161).

[801] Wheate/Jamieson, note 715, at 6.

[802] *R v Dallagher* [2002] EWCA Crim 1903 at [29]; *R v Ciantar* [2005] EWCA Crim 3559 at [25].

[803] The Law Commission "The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales: A New Approach to the Determination of Evidentiary Reliability" (2009) Consultation Paper 190.

which is relevant, scientifically valid, and proffered by a witness who is an expert, and exclusion of evidence that fails those standards) should be introduced,[804] to avoid miscarriages of justice due to the current practice.[805]

However, to date no such test has been introduced, thus the traditional approach of receiving the opinion of an expert on the tools and methods in question continues. Thus far, digital evidence processing tools and techniques have withstood scrutiny when evaluating scientific evidence.[806]

However, what has become clear when analysing the above authentication methods for digital evidence, is that these are premised on physical interaction with a static system, and the seizure of the system by a human officer, obeying to a generally accepted method.

MIA tools, however, seize evidence remotely from live systems. As shown in the case example above,[807] this means that no original, of which a bit-stream image could be created, exists. Therefore, the identity and provenance of the data collected are questionable, and thus the authenticity of the evidence cannot be established.

It can therefore be concluded, that generally digital evidence can be authenticated under the current legal framework in England and Wales.

However, the authentication of digital evidence collected by MIA tools based on the current methods for authentication is not possible.

This means that digital evidence collected by MIA tools can be classified as an admissible evidence type; however, it will most likely be considered unreliable.

7.2.3 The Admissibility of Digital Evidence – Germany

This section aims to introduce the main structure and principles of the German evidence law in criminal proceedings, and analyse whether the existing legal framework is sufficient and adequate to deal with matters of admissibility of digital evidence (standard digital evidence and that collected by MIA tools).[808]

---

[804] The Law Commission, ibid, at Part 6.

[805] The Law Commission recognises that miscarriages of justice have occurred under the existing system, and goes into some detail outlining a few examples, The Law Commission, ibid, at 2.13-24.

[806] Casey, note 637, at 75.

[807] See p. 204ff.

[808] This is by no means an account of the existing evidence law in its entirety in Germany, nor meant to be. See e.g. C Roxin, H Achenbach, *Strafprozessrecht* (München: Beck, 2006, 16th ed), for an extensive discussion of the law of evidence in Germany.

The law of evidence for criminal procedures is rooted in Germany in the *German Federal Criminal Procedure Act* (Strafprozessordnung - StPO).[809]

It is premised on two main principles: the principle of judicial investigation (§§ 155 II 2, 160 II, 244 II 2 StPO), and the principle of free assessment of evidence (§ 261 StPO). These two principles greatly influence the admissibility of evidence in criminal proceedings.

The principle of judicial investigation (*Untersuchungsgrundsatz*) according to §§ 155 II 2, 160 II, 244 II 2 StPO, obligates the court to investigate the truth. It further states that all relevant pieces of evidence need to be evaluated.[810] The introduction of evidence at trial serves the investigation of facts and other matters relevant to the court's decision. Thus, presentation and evaluation of the evidence is the core of the trial and the primary task of the court.

The reason for this is that the aim of the criminal procedure is to establish the true facts to enable a fair judgment.[811]

According to § 261 StPO, the court decides in criminal proceedings about the value of the proffered evidence on the basis of convictions formed in the course of the proceedings. This is the principle of the judge's 'free assessment of evidence' (*freie Beweiswürdigung*). The judge is thus not bound by any formal rules in deciding whether a fact has been proven or not.[812]

The process of establishing the truth in criminal proceedings requires that the judge gains a personal certainty about the relevant facts.[813] However, the principle of *in dubio pro reo* establishes that the accused enjoys the benefit of the doubt, thus after evaluating the evidence, the court needs to be convinced of the guilt of the accused beyond reasonable doubt.[814]

The above-described principles highlight that the question of evidentiary weight under German law is premised on the discretion and opinion of the judge, as opposed to English law, where the focus is on the specifics of the evidence.

Thus the judge has the power to determine whether a fact is proven by a proffered piece of evidence.

---

[809] As amended and promulgated on 7th April 1987.
[810] K Haller, K Conzen, *Das Strafverfahren* (Heidelberg, München: C.F. Müller, 2008) 7.
[811] BGH, NJW 2005, 1442.
[812] U Hellmann, *Strafprozessrecht* (Berlin, Heidelberg: Springer, 2006, 2nd ed) 280.
[813] OLG Celle, NJW 1976, 2030,2031.
[814] Haller/Conzen, note 810, at 14.

The question of admissibility of evidence, however, is more restricted and premised on the regulations in the German criminal procedure code.

Traditionally, the criminal procedure law in Germany recognises physical objects as evidence.[815] As highlighted in the case scenario above, this could be a knife or a document.[816] The question is therefore whether digital data is recognised as a means of proof by German criminal procedure law.

As analysed above, digital evidence fundamentally differs from physical evidence.[817] Most significantly, it is latent to the human eye. Therefore, data as such is not recognised as a means of proof under criminal procedure law.[818]

However, it is generally accepted that if digital data is stored on a data storage medium, this medium can be proffered as evidence into criminal proceedings.[819] Nevertheless, the problem of introducing the digital data stored on the device as evidence remains. As discussed above,[820] digital data can only be of relevance, if it is transformed into readable format, on screen or as printouts. These outputs could therefore be proffered as evidence into criminal proceedings.

Criminal procedure law only recognises those types of proof that are specified in the Criminal Procedure Code. Digital data in readable format therefore must fall into these recognised classes of evidence.

7.2.3.1 Types of Evidence

The Criminal Procedure Code recognises 4 different classes of permissible evidence:

- Witness (§ 48 ff StPO)
- Expert (§ 72 ff StPO)
- Certificate (§ 249 ff StPO)
- Observational evidence (*Augenscheinbeweis*) (§§ 86 ff, 225 StPO)

---

[815] M Gercke, P W Brunst, *Praxishandbuch Internetstrafrecht* (Stuttgart: Kohlhammer, 2009) 374.

[816] See p 204.

[817] See p 214ff.

[818] Gercke/Brunst, note 815, at 374.

[819] See e.g. BVerfGE, 113, 29, where the German Federal Constitutional Court decided that digital data from seized data storage media can be used as evidence in criminal proceedings.

[820] See p 214ff.

Proof by witness and expert is thereby classed as personal proof, whereas proof by certificate or visual inspection is classed as factual proof.[821]

Proof by witness (§ 48 ff StPO) refers to the statement of a person about his own perception of facts in question.[822] Perception in this context also encompasses information the witness has heard from a third person about the matter in question (i.e. hearsay, which German law does not exclude as evidence).[823]
A witness, such as a police officer present at the search, can make a statement about digital data perceived on the screen of an ICT device. Thus, digital data could be introduced indirectly, through the perception of a witness. Such a proof could be relevant, if certain data was visible on the screen but later, for example, deleted from the hard disk. However, such proof by witness needs to be handled with great care, since perceptions can be very subjective, and in particular if the data cannot be reconstructed at a later stage.[824] Knopp therefore excludes proof by witness for digital data, though justifying this only generally stating that this is an unsuitable means of proof for digital data.[825] Generally, this means of proof should not be excluded outright, however, the weight of evidence in this form will probably be very low in court proceedings, and can only be used to back up other facts.

Expert witnesses (§ 72 ff StPO) are primarily assistants to the court. They provide expertise, which the court lacks.[826] The expert witness has three potential functions. Firstly, he may acquaint the court with general matters of knowledge and experience established within his area of expertise. Secondly, he may determine facts that may only be perceived, understood or assessed on the basis of particular knowledge. And thirdly, he may use scientific principles and methods to draw inferences from facts.[827]

---

[821] W Beulke, *Strafprozessrecht* (Heidelberg, München: C.F. Müller, 2010, 11th ed) 116; Hellmann, note 815, at 248.
[822] O Klemke, H Elbs, *Einführung in die Praxis der Strafverteidigung* (Heidelberg, München: C.F. Müller, 2010) 275.
[823] Beulke, note 821, at 270.
[824] Gercke/Brunst, note 815, at 375.
[825] M Knopp, "Rechtliche Perpektiven zur digitalen Beweisführung" (2009) *Proceedings of GI Jahrestagung'2009*, 1552-1566.
[826] Beulke, note 821, at 126.
[827] See for a detailed analysis: F Toepel, *Grundstrukturen des Sachverständigenbeweises im Strafprozessrecht* (Tübingen: Mohr Siebeck, 2002).

Therefore, an expert witness can also indirectly introduce digital evidence during court proceedings. He can, for example, be requested by the court to examine seized ICT devices and report about the content and reliability of the devices. Thus a forensic examiner can, as an expert witness, provide proof of digital evidence in criminal proceedings. This method of proof for digital evidence is undisputed in literature.[828]

In addition to these two personal means of proof, the factual methods of proof could introduce digital evidence directly into criminal proceedings.

A certificate under criminal procedure law (§ 249 ff StPO) refers to a document with a readable thought content.[829] In criminal procedural law, the author of the document does not need to be recognisable (e.g. by signature).[830] Importantly, the focus of this proof is on the readable content of the document, not the outer appearance of the document.
Digital data can therefore be introduced into criminal procedures in form of readable printouts that constitute certificates according to § 249 StPO.[831] However, only if it is a readable reproduction of digital data stored on the device (such as a word processing document).

Observational evidence (§§ 86 ff, 225 StPO) is derived from the sensory perception of persons or things by sight, hearing, touch, taste, or smell.[832] This includes, for example, the viewing of corpses, weapons, and pictures or movies. It also includes listening to recordings.[833]
All digital data that does not satisfy the requirements of readable content can therefore be classified as observational evidence.[834] Digital data in form of a printout of a screenshot, or of an image can therefore be proffered as observational evidence into criminal procedures.[835]

---

[828] See e.g. Knopp, note 825, at 8; Gercke/Brunst, note 815, at 376.
[829] Beulke, see note 821, at 129.
[830] Note that the meaning of certificate in criminal procedure law differs from that in civil procedure law and criminal law. In civil law, for example, a signature is required for a document to be considered a certificate.
[831] Gercke/Brunst, note 815, at 374.
[832] BGHSt, 18, 51, 53; Beulke, note 821, at 130.
[833] BGHSt 14, 339.
[834] Böckenförde, note 188, at 313.
[835] Gercke/Brunst, note 815, at 374.

Therefore, both types of factual evidence are applicable to digital data. The reason why German criminal procedure law is relatively flexible as to admissibility of digital evidence is, as stated above, that it is premised on the principal of judicial investigation, which obligates the court to determine the truth.[836] The introduction of evidence at trial serves the investigation of facts and other matters relevant to the courts decision (§ 244 II StPO). Thus, presentation and evaluation of all available evidence is at the core of the trial and the primary task of the court.[837]

7.2.3.2 Authenticity of Digital Evidence

The previous section has shown that digital evidence is generally admissible under German criminal procedural law, if it can be subsumed under one of the evidence classes. However, the weight of the evidence is to be freely assessed by the judge (§ 261 StPO).[838] Generally, this assessment takes into consideration the authenticity and integrity of evidence, and the credibility of witness statements.

The authenticity and integrity of evidence derived from digital data is generally problematic.[839] As established above,[840] digital evidence is a particularly volatile and fragile type of evidence. It can easily be tainted and altered in any way. Thus proving the authenticity and integrity of the evidence is much more difficult than doing so with a piece of physical evidence.

The process of establishing authenticity of evidence is less structured under German criminal procedural than it is in England and Wales. The reason is that it is the discretion of the judge to decide whether evidence is authentic and reliable. However, as a general rule judges rely on forensic examiners to determine the authenticity of digital evidence, and forensic science plays an important role in ensuring that digital evidence is authentic and reliable.[841] This technical process is the

---

[836] See p. 241.
[837] Even though exclusionary principles for evidence exist. See Roxin, note 808 for a discussion of this.
[838] See p. 241.
[839] Böckenförde, note 188, at 317; Gercke/Brunst, note 815, at 376.
[840] See pp. 214ff.
[841] Gercke/Brunst, note 815, at 376.

same in Germany, as it is in England and Wales. Therefore, the analysis above in section 7.2.2.4 for details of this process is applicable.[842]

In essence, a bit-stream image of the seized ICT device should be created, and all examination undertaken on this copy.

The German ministry for security in information technology has issued a guideline for "IT-Forensic" that is equivalent to the ACPO guidelines, and serves to ensure that the forensic science methods applied are standardised, and therefore reliable.[843]

The approach to determine authenticity of digital evidence is therefore to receive the opinion of an expert on the tools and methods in question. Generally, courts have admitted digital evidence that has been seized and examined in line with the best practice guidelines developed in forensic examinations.

However, as discussed above,[844] the guidelines have been developed with static systems in mind. Digital evidence seized from live systems using MIA tools challenges these best practice guidelines, and it seems questionable that a forensic expert could positively comment on the reliability and authenticity of such evidence.

This is confirmed by recent case law. A defendant was acquitted of blackmail because the relevant digital evidence was seized from his computer instead of creating a bit-stream image, and working on the copy. The court found that it could not be proven beyond reasonable doubt that during the examination process, a third person implanted the evidence on the computer.[845]

This decision is in line with the above described *in dubio pro reo principle*.[846]

Thus it can be concluded that generally digital evidence is admissible in both jurisdictions of England and Wales, and Germany.[847] However, digital evidence seized

---

[842] See p. 237 onwards, see also Gercke/Brunst, note 815, at 376, referring to English scientific literature for an overview of the forensic examination process.

[843] Bundesamt für Sicherheit in der Informationstechnik, Leitfaden "IT-Forensik", Version 1.0 (September 2010) available online at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile.

[844] See p. 240.

[845] P Mühlbauer, "Wie verlässlich sind digitale Beweise?" (2007) *Telepolis*, available online at http://www.heise.de/tp/r4/artikel/24/24638/1.html; in this case the accusation rested entirely on the digital evidence, thus the decision to acquit the accused of the offense. In other cases, the judge would merely consider the weight of the evidence to be minimal, or the evidence inadmissible.

[846] See p. 241.

by MIA tools challenges existing legal frameworks, and the conclusion of the above analysis, in absence of any case law dealing with this specific matter, is that this is currently inadmissible in both jurisdiction: England and Wales, and Germany.

7.3 A Scientific Solution?

The likely inadmissibility of digital evidence collected by MIA tools poses a problem for the future use of these technologies. If the evidence seized by these investigative tools cannot be admitted in court proceedings, the value of these tools is limited.
As discussed above,[848] science has historically provided a foundation for legal proceedings. As shown there, this is particularly the case in forensic science. The existing guidelines for the best handling of digital evidence evolved from this confluence of science and law. The above-depicted paradigm of forensic science (see Figure 1) reflects this interaction.

Thus, the question is whether scientific research has produced findings that could be applied to the authentication problem of digital evidence collected by MIA tools. Such findings would need to acknowledge the principles and processes developed for the forensic science paradigm, and be consistent with the best practice regulations of forensic computing.

The need for remote live evidence acquisition has been recognised by several authors, and scientific research has been undertaken to develop robust methods to collect reliable and authentic digital data.[849]

---

[847] The research for this chapter has shown that this is generally the case in most countries. See e.g. Casey, note 637; S Mason (ed) *Electronic Evidence* (London: Lexis Nexis Butterworths, 2010) covering Australia, Canada, England & Wales, Hong Kong, India, Ireland, New Zealand, Scotland, Singapore, South Africa and the United States of America; S Mason (ed), International Electronic Evidence (London: British Institute for International and Comparative Law, 2008) covering Argentina, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, Norway, Poland, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Thailand and Turkey; O Leroux, "Legal Admissibility of Electronic Evidence" (2004) 18:2 *International Review of Law, Computers & Technology*, 193, for a comparison between common law and civil law countries.

[848] See section 7.1.3 p 217ff.

[849] See e.g. Kenneally, note 639; Nikkel, note 640; A Case et al., "FACE: Automated digital evidence discovery and correlation" (2008) 5 *Digital Investigation* 65; F Adelstein, "Live Forensics: Diagnosing Your System Without Killing it First" (2006) 49:2 *Communications of the ACM*, 63; R Koen, M Olivier, "An Evidence Acquisition Tool for Live Systems" in I Ray, S Shenoi (eds.) *IFIP International Federation for Information Processing, Volume 285; Advances in Digital*

Generally, this research has established that the same types of data can be analysed using dead and live analysis techniques.[850] This is an important finding, highlighting that investigations of the virtual living space, such as online searches by MIA tools are apt to produce the same evidence that common digital examinations of bit-stream images can produce.

However, considering the legal requirements, the difference between live and dead analysis is the reliability of the results.[851] Thus Koen and Olivier establish that it is important to ensure that digital evidence is not modified during a live acquisition process.[852] Walker observes that even a single file timestamp found to be later than the date of acquisition may cause digital evidence to be declared inadmissible in court.[853] Hence, the ability of the operating system to update the file access time is useful for system administrators, but it is highly undesirable for digital forensic investigations. Thus one important finding is that the use of standard file access routines should be avoided during live acquisition.[854]

Therefore, live acquisition software should have the capability to perform low-level file access without the help of the operating system, and access all files in read-only mode to preserve the integrity of file data and metadata.[855]

To satisfy these requirements, Koen and Olivier have developed the *Reco Platform*, which provides low-level functionality for live acquisition tools.[856] Tools based on this platform can be used to access files on a live target without compromising the state of the files and their metadata.

Thus, developing MIA tools based on this platform would enable the examination and seizure of data without altering the original data stored on the ICT tool. However, there

---

Forensics IV (Boston: Springer, 2008) 325; B Carrier, *"Risks* of live digital forensic analysis" (2006) 49:2 *Communications of the ACM*, 56; C Hosmer, "Digital Evidence Bag" (2006) 49:2 *Communications of the ACM*, 69; P Turner, "Selective and intelligent imaging using digital evidence bags" (2006) 3 *Digital Investigation*, 59; G Richard, V Roussev, "File System Support for Digital Evidence Bags" M Olivier, S Shenoi (eds) *Advances in Digital Forensics II* (New York: Springer, 2006) 30.

[850] B Carrier, ibid, at 59.

[851] Ibid.

[852] Koen/Olivier, note 849, at 326.

[853] C Walker, "Computer Forensics: Bringing the Evidence to Court" (2007) *infosecwriters*, available online at http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf.

[854] Koen/Olivier, note 849, at 326.

[855] Casey/Stanley, note 637, at 285.

[856] Koen/Olivier, note 849, at 327.

are significant limitations to this approach. Firstly, access to files stored on the ICT tool in a logical partition requires administrator privileges. Secondly, access to file system data is by no means absolute – the low-level data access mechanism can be bypassed by sophisticated kernel rootkits.[857]

Hence, this approach provides a promising starting point for developing live remote acquisition tools that do not alter the data on the target ICT tool. However, in its current state, the platform does not support the access rights necessary for successful searches deploying MIA tools.

Another critical problem that arises from the use of MIA tools for evidence seizure from live systems is the storage of the data during the seizure, and the guarantee of the chain of custody. As discussed above,[858] if it cannot be proven that the digital data has not been altered or modified during and after the seizure and examination, its authenticity cannot be proven.

This problem could be solved by the concept of a digital evidence bag (DEB).[859] The DEB was developed to create a digital evidence container that metaphorically mimics the familiar plastic evidence bag used by crime scene investigators to collect physical crime scene evidence.[860]

Turner explains further "a DEB is a universal container for digital information from any source. It allows the provenance of digital information to be recorded and continuity to be maintained throughout the life of the exhibit."[861] DEBs bundle digital evidence, associated metadata and audit logs into a single structure, providing an audit trail of operations performed on the evidence as well as integrity checks.[862]

Therefore, a DEB application integrated into a live acquisition tool, such as a MIA tool, would ensure that the digital data remains in its original state, and could prove identity and provenance requirements, thus establish authenticity of the digital data.

The above-presented scientific findings have shown that relevant research is undertaken to develop applications that ensure the reliability and authenticity of digital data seized from live systems with remote acquisition tools, such as MIA tools. The

---

[857] Koen/Olivier, note 849, at 332.
[858] See p. 236ff.
[859] Hosmer, see note 849, at 69.
[860] Ibid.
[861] Turner, see note 849, at 61.
[862] Richard/Roussev, see note 849, at 30.

analysis of these findings has highlighted that the research is in line with the forensic paradigm, and incorporates the legal authentication principles. This means that any reliable and robust results are likely to stand in court.

However, the analysis has also revealed that the research is currently still in its infancy,[863] and thus far only partially usable for MIA tools. It has also revealed that some critical problems have yet to be solved. Most significantly, the lack of a static original system, that can serve to compare the evidence with to prove that the data originated from the ICT system in question, as suggested by the evidence. Solving this is more difficult, and it remains to be seen whether a proven chain of custody (such as through DEBs), including metadata that shows the origins of the data, is sufficient and adequate to establish authenticity and therefore admissibility of the data in criminal court proceedings.

7.4 Conclusion

This chapter has analysed and examined the admissibility of digital evidence in criminal proceedings with a focus on England and Wales, and Germany.

It has shown that the characteristics of digital evidence are fundamentally different from those of traditional physical evidence.[864] Therefore, this new type of evidence challenges existing legal frameworks regulating the admissibility of evidence.

However, digital evidence is not the first new type of evidence to challenge existing legal concepts and frameworks. DNA evidence, for example, was treated initially with great caution, until guidelines and best practice principles had evolved.[865] Such guidelines and principles resulted from the application of scientific findings to the law. This convergence of disciplines has a long history in evidence law, and has resulted in the emergence of forensic science.

Forensic science has generated principles and standards for the handling of evidence that are also applicable to digital evidence.[866] These principles set out the proper

---

[863] Generally, scientific findings need to be widely accepted by the scientific community to establish authenticity of evidence. This could be the case, if findings are published in peer-reviewed journals and confirmed by other scientists. Some authors have raised concern about the general validity of findings in forensic science, claiming the community is so small, that general acceptance cannot be established (see e.g. Wheate/Jamieson, note 715, at 8 with further references).

[864] See p 214.

[865] See e.g. L L Swafford, "Admissibility of DNA Genetic Profiling Evidence in Criminal Proceedings" (1990) 18:1 *Pepperdine Law Review*, 123.

[866] See p 236ff.

handling and examination of evidence to ensure that it is authentic and reliable, and therefore admissible during court proceedings.
The authenticity of digital evidence can be assessed based on these principles, and past case law has evidenced that these methods have stood in courts.

However, the above analysis has also highlighted that digital evidence collected by MIA tools challenges these principles and existing legislation. Existing methods proving authenticity of digital evidence were developed with static systems in mind, and generally accepted techniques to examine digital evidence and ensure the chain of custody is intact are based on the interaction with offline ICT systems and the examination of copies.

The techniques used to remotely seize and examine digital evidence with MIA tools are fundamentally different, and therefore the admissibility of this evidence questionable.

However, as stated above, it seems a reoccurring pattern that new types of evidence challenge existing legal frameworks. Scientific findings have traditionally bridged the gap between technological possibilities and legal uncertainties. Current research findings already indicate that this could also be true for digital evidence collected remotely from live ICT systems by MIA tools. Significantly, however, here the focus is on modifying the tool itself to ensure that the forensic science principles are obeyed.

This bears a resemblance with the conclusion of the previous chapter, where the best solution to the cross-jurisdictional investigation problem appeared to be a modification of the tool to obey existing international legislation.[867]
Whether this is indeed the best option to regulate the use of MIA tools, and enable the use of the evidence collected by these tools is discussed in the following chapters.

[867] See p 201.

8 MIA LAW

The previous two chapters (6 and 7) have highlighted how the new cyber-policing system with its novel investigative tools challenges existing legislation regulating criminal investigations. The substitution of human officers by cyber-cops, and human discretion by technical intelligence and automation for the investigation of the virtual living space causes problems for the traditional law enforcement system, which is still tied to traditional concepts of policing.

So far, this new cyber-policing system has evolved without any clear legal structure and few restraints. The focus has predominantly been on the technical development of the new technologies. The reasons for this are twofold: Firstly, the increasing widespread of ICTs has changed society and crime.[868] As a result, law enforcement requires novel investigative methods to enable the policing of the virtual living space. To keep up with the technological progress, the focus has been almost solely on the development of new technologies, and legal considerations have largely been left aside.
Secondly, the current policing system of new technologies tends to focus on the ex-ante authorisation or prohibition of individual technologies. Chapter 6 has shown how difficult, and often even impossible, it is to reach consensus among the international community on the regulation of a single software-based investigative method (i.e. the online search).
Thus the current regulatory system in place has facilitated the evolvement of a new cyber-policing system without any or very little adequate regulation in place.

The judgment of the BVerfG has emphasised how important a sustainable regulatory approach is for this new class of investigative tools to avoid rights violations of affected people.[869] Additionally, the previous two chapters have highlighted that the existing legal framework prevents MIA tools from reaching their maximum utility during investigations (the seized evidence is likely to be dismissed during court proceedings)[870] and cannot prevent actions that violate international law.[871]

---

[868] See chapter 1 at 20.
[869] See chapter 2 for the discussion of the development of the new fundamental right.
[870] See chapter 7.
[871] See chapter 6.

The existing legal framework particularly struggles with the complexity of MIA tools, and their unique abilities, which set them apart from traditional investigative tools and turn them into autonomous entities. However, this complexity can also serve as a solution for the current regulatory problem. The previous chapters have indicated how the software code of MIA tools could be used to enable law-compliant behaviour.[872]

Software code as a regulatory means is not a new concept. In his influential book *Code and Other Laws of Cyberspace*, Lessig was among the first to develop a notion of *code as law*.[873] He reveals how architecture (software code) can be designed or changed to realise and enforce norms.

Brownsword and Yeung find that the *Rule of Law*, the traditional approach of regulating technologies through legislation, might be inadequate for future regulation of software-based investigative tools.[874] Instead, they claim that the Rule of Technology is displacing the traditional Rule of Law.[875]
Koops states that "technology increasingly enforces or supplements law as an important regulatory instrument."[876]

Hence, the question is whether the complex software code of MIA tools that currently challenges the law, could be modified to make these tools law-complicit.

In section 8.1 the concept of regulation through code as introduced by Lessig and others is discussed. In section 8.2 the integration of values into technology is discussed as a link between Lessig's notion, and the notion of Ambient Law discussed in section 8.3. Section 8.4 develops the concept of MIA Law. Section 8.5 discusses the technical

---

[872] See pp. 200ff, 251.
[873] Lessig (1999), note 24; Lessig (2006), note 627.
[874] R Brownsword, K Yeung, "Regulating Technologies – Tools, Targets and Thematics" in R Brownsword, K Yeung (eds) *Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes* (Oxford, Portland: Hart Publishing, 2008) 3.
[875] Ibid.
[876] B-J Koops, "Criteria for Normative Technology – The Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values" in R Brownsword, K Yeung (eds) *Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes* (Oxford, Portland: Hart Publishing, 2008) 157.

and legal risks of law-complicit technologies. Section 8.6 concludes with the most important findings of the chapter.

8.1 Code As Law – Modalities of (Technology) Regulation

The emergence and widespread of the Internet prompted a debate on the regulability of this new technology. Its unique nature required new regulatory approaches, since the traditional approach – regulation through law – was challenged by the new medium.[877]

This led to the development of regulation theories concerned with the governance of the Internet and its many applications.[878] These theories, which are still valid today, have fundamentally influenced academic thinking on Internet and ICT regulation.

8.1.1 Cyber-federalism

Initially, the debate focused on the question whether the newly evolved Internet could and or even should be regulated at all.

Cyber-libertarians, such as Johnson and Post, argue that formal and centralised regulatory mechanisms (such as laws) should and could not be applied to the Internet because they do not work in the context of this new technology. Instead, they propose that a decentralised decision-making mechanism, which they call "the law of the Internet" and "the law of the nets" should be applied to regulate this medium.[879]

Their argument is that the most successful regulatory model for the Internet is a form of "net federalism" or "decentralised, emergent law" that is the result of the complex interplay of individual decisions by users and system administrators.[880] More specifically, they argue that "Internet federalism looks very different from what we have become accustomed to, because here individual network systems, rather than territorially based sovereigns, are the essential governance units. The law of the Internet has emerged, and we believe can continue to emerge, from the voluntary adherence of large numbers of network administrators to basic rules of law, with

---

[877] The unique nature of cyberspace has been discussed elsewhere in this work. See e.g. p. 14.

[878] Arguably the most influential works developing these theories are: Lessig (1999), note 24; Lessig (2006), note 627; L Lessig, "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 *Harvard Law Review* 501; J Reidenberg, "Lex Informatica" (1998) 76 *Texas Law Review* 553; Johnson/Post, note 477.

[879] Johnson/Post, note 477, at 90.

[880] Johnson/Post, note 477.

individual users "voting with their electrons" to join the particular systems they find most congenial."[881]

Essentially what Johnson and Post suggest is a form of self-regulation.[882] It is therefore not a suitable theoretical model for Internet regulation, but rather a political and moral concept applied to the new technology. It follows the directions of Barlow's *Declaration of the Independence of Cyberspace*, where he argues that regulators of the offline world (i.e. governments) have no sovereignty over cyberspace, and should refrain from any regulatory attempts of the Internet.[883] While there is an important underlying argument, namely that the Internet and associated technologies can and are regulated by more modalities than government enacted laws, the cyber-federalism approach is insufficient for the regulation of the Internet as it exists today, where economic factors are at the forefront of the development, and the average user profile has changed significantly from the late '90s.

In addition, cybercrimes have developed and increased immensely. Problems like spam, viruses, identity theft, the sexual exploitation of children, and cyber-terrorism have made a more structured approach to the regulation of the Internet a necessity. Self-regulation is therefore not an adequate option for the policing of the virtual living space by MIA tools.

8.1.2 Lex Informatica

Reidenberg in his work acknowledges that a more unified approach to Internet regulation is necessary to ensure that a stable environment is provided.[884]

He states that default rules and principles are essential for participants in the information society.[885] Such principles governing the treatment of digital information offer stability and predictability so that participants have enough confidence in the use of the Internet.[886] This is particularly important given the significance of the virtual living space.

---

[881] Johnson/Post, note 477, at 89.

[882] See e.g. L J Gibbons, "No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace" (1997) 6 *Cornell Journal of Law and Public Policy*, 475, for a discussion of the notion of self-regulation (as opposed to co-regulation and government regulation).

[883] J P Barlow, note 477.

[884] Reidenberg, note 878, at 553.

[885] Reidenberg, note 878, at 554.

[886] Ibid.

Reidenberg argues that in the digital realm, law and government regulation are not the best approaches to ensure that default rules and principles are enforced.[887] He observes that cyberspace, being a global network, challenges national concepts of law.[888] Reidenberg suggests as a solution to this problem the implementation of information policies into network designs and standards, and system configurations. He refers to this regulatory approach as *Lex Informatica*, thus comparing the newly emerging technology-embedded 'law' with the largely bottom-up-developed Lex Mercatoria of the Middle Ages.[889]

Reidenberg explains the notion further, stating, "in the context of information flows on networks, the technical solutions begin to illustrate that network technology itself imposes rules for the access to and use of information. Technological architectures may prohibit certain actions on the network, such as access without security clearances, or may impose certain flows, such as mandatory address routing data for electronic messages. Policy choices are available either through technology itself, through laws that cause technology to exclude possible options, or through laws that cause users to restrict certain actions."[890]

Reidenberg was among the first scholars to suggest that in cyberspace, the technology itself can constitute a means of regulation. That is the design of hardware and software can be amended to allow or disallow certain behaviour. He states that Lex Informatica has distinct enforcement properties, allowing for automated and self-executing rule enforcement. Technology standards may be designed to prevent actions from taking place without proper permission or authority.[891]

He identifies software designers (commercial and private), and users - through software configuration as the main developers of Lex Informatica, establishing the required principles through software design.[892] However, he also states that policymakers are able to influence this process, and should "add Lex Informatica to their set of policy instruments, and substitute this for law where self-executing, customised rules are desirable."[893]

---

[887] Ibid.
[888] Ibid.
[889] Ibid.
[890] Reidenberg, note 878, at 565.
[891] Reidenberg, note 878, at 568.
[892] Reidenberg, note 878, at 568.
[893] Reidenberg, note 878, at 578.

8.1.3 Lessig's Theorem

Lessig has developed a more comprehensive approach to cyberspace regulation, taking into account the complex synergies that exist between the different actors involved in the development and use of the Internet.[894]

His approach rests on the argument that four types of constraints in general regulate behaviour: laws, social norms, markets, and architecture (or code).[895]

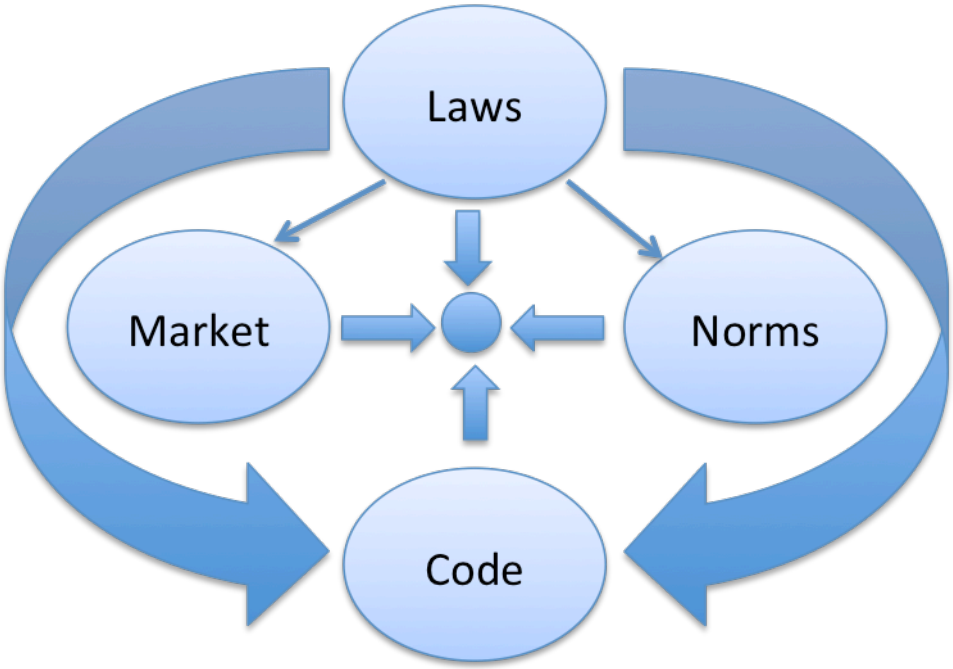

Figure 1: Four modalities of regulation (adapted from Lessig)[896]

Laws are the legal constraints that regulate behaviour. Laws typically regulate individual behaviour directly, and do so by threatening ex post facto sanctions.[897] Laws are the means of the traditional regulatory approach, which has functioned in the real world more or less successfully for centuries.[898] As illustrated in figure 1 above, laws, however, also regulate behaviour indirectly, by regulating markets, norms, and code.

---

[894] Lessig, note 24; Lessig, note 878.

[895] Lessig, note 878, at 506; Lessig (2006), note 627, at 123.

[896] Lessig (2006), note 627, at 130.

[897] G Greenleaf, "An Endnote on Regulating Cyberspace: Architecture vs Law?" (1998) 21:1 *University of New South Wales Law Journal*, 593, 604.

[898] This is not the place to review and assess the effectiveness of regulation through law in general. In criminology in particular, the effectiveness of the regulation through law has been questioned long before, and regulation through architecture has been researched as an alternative approach. This research is founded on the ideas of Foucault, M Foucault, Discipline

Similarly, law also regulates behaviour in cyberspace. Copyright regulations, defamation, and obscenity law are equally applicable to the online sphere, and threaten ex post sanctions for violations.[899] However, recent regulatory attempts have shown that law is not always suitable to regulate behaviour online.[900]

Norms, in the sense of social norms, are the bundle of publicly accepted and unaccepted behaviour. Like law, norms regulate behaviour by threatening punishment ex post.[901] But unlike law, as Lessig highlights, the punishment of laws is not centralised. Norms are enforced (if at all) by a community, not by a government.[902] Greenleaf explains this further, stating that "social norms, for example, cause us to frown on racist jokes, to tell the truth about our age where concessions might be available, and to observe other conventions both because we have been brought up to feel guilty if we act otherwise, and also because we fear social embarrassment by doing otherwise (at least if caught). Norms also aid the observance of the sanctions of law by making us guilty about breaking laws even if the likelihood of enforcement is next to nil."[903]
Norms in cyberspace regulate behaviour in particular on social networking websites, where so called "Netiquettes" attempt to enforce what is considered to be acceptable behaviour.

Markets are an economic way of regulating behaviour. They do so by regulating the price of goods. Lessig highlights, that the market is only able to constrain in this manner because of other constraints of law and social norms: property, and contract law govern markets; markets operate within the domain permitted by social norms.[904] The influence of the law on the market is also illustrated above in figure 1.

---

and Punish (New York: Pantheon, 1977), who discussed in his work how architecture can regulate behaviour. See e.g N K Katyal, "Digital Architecture as Crime Control" (2003) 112 *The Yale Law Journal*, 2261; R Jones, "Architecture, Criminal Justice, and Control" in L McAra, S Armstrong (eds) *Perspectives on Punishment: The Contours of Control* (Oxford: Oxford University Press, 2005) 471 for an application of those ideas to the digital realm.

[899] Sufficient case law exists to highlight the influence of law on cyberspace, and sanctions imposed for violations. See e.g. *Dow Jones v Jameel* , [2005] EWCA Civ 75; *Al Amoudi v Brisard and JCB Consulting International SARL* [2006] EWHC 1062 (QB); G and G v Wikimedia Foundation [2009] EWHC 3148 (QB); BGH, Az. I ZR 57/09, 17. August 2011.

[900] See e.g the above discussed *Digital Economy Act* in UK, and the *Access Restriction Act* in Germany, p. 74.

[901] Lessig, note 878, at 507.

[902] Ibid.

[903] Greenleaf, note 897, at 603.

[904] Lessig, note 878, at 507.

In cyberspace, markets regulate behaviour by, for example, constraining access through price structures, as Lessig explains.[905] In addition, popular websites receive more funds through advertisements, and therefore will more likely remain online.

Architecture, or code, is the fourth modality in Lessig's approach. Architecture in the real world regulates behaviour by being designed in a certain way. Lessig explains that architecture in the physical world refers to "how it has been made".[906] Greenleaf states further that when considering regulation in real space, "it is easy to ignore the roles of the natural environment, the artefacts of the built environment, and human biology, because we so often take them as the 'givens' of the situation being regulated."[907] Bing emphasises this point stating "numerous instances in the physical world exist where physical barriers make the enforcement of man-made rules mandatory, or at least more efficient."[908]

In cyberspace, however, architecture, or rather code as Lessig refers to this modality in the online sphere, is the software and hardware that constitutes cyberspace. Lessig further describes this as the rules and instructions embedded in the software and hardware that together constitute cyberspace as is.[909] Code can change, either because it evolves in a different way, or because government or business pushes it to evolve in a particular way. The code constitutes a set of constraints on how one can behave. The substance of these constraints can vary, but they are all experienced as conditions on one's access to cyberspace.[910] These can, for example, be password protected websites, encryption options, or the tracking through cookies.

While these four modalities are separate means of regulation, as evidenced in figure 1 above, they necessarily influence each other in their regulatory quest. As depicted in figure 1, law influences all other modalities. It defines the principles and boundaries of the regulatory powers of the other modalities. The analysis of all interactions and influences of these modalities on each other is beyond the scope of this thesis. The details of this confluence of modalities concern this thesis only marginally. The focus is

---

[905] Lessig, note 878, at 508.
[906] Lessig, note 878, at 507.
[907] Greenleaf, note 897, at 604.
[908] J Bing, "Human Rights in the Digital Age" in M Klang, A Murray (eds) *Human Rights in the Digital Age* (London: Glasshouse Press, 2006) 203-217, 210.
[909] Lessig, note 878, at 506.
[910] Lessig, note 878, at 509.

on the confluence of law and code, to determine whether regulation through code could be a solution for the problems that arise from the regulation of MIA tools through law.

Lessig argues that code will be the regulator of choice in cyberspace because it is the most pervasive modality.[911]

The reason why code is of such high significance for the regulation of the Internet and ICTs is that cyberspace is a man-made space. By changing the technical aspects of the Internet, its core functionality can be changed, and behaviour can be regulated. Kohl makes an important observation, stating that "while often change of design means an increase in user-friendliness and convenience; it can also be used to implement regulatory objectives."[912]

Lessig provides an example in point, and thereby illustrates the difference between architecture or code as a regulatory modality in real space and cyberspace, discussing how regulators can invade privacy through design. He discusses the example of a customer in a store, being tracked by cameras, a shop assistant noting down every item placed in the shopping cart, and calculating the time spent in any given aisle. The cashier, demanding to see identification before the purchase can be made.[913] In real space, the customer notices this, and can choose to abandon the purchase at this specific store.

In cyberspace, however, he argues correctly, these actions are not similarly visible. The purchaser's movements and actions are recorded by a piece of software designed into the code that constitutes the online store. The customer is unaware that these monitoring actions are undertaken.[914]

Thus code in the online context influences how people *can* behave (hard criteria), whereas law influences how people *should* behave (soft criteria).[915]

Brownsword adds that "regulators, having identified a desired pattern of behaviour (whether morally compliant or not), secure that pattern of behaviour by designing out any option of non-conforming behaviour. Such measures might involve designing regulatees themselves, their environments, or the products that they use in their

[911] Lessig, note 878, at 510.
[912] Kohl, note 14, at 31.
[913] Lessig, note 878, at 504.
[914] Lessig, note 878, at 505.
[915] Koops, note 876, at 159.

environments, or a combination of these elements. Where this techno-regulation is perfectly instantiated, there is no need for either correction or enforcement.[916]

This discussion about the different regulatory approaches to Internet and ICT governance and regulation has highlighted that regulation through code (also referred to as Lex Informatica, or techno-regulation)[917] has assumed a central role in the governance of these technologies. The unique problems that these technologies pose for the regulation through law combined with their distinct nature that lends itself to changes in design, have made the regulatory modality architecture, which has often been disregarded in the real world,[918] a primary choice. The creation or existence of design constraints that enable or disable certain behaviour is a particularly effective way of the regulation of cyberspace.

Since the seminal works of Lessig and Reidenberg, the concept of regulation through code has been researched and discussed from different perspectives.[919]
However, the focus of all this research has been on the regulation of human behaviour through code. The concept *code as law* thus refers to the use of technologies to enforce law and legal concepts online. The interaction of code and law in this concept thus refers to the prevention of illegal or otherwise undesirable behaviour and activities on the Internet by design.

---

[916] R Brownsword, "Code, Control, and Choice: Why East is East and West is West" (2005) 25:1 *Legal Studies*, 1, 13.
[917] Reidenberg, note 878, Brownsword, ibid.
[918] It is, however, important to note that this is not per se a new regulatory modality. Bing reasons correctly that "the implementation of regulations in computer programs […] are not radical, new ways of forging links between the physical world and law. It is rather part of a continuum that streches far back in the history of man, to the very origins of law. But information technology offers us ever more subtle means and more sophisticated possibilities than before (Bing, note 908, at 210).
[919] For but a few examples, see C Ahlert, "Technology of Control: How Code Controls Communication" (2003) in Organization for Security and Co-operation in Europe (OSCE), *Spreading the Word on the Internet*, 119; T Wu, "When Code Isn't Law" (2003) 89 *Virginia Law Review* 679; M Rotenberg, "Fair Information Practices and the Architecture of Privacy" (2001) *Stanford Technology Law Review* 1; L J Camp, S Syme, "Code as Governance, Governance of Code" (2001) *John F. Kennedy School Government Faculty Research Working Paper Series*; N Nguy, "Using Architectural Contraints and Game Theory to Regulate International Cyberspace Behaviour" (2004) 5 *San Diego International Law Journal*, 431; L Edwards, "The Changing Shape of Cyberlaw" (2004) 1:3 *SCRIPTed*, 363; Z Chenwei, "In Code, We Trust? Regulation and Emancipation in Cyberspace" (2004) 1:4 *SCRIPTed*, 585; T B Nachbar, "Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character" (2000) 85 *Minnesota Law Review*, 215; R Brownsword, "Neither East Nor West, Is Mid-West Best?" (2006) 3:1 *SCRIPTed*, 15.

This, however, is not the focus of this thesis. The question here is if and how software tools can be designed to obey the law. Thus it is about the regulation of software, and not the user's behaviour. The question is therefore whether the concept of code as a regulatory modality is applicable to this problem.

While the concept code as law is not of direct relevance for this thesis, the above discussion was nevertheless important for the general understanding of the regulatory modality code, and the finding that technologies through their code can have a normative impact.

8.2 Embodying Values in Code

What can be derived from the above discussion of the notion of code as law is that the design of code is crucial for the normative impact it can potentially have. Thus as a next step it needs to be established whether code can be designed to obey norms and laws, and whether this can constitute a viable regulatory option for the governance of MIA tools.

Nissenbaum has contributed important findings to this debate, albeit her focus is not specifically on legal norms, but on societal norms in general.[920] She established that the potentially significant influence of ICTs on societies challenges previous commitments to values and principles.[921] These values could include liberty, justice, enlightenment, privacy, security, friendship, comfort, trust, autonomy and sustenance,[922] thus substantive social, moral and political values, which are coherent to the functioning of societies. To address these challenges, she suggests embodying values into technical systems and devices.[923]

She hypothesises that ICTs pose a challenge for societies by threatening values that were inherent to the functioning of the "pre-technology" society. Privacy is an obvious example among the values she has listed. The potential impact of ICTs on privacy rights

---

[920] H Nissenbaum, "How Computer Systems Embody Values" (2001) 3 *IEEE Computer*, 120; M Flanagan, D C Howe, H Nissenbaum, "Embodying Values in Technology – Theory and Practice" in J van den Hoven, J Weckert (eds) *Information Technology and Moral Philosophy* (Cambridge: Cambridge University Press, 2008) 322.

[921] Nissenbaum, note ibid, at 120.

[922] Flanagan/Howe/Nissenbaum, note 920, at 322.

[923] Nissenbaum, note 920, at 119.

has been discussed in the previous section.[924] She argues further, that these threats to values and principles cannot be addressed by existing regulatory mechanisms.[925] Therefore, asserting that a different approach is required.

The idea of modifying the underlying architecture/code of the technologies to address these problems, is a logical continuum (though her work is not necessarily built on that of Lessig and others focusing on the law alone) of the concept code as law, that is based on the fact that design is an important step that determines the shape of technologies. However, as opposed to the concept of code as law that looks at modifying code to influence human behaviour, this approach suggests to modify code of technologies to adhere to existing normative frameworks and principles. Thus, this line of research confirms the hypothesis of this thesis that code can be designed to obey legal concepts. The question is whether the incorporation of norms as suggested by Nissenbaum can be accomplished. This would be a strong indicator that this is also possible for laws. Generally, as Nissenbaum points out, the problem is that technologies are developed without the societal values in mind.[926] This is in large part due to the sparseness of methodologies that exist for designers willing to incorporate values into technologies.[927] However, this is also due to the fact that technology development and design focuses on economic demands, and recent scientific findings, instead of the impact these technologies can have on societies and users.

Flanagan et al. tested the theoretical idea of incorporating values into technology on an experimental game prototype, to assess the feasibility of the approach.[928] While the details of this experiment are not relevant for this thesis, the outcomes are.

In this experiment it could be established that the incorporation of values into technologies is possible. However, this is only the case if a structured methodology is applied.[929] This methodology[930] includes (1) a discovery phase, in which a list of relevant values is compiled, followed by (2) a translation phase, where the relevant values are translated into machine-readable code and implemented in material design features corresponding to these values. The final (3) verification phase determines

---

[924] See p. 261.
[925] Nissenbaum, note 920, at 120.
[926] Nissenbaum, note 920, at 119.
[927] Flanagan/Howe/Nissenbaum, note 920, at 329.
[928] Flanagan/Howe/Nissenbaum, note 920, at 331.
[929] Flanagan/Howe/Nissenbaum, note 920, at 347.
[930] Flanagan/Howe/Nissenbaum, note 920, at 347.

whether the implementation has been successful, using a variety of methods in order to ascertain whether the designers' intentions have been met.

One potential problem in applying these academic results to mainstream technology design is the potential lack of influence that designers have on the realisation of the end product.[931] The design is influenced by consumer demands as well as economic factors (i.e. the market). Thus incorporating values might contradict these demands and therefore render any potential progress in this area. Moreover, ICT technologies are so manifold and can even change significantly from generation to generation, that a constant evaluation of the relevant values might be necessary, which could be deemed too costly.

All these problematic issues would not apply to MIA tools. This class of technologies is designed for a specific purpose, and commercial factors do not affect the design. Therefore, having determined that generally code can be designed to incorporate certain rules to obey principles, it needs to be established whether this is also true for the specific case of law.

8.3 Ambient Law

Values can be defined as concepts that describe the beliefs of individuals and society. These concepts, such as the general understanding of justice, trust, and privacy, often influence the interpretation or drafting of statutory laws,[932] but are in general more vague and flexible than codified laws. They do not usually exist in written form, and as discussed above for norms,[933] these concepts are not centrally enforced. Indeed the precise understanding can vary between different groups in a society. While the violation of these concepts can result in ex post punishment, punishment is executed through a community and not normally the government (it can in as much as values influence the interpretation of laws).

Contrary to this, laws are often codified, and the exact wording is important for the understanding and interpretation of the laws. Violations can therefore occur, if there is a lack of knowledge about the exact wording of a specific law, or if these are wrongly

---

[931] Flanagan/Howe/Nissenbaum, note 920, at 349.

[932] W N Eskridge, "Public Values in Statutory Interpretation" (1989) 137:4 *University of Pennsylvania Law Review*, 1007, 1009.

[933] See p. 259.

interpreted. Thus in essence, values are vague concepts of interchangeable and alterable beliefs, whereas laws are explicit and often codified concepts of mandatory and binding rules.

This means that the requirements for the incorporation of values into code as discussed in the previous paragraph differ from those for the incorporation of laws. The translation of values into code can be vague, with a focus on those principles relevant for the specific application of the technology and easily translatable into code. It is generally sufficient to focus on the main principles of the specific value to ensure the technology is value-complicit. Contrary to this, the exact wording and meaning of laws, including every detail and possible variation and exclusion, need to be translated into code to ensure technology is law-complicit.

It is therefore essential to analyse whether research has been undertaken into the incorporation of laws into technologies to assess whether this is a viable option for the regulation of MIA tools.

The above-discussed concept of code as law has evidenced that code can constitute a modality for technology regulation.[934] This concept was developed for the regulation of a specific technology – the Internet – that was at the time in a transition phase from being a specialised tool, mainly deployed by academics and other technology-aware groups of people, to becoming a mainstream medium.

This transition has also included the development of a class of ICTs, most commonly referred to as ambient technologies (such as RFID chips, CCTV) that are fully integrated into every day life, and can be highly pervasive and covert.[935] These technologies have given rise to a number of legal concerns,[936] and their adequate regulation has been one of the aspects researched by scholars.

---

[934] See e.g. p. 255ff.

[935] See e.g. D J Cook, J C Augusto, V R Jakkula, "Ambient Intelligence: Technologies, applications, and opportunities" (2009) 5:4 *Pervasive and Mobile Computing*, 277, for a discussion of the technologies and their application. The detailed discussion of this class of technologies goes beyond the scope of this thesis. In fact, the exact nature of these technologies is only of minor interest for this work. What is relevant is the fundamental conceptual similarity between ambient technologies and MIA technologies.

[936] For a discussion of the legal problems of these technologies see e.g. A Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence" (2008) 2:1 *Studies in Ethics, Law, and Technology*, Article 3; P de Hert et al., "Legal Safeguards for Privacy and Data Protection in Ambient Intelligence" (2009) 13 *Personal Ubiquitous Computing*, 435.

The reason why the results of this research could be relevant for the research question at hand is that ambient technologies share certain fundamental characteristics with MIA technologies.

Ambient technologies are dependent on the networked environment of the Internet, while they are at the same time self-contained technologies that are primarily designed and deployed to monitor people and collect data.

One major difference is that these technologies, as opposed to MIA tools, consist of software and hardware. Similar to MIA tools, the use of ambient technologies has challenged existing legislation and regulatory approaches, which has stipulated research into alternative ways of regulation.

Ambient technologies are smart environments that continuously make instantaneous decisions on citizens and consumers based on profiles and large collections of personal data.[937] These technologies are the outputs of a research field called ambient intelligence (AmI). The vision of AmI is that "technology will become invisible, embedded in our natural surroundings, present whenever we need it, enabled by simple and effortless interactions, attuned to all our senses, adaptive to users and context-sensitive, and autonomous."[938]

Hildebrandt and Koops explain further that "the vision of AmI assumes that keyboards and computer screens will disappear as human-machine-interfaces, and instead, the environment will infer a persons' preferences from her machine-readable behaviours, recorded by a set of invisible technologies, stored in large databases and mined by means of mathematical techniques that allow the detection of relevant patterns."[939]

Thus by virtue of its very definition, the vision of AmI has the potential to create an invisible and comprehensive surveillance network, covering an unprecedented share of our public and private life.[940]

---

[937] Koops, note 876, at 172.

[938] W Weber, J Rabaey, E Aarts, "Introduction" in W Weber, J Rabaey, E Aarts (eds) *Ambient Intelligence* (Berlin, Heidelberg, New York: Springer, 2005), 1.

[939] M Hildebrandt, B-J Koops, "The Challenges of Ambient Law and Legal Protection in the Profiling Era" (2010) 73:3 *Modern Law Review*, 428, 430.

[940] J Bohn et al., "Ethical Implications of Ambient Intelligence and Ubiquitous Computing" in W Weber, J Rabaey, E Aarts (eds) *Ambient Intelligence* (Berlin, Heidelberg, New York: Springer, 2005), 14.

Therefore, this new paradigm (while undoubtedly providing opportunities, as among others Hildebrandt and Koops point out)[941] has potentially negative implications for privacy and data protection rights.

However, as established by scholars undertaking research in this area, existing privacy and data protection laws are inapt to regulate these implications posed by AmI technologies.[942] Thus similarly to the regulatory problems of MIA tools analysed in the previous chapters, a different approach to regulation through law needed to be explored.

Hildebrandt and Koops have introduced an alternative regulatory approach they coined *Ambient Law*.[943] This notion builds on the findings of Lessig that code is a regulatory modality, and can be designed to support specific legal norms, inducing compliant behaviour,[944] and those of Nissenbaum that values can be embedded into software code.[945] It pays tribute to the fact that the process of digitalisation has an impact on the law as shown above.

Hildebrandt argues that "if 'regulating technologies' is indeed understood as the double challenge of sustaining a legal framework that regulates emerging technologies, while acknowledging that technologies themselves have a regulative (normative) impact on human society, we need to urgently face the issue of digitilisation as a process that will regulate and constitute our life world and for that very reason needs to be regulated and constituted by law. In that sense 'regulating technologies' implies mutual transformations of law and technology."[946] The concept of Ambient Law represents such a transformation of law and technology, merging both disciplines.

Ambient Law refers to the incorporation of legal norms into the socio-technical infrastructures to enable ambient technologies to guarantee the safeguarding of privacy and data protection rights.[947] It thus requires the translation and incorporation of legislation into technologies to ensure that these are law-complicit.

---

[941] Hildebrandt/Koops, note 939, at 433.

[942] For details on why existing legislation is challenged by AmI technologies see e.g. Hildebrandt/Koops, note 939, at 429, 439; de Hert et al., note 936, at 440.

[943] Hildebrandt/Koops, note 939, at 429; Koops, note 876, at 172; M Hildebrandt, "A Vision of Ambient Law" in R Brownsword, K Yeung (eds) *Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes* (Oxford, Portland: Hart Publishing, 2008) 175.

[944] See p 255ff.

[945] See p 263ff.

[946] Hildebrandt, note 943, at 186.

[947] Hildebrandt/Koops, note 939, at 459; while not referring to it as Ambient Law, de Hert et al., note 936, suggest a similar regulatory model for these technologies.

However, this migration from 'law in the books' to 'law in technologies' poses several problems.[948] As indicated in the first part of this section, the translation of laws into code constitutes a technical challenge. "Sustaining the contestability of law in a constitutional democracy; to meet this challenge, rules must be embedded in such a way that they share the nuance and flexibility of the natural-language rules that determine the written law."[949]

The problem here is that laws are formulated in human language and inscribed in written and printed script, whereas code rules are formulated in machine language. Despite much research in computer science, the translation of human language concepts into machine-readable concepts remains a challenge.[950] This is particularly true for legal concepts.[951] Hildebrandt and Koops point out that "software code can of course be made more fexible, nuanced, and resilient than the architecture of a physical object. Code can also 'learn' from experience through the use of feedback loops and evolutionary programming. The 'ought' and 'permissible' operators of deontic logic are a welcome extension of the 'is' and 'not' of classic logic employed in computer science. Nevertheless, machine language will still encounter difficulties in dealing with open norms like 'reasonable care' or 'necessary in a democratic society', which need to be interpreted with considerable attention to the context of a concrete case. This will require detailed refinements, specifying relevant circumstances and the weight that must be attributed to them."[952]

The second challenge that Hildebrandt and Koops identify is whether the articulation of legal norms in digital technologies is legitimate in a democratic sense.[953] In their work, they refer to the problem that Ambient Law in particular is intended to influence human behaviour, and therefore needs to comply with criteria that society considers important for public regulation.[954] This however, is true for technology that is intended to be law-complicit in general, particularly, if it is designed to execute law enforcement actions.

---

[948] Hildebrandt/Koops, note 939, at 452.
[949] Hildebrandt/Koops, note 939, at 452.
[950] J Olive, C Christianson, J McCary (eds) *Handbook of Natural Language Processing and Machine Translation* (New York, Heidelberg, London: Springer, 2011), vii.
[951] E Francesconi, S Montemagni, W Peters, D Tiscornia (eds) *Semantic Processing of Legal Texts: Where the Language of Law Meets the Law of Language* (Berlin, Heidelberg: Springer, 2010).
[952] Hildebrandt/Koops, note 939, at 453.
[953] Hildebrandt/Koops, note 939, at 452.
[954] Hildebrandt/Koops, note 939, at 454.

Legitimacy has various dimensions in the context of Ambient Law. Koops has developed a full account of these in his work.[955] Substantive elements include, for example, human rights and moral values. Procedural elements relate to the rule of law, transparency of the rule-making process, and accountability; result criteria ensure that the rules should be flexible and transparent.
Hildebrandt and Koops derive from these legitimacy challenges that a digital literacy of those who enact laws and those who guard the internal and external coherence of the legal system is required.[956] They rightly point out that these matters cannot be left to be solved by technology developers.[957] The embodiment of laws into technology changes the nature of the rule. Therefore, new tests and balances for the process of inscribing rules into technology are required.

Thirdly, they find that challenges of political-legal theory need to be addressed in order to prevent an uncritical embrace of 'digital law'.[958] This refers to the fact that the above-discussed challenges of a technical and legal nature are cost-intensive and it needs to be ensured that (particularly for the case of ambient technologies that are developed by industry based on consumer demands) the development of Ambient Law does not depend on market forces, and is therefore influenced by industry.[959] This is consistent with traditional rules of law making, which require objective procedures to ensure that legislation is neutral and fair.

The successful incorporation of laws into technologies therefore requires that these challenges are adequately addressed before the concept of 'law in technologies' can be used as a regulatory modality. This is particularly the case if technology is utilised by the government to execute potentially highly infringing acts, such as the search and seizure of private data.

The analysis of Ambient Law has shown that provided a set of challenges is sufficiently addressed, laws can be incorporated into technologies to ensure that the technologies are law-complicit.

---

[955] Koops, note 876, at 168.
[956] Hildebrandt/Koops, note 939, at 456.
[957] Ibid.
[958] Hildebrandt/Koops, note 939, at 452.
[959] Hildebrandt/Koops, note 939, at 457.

The question is therefore whether these challenges can be sufficiently addressed for the specific case of MIA technologies.

8.4 MIA Law?

The previous sections have established that software code is a regulatory modality, and can be designed to incorporate laws if a structured methodology is applied to the process, and specific technical and legal challenges are sufficiently addressed.

Lessig's theorem *code as law* can be regarded as the foundation for all subsequent research in the area of ICT technology regulation. His work has identified code as a modality in technology regulation, and arguably thereby prompted the convergence of AI and law research in this field.

However, as discussed above, the concept of *code as law* is concerned with the question in how far law-compliant human behaviour can be stipulated through software code. [960] It falls short to discuss in how far code could also serve to regulate technologies by designing these to be law-complicit. This is partly due to Lessig's under-conceptualisation of 'code' and its many facets, as well as the four modalities of regulation. However, the main reason is that Lessig wanted to contribute with his work to the broader debate over freedom of expression, and not explore fundamental issues of ICT regulation.[961]

Subsequent research building on Lessig's work, in particular the work of Hildebrandt and Koops, has explored the many more facets of code as a regulatory modality, but remained entirely theoretical, and mainly focused on the theoretical legal aspects of incorporating laws into technologies. Like Lessig's work and that of others,[962] a discussion of how concepts such as *Ambient Law* could be technically realised are lacking. Nevertheless, the theoretical framework that has evolved from this research is of great significance for any work on this topic, thus also for this thesis.

---

[960] See p 262.

[961] D S Wall, "Digital Realism and the Governance of Spam as Cybercrime" (2005) 10 *European Journal on Criminal Policy and Research*, 309, 324.

[962] Hildebrandt/Koops, note 939; Brownsword, note 915; Reidenberg, note 878; J P Kesan, R C Shah, "Deconstructing Code" (2003-04) 6 *Yale Journal of Law & Technology*, 277; L F Asscher, "'Code' as Law – Using Fuller to Assess Code Rules" in E J Dommering, L F Asscher (eds) *Coding Regulation. Essays on the Normative Role of Information Technologies*, IT & Law Series vol 12 (The Hague: TMC Asser Press, 2006) 85.

However, any significant research into the feasibility of incorporating laws into technologies requires exploring the technical details of this approach. In this regard, the challenges developed by Hildebrandt and Koops provide a useful framework. Thus, the regulatory approach of incorporating laws into technologies depends in particular on whether laws can be adequately translated into a machine-processable format.
As suggested by Hildebrandt and Koops, who developed the notion of Ambient Law for the regulation of ambient technologies, such research requires a technology-specific approach.
As discussed in chapter 5, technology legislation needs to be sufficiently technology-neutral to remain valid for a long time, but technology-specific enough to develop meaningful regulatory powers.[963] The same is true for other regulatory approaches. ICT technologies differ fundamentally in design, leading to a variety of abilities and characteristics. These differences greatly impact the feasibility of incorporating laws into the code of a technology. This highlights again the importance of defining a new class of technologies – MIA tools – in chapter 5.
The analysis of the feasibility of incorporating laws into technologies is therefore undertaken for MIA tools alone.

As discussed previously, MIA technologies are similar in nature to Trojan software, and share crucial features with autonomous agent software.[964] Thus any previous research into the feasibility of incorporating laws into the code of these technologies can be applied to MIA technologies.
The need to imbue software, and more explicitly autonomous agent software, with explicit legal knowledge was first recognised in commercial applications.[965] With advancements in autonomous agent design and e-commerce applications, it became clear that agents operating in a society need to be constrained in order to avoid and address conflicts, make agreements, reduce complexity, and, generally, to achieve a desirable social order.[966]

---

[963] See p. 122.
[964] For the technical particulars of MIA technologies see chapters 4 and 5 above.
[965] See e.g. C Hahn et al., "Self-regulation through social institutions: A Framework for the Design of Self-Regulation of Open Agent-based Electronic Marketplaces" (2006) 12:1-2 *Computational & Mathematical Organization Theory.* Special Issue on Normative Multiagent Systems, 181-204.
[966] d'Inverno/Luck, note 274, at 182.

As established above, the feasibility of incorporating laws into the code of a technology depends in particular on whether laws can be adequately translated into machine-processable format. However, a prerequisite for the capability of processing laws adequately, and adopting and complying with rules, is that technologies are capable of acting on and reasoning about them.

The following simple example demonstrates why these capabilities are important.

If a MIA tool is employed during an investigation and the suspect travels abroad taking his laptop that was previously infiltrated by the MIA tool, the tool needs to 'understand' that all data downloaded and any communication data that has been generated since crossing the border is protected by sovereignty, which triggers a corresponding *disability* by the tool to collect information unless there is also a superseding *power* to grant authority over the data, such as a *privilege* by the country where the data originates.

Thus the MIA tool would as a default rule stop analysing data once it "knows" it is outside the country of origin.[967] Crossing the border therefore triggers by default an immunity of the suspect.

This reasoning is based on legal principles and laws integrated into the design of the software. However, the software needs to be capable of processing this information, applying it to the context, and communicating it to other pieces of software and the operator. If the software is incapable of such actions, the question of whether laws can be adequately translated into machine-processable format is irrelevant.

The question is therefore whether MIA technologies are capable of such adaptive reasoning and acting.

8.4.1 Computational Legal Reasoning

Several authors have addressed the issue and developed different approaches to imbue autonomous agents with legal reasoning capabilities. At the core of these approaches is the development of a suitable agent communication language (ACL). This language enables the software tools to reason about facts and circumstances, draw conclusions

[967] Discussing the technical details of how a MIA tool can 'know' that the suspect has crossed a border would go beyond the scope of this thesis. For example, the accessing the Internet from a foreign telephone line, the assigned IP address are indicators for the suspect residing in a different jurisdiction.

and make decisions independently, and communicate with other software tools and operators.[968]

8.4.1.1 Agent Communication Languages

A suitable ACL is a crucial factor in the process of enabling software tools to reason and act about their environment, facts and situations autonomously. It is also the key component for any dialogue and communication with its operator and other software tools.[969] Natural language in humans was developed through evolution, and arguably has been a decisive element in the establishment of complex, long-lived communities.[970] ACLs, on the contrary, have evolved through standardisation efforts.[971] At the technical level, as Labrou and Finin explain, "ACLs handle propositions, rules, and actions instead of simple objects with no semantics associated with them. They describe a desired state in a declarative language, rather than a procedure or method."[972]

Chaib-Draa and Dignum provide a short description of ACLs: "ACLs exist in a logical layer above transport protocols such as TCP/IP, HTTP, or IIOP. Such protocols deal with communication issues at the level of data and message transport, while ACLs address communication on the intentional and social level. ACLs themselves are complex structures composed of different sublanguages that specify the message content, interpretation parameters such as the sender and the ontology, the propositional attitude under which the receiver should interpret the message content, and several other components. Typical ACLs also have a characteristic mentalistic semantics that is far more complex than standard distributed object protocols. This means that ACL design is a delicate balance between the communicative needs of the agent with the ability of receivers to compute the intended meaning of the message. Further, it is important that the syntax, semantics, and pragmatics of the various components of an ACL are as precise and explicit as possible, so that the agent system

---

[968] See e.g. Y Labrou, T Finin, "Semantics for an Agent Communication Language" (1998) 1365 *Intelligent Agents IV Agent Theories, Architectures, and Languages*, 209-214, 209; B Chaib-Draa, F Dignum, "Trends in Agent Communication Language" (2002) 18:2 *Computational Intelligence*, 89-101, 89.

[969] Ibid.

[970] Y Labrou, T Finin, Y Peng, "Agent Communicaction Languages: The Current Landscape" (1999) *IEEE Intelligent Systems*, 45-52, 45.

[971] Ibid.

[972] Y Labrou, T Finin, "History, State of the Art and Challenges for Agent Communication Languages" (2000) *Swiss Federation of Information Processing Societies*, 1-16, 3.

using that ACL can be as open and accessible to developers beyond the original group."[973]

This short description of ACLs highlights why these are of such importance for artificial legal reasoning. They enable intelligent reasoning and communication, as opposed to the mere data exchange of standard software applications.

Synchronously with the software agent development, ACLs evolved initially in the 1990s in the military domain.[974] Research was then expanded to commercial applications, in line with the increased integration of software agents into e-commerce applications.[975]

The common problem of ACLs is that of interoperability. Generally, (and particularly for MIAs) it is important that agents built by different organisations using different hardware and software platforms are able to communicate with one-another via a common language with a universally agreed semantics.[976]

This need for interoperability has led to the evolvement of many standardised ACLs.[977] Verifying whether a specific ACL indeed satisfies a certain standard and conforms with interoperability criteria is a difficult task.[978] One of the most important aspects is that an ACL must be based on a valid formal system.[979]

8.4.1.1.1 Agent Communication Languages For the Legal Domain

As indicated above,[980] discussing all existing ACLs would go beyond the scope of this work. While the fundamentals of all relevant ACLs are identical, the respective application domain significantly influences the details of ACLs, and thus shapes the

---

[973] Chaib-Draa/Dignum, note 968, at 90.

[974] Labrou/Finin, note 970, at 3; Chaib-Draa/Dignum, note 968, at 90.

[975] See e.g. M Wooldridge, "Semantic Issues in the Verification of Agent Communication Languages" (2000) 3 *Autonomous Agents and Multi-Agent Systems*, 9-31.

[976] Wooldridge, ibid, at 3; Chaib-Draa/Dignum, note 968, at 95.

[977] The discussion of all these ACLs would go beyond the scope of this work. See e.g., J Mayfield, Y Labrou, T Finin, "Evaluating KQML as an Agent Communication Language" in M Wooldridge, J P Müller, M Tambe (eds.) *Intelligent Agents II (LNAI Volume 1037)* (Berlin: Springer, 1996) 347-360, for a representative summary of relevant ACLs.

[978] See Wooldridge, note 975, who develops a framework in his work for verifying the conformity of ACLs with interoperability standards.

[979] Wooldridge, note 975, at 12.

[980] See footnote 977.

requirements for the underlying formal system.[981] Relevant for this thesis are ACLs developed for the legal domain and the focus is solely on discussing details of these. Work on ACLs for the legal domain initially evolved in the area of legal argumentation automation, where the formal study of human argument and dialogue was proposed as a model for agent interactions.[982] However, deeper conceptual work on ACLs for the legal domain evolved in the AI & Law research community following the increase in autonomous agent research.[983]

As stated above, the underlying formal system is of great relevance for the development of a valid ACL. This is particularly the case for ACLs developed for the legal domain because (artificial) legal reasoning requires detailed understanding of all facts and arguments relevant for the matter at hand and the decision making process. Thus analysing the formal fundaments of ACLs is crucial for assessing their validity and suitability, and determining which, if any, existing ACL is suitable for implementation in MIA tools, and enables these tools to undertake legal reasoning at the required level.

8.4.1.1.2 Formal System

Several formal approaches have been discussed in connection with ACLs for the legal domain.[984]

---

[981] C Krogh, H Herrestad, "Hohfeld in Cyberspace and Other Applications of Normative Reasoning in Agent Technology" (1999) 7 *Artificial Intelligence and Law*, 81-96, 83.

[982] See e.g. P McBurney, S Parsons, "Games That Agents Play: A Formal Framework for Dialogues between Autonomous Agents" (2002) 11 *Journal of Logic, Language and Information*, 315-334; P McBurney, S Parsons, M Wooldridge, "Desiderata for Agent Argumentation Protocols" (2002) *Proceedings of the First International Conference on Autonomous Agents and Multiagent Systems (AAMAS-02)*, Bologna, Italy; N Maudet, B Chaib-Draa, "Commitment-baswd and dialogue-game-based Protocols: New Trends in Agent Communication Languages" (2002) 17:2 *The Knowledge Engineering Review*, 157-179.

[983] See in particular C Heesen, V Homburg, M Offereins, "LACA: An Architecture For Legal Agents" in J C Hage, T J M Bench-Capon, M J Cohen, H J van den Herik (eds) *Legal Knowledge Based Systems JURIX '95: Telecommunication and AI & Law* (Lelystad: Koninklijke Vermande, 1995) 23-32; N Graca, P Quaresma, "How to Model Legal Reasoning Using Dynamic Logic Programming: A Preliminary Report" in D Bourcier (ed) *Legal Knowledge and Information Systems Jurix 2003: The Sixteenth Annual Conference* (Amsterdam: IOS Press, 2003) 163-172; J Gelati, A Totolo, G Sartor, G Governatori, "Normative Autonomy and Normative Co-ordination: Declarative Power, Representation, and Mandate" (2004) 12:1-2 *Artificial Intelligence and Law*, 53-81; G Sartor, "Doing Justice to Rights and Values: Teleological Reasoning and Proportionality, (2010) 18:2 *Artificial Intelligence and Law*, 175-215.

[984] Discussing all would go beyond the scope of this chapter. See e.g. J Hage, "A Theory of Legal Reasoning and A Logic to Match" (1996) 4 *Artificial Intelligence and Law*, 199-273; A Jøsang, V A Bondi, "Legal Reasoning with Subjective Logic" (2000) 8:4 *Artificial Intelligence and Law*, 289-315, for an analysis of different approaches.

However, in particular Hohfeld's formal system of rights and duties has been proposed as a framework for ACLs in the legal domain, enabling the reasoning about rules.[985] Hohfeld developed a theory of rights describing what he called the fundamental legal conception:[986] *right*, *duty*, *no-right*, *privilege*, *power*, *liability*, *disability*, and *immunity*.[987] Hohfeld's rights were intended to serve as the smallest common denominators in jurisprudential reasoning. However, in his work he does not provide definitions of these concepts, rather, he tries to systematise them. *Right* and *duty*, for example, are correlatives, *right* and *no-right* are opposites, and so forth.

These denominators have subsequently been used as the basis to develop formal legal theories.[988]

Other attempts at computational implementation of Hohfeld's theory have been developed in the wider AI and law community, but not for use with autonomous agents in mind. Allen and Saxon's language "A-Hohfeld"[989] and Sergot's analysis of normative positions[990] have been the most developed approaches so far. However, their intended use as interpretative tools for text analysis and analysis of bureaucratic organisations, respectively, make a transfer of these ideas to ACLs less straightforward.

The original work of Hohfeld was primarily concerned with private law concepts, and it is at least not obvious how his framework could be applied to the criminal law, and criminal procedure law setting. However, there has been an intensive debate in analytical jurisprudence following Hohfeld's paper and further positions and correlations have been identified.[991]

Due to their intended use in jurisprudence, they do not take computational characteristics at their heart, but offer the advantage of considerably extending the expressive power of the resulting formalism, thus providing expressive power that may

---

[985] See e.g. Krogh/Herrestad, note 981.

[986] W N Hohfeld, "Some Fundamental Legal Conceptions As Applied in Judicial Reasoning" (1913-1914) 23 *Yale Law Journal*, 16; W N Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning and Other Legal Essays* (New Haven: Yale University Press, 1923).

[987] Hohfeld (1913-1914), ibid, at 30; Hohfeld (1923), ibid, at 63.

[988] See e.g. S Kanger, "New Foundations For Ethical Theory", (1957) *Technical Report, Stockholm Unversity*; S Kanger, "Law and Logic" (1972) 38 *Theorica*, 105-132; D Makison, "On the Formal Representation of Rights Relations" 15 *Journal of Philosophical Logic*, 403-425.

[989] A E Allen, C S Saxon, "A-Hohfeld: A language for Robust Sturctural Representation of Knowledge in the Legal Domain to Build Interpretation-Assistance Expert Systems" in J Meyer, R J Wieringa (eds) *Deontic Logic in Computer Science: Normative System Specification* (Chichester, New York: J Wiley, 1993).

[990] M Sergot, "A Computational Theory of Normative Positions" (2001) 2:4 *ACM Transactions on Computational Logic*, 581-622.

[991] See in particular L Lindahl, *Position and Change: A study in Law and Logic* (Dordrecht: D. Reidel Publishing, 1977); A Ross, *Directives and Norms* (London: Routledge, 1968).

well be necessary to represent the legal concepts necessary for law-compliant behaviour.

Hohfeld's theory and subsequent other formal legal theories based on his work are premised on the logic that if x then y,[992] which is deontic logic.

Deontic logic is concerned with the logic to reason about ideal and actual behaviour.[993] As such, as highlighted by Hohfeld's system above, it is concerned with concepts such as obligation and permission. It studies logical relations among obligations and permissions, and more particularly violations and contrary-to-duty obligations, permissions and their relation to obligations, and the dynamics of obligations over time.[994] Deontic logic has traditionally been used to analyse the structure of normative law and normative reasoning in law.[995] It is therefore the obvious choice for the representation of norms and laws.[996] Insights from deontic logic can be used to represent and reason with norms.[997]

Generally, in its most basic form, deontic logic can be presented as:

◯p, which is read as 'p ought to be (done)';
Fp as 'p is forbidden to be (done)'; and
Pp as 'p is permitted to be (done)'.[998]

As indicated above, deontic logic has been proposed for the formal representation of norms in autonomous agents.[999] However, there are several problems with deontic logic as the sole means for the representation of norms and laws.

---

[992] A R Anderson, "The Logic of Hohfeldian Propositions" (1971-72) 33 *University of Pittsburgh Law Review*, 29, 31.

[993] R J Wieringa, J-J Ch Meyer, "Applications of Deontic Logic in Computer Science: A Concise Overview" in J-J Ch Meyer, R J Wieringa (eds) *Deontic Logic in Computer Science* (Chichester: Wiley, 1993) 17.

[994] G Boella, L van der Torre, H Verhagen, "Introduction to Normative Multiagent Systems" (2006) 12 *Computational and Mathematical Organization Theory*, 71, 74.

[995] Wieringa/Meyer, note 993, at 17.

[996] L van der Torre, "Contextual Deontic Logic: normative agents, violations and independence" (2003) 37 *Annals Mathematics and Artificial Intelligence* 33.

[997] Boella/van der Torre/Verhagen, note 994, at 74.

[998] Van der Torre, note 996, at 17.

[999] See in addition to the previous footnotes, C Castelfranchi et al., "Deliberative Normative Agents: Principles and Architecture" (2000) 1757 *Intelligent Agents VI. Agent Theories Architectures, And Languages. Lecture Notes in Computer Science*, 364-378; M Barbuceanu, T Gray, S Mankovski, "The Role of Obligations in Multiagent Coordination" (1999) 13:1-2 *Applied Artificial Intelligence*, 11-38.

Most importantly as pointed out by Boella et al. there are several aspects of laws, which are not covered by constraints nor by deontic logic, such as the relation between the cognitive abilities of agents and the global properties of norms.[1000] Other problems of representing laws with deontic logic are, for example, how conflicts of norms can be taken into account, and how explicit permissions relate to, and change, an agent's obligations.[1001]

However, taking the short example above, it becomes clear that MIA tools need to be capable of dealing with conflicting laws, or explicit permissions.

If generally the investigation of ICT devices on foreign territory is impermissible, this can be permitted (exceptionally) under certain circumstances, for example if a permission of the country in question is granted. Thus MIA tools need to be flexible enough and capable of such "defeasible" reasoning: applying a general rule first, but capable of revising the result of the rule application if exceptions are triggered.

Sartor has shown how these legal relations can be expressed formally in a system that combines action logic with a minimal deontic logic using a formalisation of basic legal concepts inspired by Hohfeld's work, but intended for agent communication.[1002]

Laws are complex artefacts that attempt to prescribe how something should be; meaning, it describes the properties of the desired situation, out of all the possible alternative situations.[1003] This means that the most basic function of law is the stipulation of an action.

This requires as a first step that the notion of an action is formalised. Sartor distinguishes between two characterisations of actions:[1004] (1) the behavioural characterisation, which consists of describing the type of behaviour that an agent is holding, abstracting from the consequences of such behaviour; and (2) a productive characterisation, which consists in describing the results that the agent's behaviour produces, abstracting from the behaviour that produced those results.

Behavioural characterisation can be expressed formally as "Does $_{(x,t)}$". Productive characterisation can be expressed formally as "Brings $_{(x,t)}$".

[1000] Boella/van der Torre/Verhagen, note 994, at 75.

[1001] J Hansen, G Pigozzi, L van der Torre, "Ten Philosophical Problems in Deontic Logic" (2007) *Normative Multi-agent Systems*, *Dagstuhl Seminar Proceedings 07122*, 2, also discussing further problems of deontic logic.

[1002] G Sartor, "Fundamental Legal Concepts: A Formal and Teleological Characterisation", (2006) 14 *Artificial Intelligence and Law*, 101-142.

[1003] A Siena, et al., "Towards a Framework for Law-Compliant Software Requirements" (2009) *IEEE ICSE-Companion, 31st International Conference on Software Engineering*, 251, 252.

[1004] Sartor, note 1002, at 103.

Applying this to the case scenario introduced above, these two operators can be used to express, for example, the following:[1005]

1. Does $_{(MIA, t)}$ [search]
This can be read as "the MIA tool undertakes a search at time t".

2. Brings $_{(MIA,t)}$ [evidence]
This can be read as "the MIA tool brings about evidence at time t".

However, in addition to actions that can be stipulated by laws, these also pose constraints for these actions in form of obligations and permissions. Sartor states that by applying the usual basic deontic modalities to actions, such obligations and permissions can be formalised.[1006]
Generally, obligations can be expressed formally through "Obl A", meaning that A is obligatory. These can then be supplemented by the above-introduced formulas.
Thus applied to the case scenario, the following example can be formalised:

Obl Does$_{MIA}$ [respect territoriality principle]
This can be read, as "it is obligatory that the MIA tool respects the territoriality principle.

By contrast, a "bring about" sentence within the scope of the Obligation modality can express the idea that a MIA tool may have to "forget" or exclude data that it obtained during an investigation, for instance if it copied sensitive private data (such as a diary or medical records) in Germany,[1007] before the seized data can be transmitted back to the operator of the tool. This could be expressed formally in the following way:

Obl Brings$_{MIA}$ [suspect's personal data are cancelled]
This can be read, as "it is obligatory that MIA brings it about that the suspect's personal data are cancelled.

[1005] Appropriate axiomatisations for both the temporal and the action logic dimension can be found in the work of J Horty, *Agency and Deontic Logic* (Oxford: Oxford University Press, 2001).
[1006] Sartor, note 1002, at 104.
[1007] See p 47ff above, for an analysis of the BVerfG on the illegitimacy of such actions.

This allows at least partly for the adequate handling of the changing status of evidence over time by the MIA tool.

In addition, when opposed to the obligation to perform a certain action, this is (exceptionally) forbidden; this can constitute absolute investigative prohibitions. For example, carrying out extraterritorial investigative actions abroad without the explicit permission of the target state violates international law.[1008]
This can be expressed formally in the following way:

Forb $Does_{MIA}$ [undertake search and monitoring activities while ICT device is abroad]

This can be read, as "it is forbidden that the MIA tool undertakes search and monitoring activities while the suspect's ICT device is abroad".

As discussed above, this is a defeasible norm that can be overridden once the permission has been granted.[1009] Such permission, meaning the qualification of an action as being not forbidden, can be formally expressed as follows (assuming that the MIA tool is operated by German law enforcement and the ICT device located in UK):

Perm $Brings_{UK}$ [$Perm_{MIA}$ carry-out investigative action X]

This can be read, as "it is permitted that the UK allows that the MIA tool can undertake investigative action X.

In this case, the UK grants German law enforcement a permission to undertake the specified investigative actions on their territory. This changes the normative position of the MIA tool. It is particularly important for the use of MIA technologies that the normative position of the tools can be changed according to needs, as this is a typical situation that these cyber-cops will face.

Hohfeld, and in his subsequent work, Sartor consider these types of interaction important and disctinct enough to merit their own category. Hohfeld has coined this

---

[1008] See chapter 6, particularly p. 198.
[1009] G Sartor et al., "Norm Modifications in Defeasible Logic", in M-F Moens (ed.) *Proceedings of Jurix 2006* (Amsterdam: IOS, 2006) 13-22.

category "privilege"[1010], whereas Sartor refers to it as "potestative right".[1011] To provide a full analysis of these categories, and all higher-level notions based on these, would go beyond the scope of this chapter.[1012] However, one example, of a higher-level notion based on the potestative right discussed by Sartor in his work,[1013] will provide sufficient insight into the significance of this concept for this work.

This example introduces the notion *legal power*, which refers to having the ability to determine certain legal results, through one's action.[1014]

The example is based on a scenario from Roman private law:

A previously ownerless animal, through capture, becomes owned by its captor. That is, the captor has a privilege to perform a certain act (he may or may not capture the animal); but once he performs this act, the legal relation between the animal and anybody else changes. Whereas everyone initially has the same privilege, once one person substantiates it, this privilege changes into a no-right.

Formally expressed:

FORANY (x, y)

IF [animal y does not belong to anybody]

THEN^n IF Does$_x$ [capture y]

THEN^n it starts that [x is the owner of y]

This can be read as "for any person x and animal y, if y does not belong to anybody, then x has the potestative right of becoming the owner of the animal, by capturing y".

Applied to the use of MIA tools, this simple formalism can already capture some of the issues expressed above. Firstly, it can be used to "tell" the agent that unless certain conditions are met, it has no right collecting certain data. In connection with a suitable meta-rule that enshrines aspects of the legality principle, in particular the idea that an agent can only act if it has an explicit legal basis to do so, follows that the agent is prohibited from collecting data, unless a suitable antecedent is met.

For example, person P displayed suspicious behaviour y, this allows the agent to switch the legal status of P to a suspect S, and to start investigative actions.

[1010] Hohfeld (1913-1914), note 988, at 30.

[1011] Sartor, note 1002, at 105.

[1012] See Sartor, note 1002, for more details about this, and higher-level notions.

[1013] Sartor, note 1002, at 118.

[1014] Sartor, note 1002, at 118.

Formally expressed:

FORANY (MIA,P)
IF [person P displays behaviour y]
THEN^{n} IF Can$_{MIA}$ [Person P to Suspect S]
THEN^{n} it starts that [MIA investigative actions]

The above analysis of the formal foundations of ACLs has shown that generally Hohfeld's formal system is the ideal underlying fundament for ACLs deployed for legal reasoning tasks. In particular, Sartor's model is well suited to enable MIA tools to reason at the required level. Hence, his model and ACL will be used as a basis for this thesis.

The above analysis of logical and computational theories applied to agent communication languages has evidenced that it is possible to design and incorporate code into the software of tools, which ultimately enables them to reason about legal correlations, and act accordingly.
The analysis of the technical details has remained rather basic; however, of real importance for this thesis is the basic concept, and the knowledge that these technical possibilities exist.[1015]
Another issue that has not been addressed here is the problem of multi-jurisdictional usage of these tools, and the problems arising from this.[1016]

[1015] See for more detailed technical analyses e.g. G Boella, L van der Torre, "Regulative and Constitutive Norms in Normative Multiagent Systems" (2004) *Proceedings of 9th International Conference on the Principles of Knowledge Representation and Reasoning*, 255-265; A Garcia-Camino, P Noriega, J A Rodriguez-Aguilar, "Implementing Norms in Electronic Institutions" (2005) *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*, 667-673; G Governatori, A Rotolo, "BIO Logical Agents: Norms, Beliefs, Intentions in Defeasible Logic" (2007) *Dagstuhl Seminar Proceedings 07122*, 1-34; J Vazquez-Salceda et al., "From Human Regulations to Regulated software Agents' behavior: Connecting the abstract declarative norms with the concrete operational implementation" (2008) 16 *Artificial Intelligence and Law*, 73-87; R Paes et al., "Specifying Laws in Open Multi-Agent Systems" (2009) 82:4 *Journal of Systems and Software*, 629-649; F Dignum et al., "A Modal Approach to Intentions, Commitments and Obligations: Intention plus Commitment yields Obligations" in M Brown, J Carmo (eds.) *Deontic Logic, Agency and Normative Systems* (Berlin: Springer Verlag, 1996) 80-97. For an example of a multi-agent system designed to incorporate laws see e.g the outcomes of the POIROT project: B Schafer et al., "Towards a Financial Fraud Ontology: A Legal Modelling Approach" (2006) 12 *Artificial Intelligence and Law*, 419-446; A Siena et al., "Designing Law-Compliant Software Requirements" in A H F Laender et al. (eds) *Conceptual Modeling – ER 2009, Lecture Notes in Computer Science* (Berlin, Heidelberg: Springer Verlag, 2009) 472-486.

Summarising the technical findings above, it can be concluded that MIA tools can be designed to abide rules, and reason about circumstances and legal correlations. This means for the legal problems identified in the previous chapters, that these can be addressed through design. The examples have highlighted how this can be done for the issues arising from extraterritorial searches. In addition it could also enhance the currently slow mutual assistance procedures[1017] if every country would design agents that sit on network gateways and communicate to potential MIA tools the acceptable conditions for their operation.[1018] Should the conditions suffice for the specific operation, no human would have to be involved in the "permission procedure" and operations could therefore be executed swiftly.

The examples above have also highlighted how privacy and data protection issues discussed in chapter 2 can be addressed through code.[1019]

Addressing these problems contributes to the legal reliability of MIA tools, and therefore, in turn to the reliability of the evidence collected. In addition, the code of MIA tools can be designed to enable as a general rule the production of safe copies, and to incorporate techniques such as the digital evidence bag as discussed in the previous chapter.[1020]

Having determined that it is technically feasibille to endow MIA tools with legal reasoning capabilities and therefore enable them to behave law-complicit, the question is whether legislation can be translated adequately into machine-processable format.

8.4.2 Translating Laws Into Machine-Processable Format

The problem with laws in general is, as has been pointed out, that these are formulated in human natural language. More specifically, "the characteristic feature of the language

---

[1016] Since this issue is not essential for the cemtral question of this chapter, whether MIA tools can be designed to be law-complicit, this has been neglected here. However, for a discussion of this issue see W Abel, B Schafer, "Big Browser Manning the Thin Blue Line - Computational Legal Theory Meets Law Enforcement" (2008) 2 *Problema*, 51, 75.

[1017] See p.170ff for details.

[1018] See e.g. p. 114ff for a discussion of how agent software can communicate with other agents to reach a conclusion.

[1019] See example on p. 280.

[1020] See p. 247ff for details.

of legislation is that it uses natural language to express general rules, in order to regulate human affairs. To be effective for this purpose, it needs to be more precise than ordinary language and, as much as possible, it needs to be understood by different people in the same way."[1021]

Thus the problem with legal texts (i.e. laws) is that these are composed in a specific natural language that differs from the ordinary spoken natural language. The need for precision leads to the use of law-specific termini and concepts. In particular in criminal and criminal procedure law, legislation needs to clearly define what constitutes criminal behaviour, and how this is punished.

A brief example illustrates this:

Under the *UK Theft Act 1968* S.1(1) "Theft" is defined as "A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it".

This example highlights that legal natural language is highly conceptual and hieratic. The question is thus whether this language can be adequately translated into a formal, machine-processable format.

The formal translation of laws, including the particular termini and concepts has been a central issue in the field of AI and law.

Kowalski established that the legal language shares crucial features with the language of logic programming.[1022] He establishes in his work, that the linguistic style in which legislation is drafted combines in one language the expressive power of computer languages for such diverse areas as programming, program specification, database description and query, integrity constraints, and knowledge representation in AI.[1023] What he suggests with this is that legislation can be regarded as a programming language, to be executed by humans. As such, he suggests that this analogy could lead to a solution for the translation of legislation into formal, computer-processable format. He concludes in his work that logic programming techniques offer suitable tools for the translation of legislation into formal format. He derives this conclusion from the fact

---

[1021] R A Kowalski, "Legislation as Logic Program" in G Comyn, N E Fuchs, M J Ratcliffe (eds) *Logic Programming in Action* (Berlin, Heidelberg: Springer Verlag, 1992) 203.

[1022] Kowalski, ibid, at 203.

[1023] Kowalski, ibid, at 227.

that in his opinion, legislation is generally an expression of a factual situation followed by consequences.

While this is true to some extent, the problem of his approach is that, for example, definitions of the termini cannot be represented with Kowalski's approach. Another problem is the referencing of laws by laws.

However, the importance of the general idea of applying logic programming techniques to the task of translating laws into formal language is an important one.

Similarly, Biagioli et al. specify that normative texts can be viewed as composed by formal partitions (articles, paragraphs, etc) or by semantic units containing fragments of a regulation (provision).[1024] They state that this abstraction of the legislative system is necessary, because "the legal system usually suffers from scarce transparency, which is caused by a non-systematic organisation of the legal order".[1025] Considering examples in the previous section, depicting logical programming language examples, it can be observed that unambiguous information and a hierarchical relationship between the conditions is necessary for formalisations to be feasible.

Accordingly, Raz suggests in his work that the entire body of law, with its articles and paragraphs, may be seen as a set of provisions, intended as rules and carried by linguistic acts, and therefore propositions, whether simple or complex, endowed with meaning.[1026]

Thus far, it can be ascertained that one prerequisite of the translation of laws into machine-processable format is the structuring of the laws to make these easier accessible to logical programming languages.

De Maat and Winkels in their work confirm this, specifying further that laws can be distinguished into two types: primary and secondary rules.[1027] Here, the primary rules are the rules that refer to human behaviour, whereas secondary rules are actually rules about primary rules, and form a meta-level. This meta-level consists of three sub-groups: (1) rules of recognition, (2) rules of change, and (3) rules of adjucation.[1028]

The structuring of laws and recognition of normative rules therefore enables the translation of laws into machine-processable, formal language. Such a recognition of

---

[1024] C Biagioli et al., "Automatic Semantics Extraction in Law Documents" (2005) *Proceedings of the International Conference on Artificial Intelligence and Law '05*, 6.

[1025] Ibid, at 6.

[1026] J Raz, *The Concept of a Legal System* (Oxford: Oxford University Press, 1980, 2nd ed) 45.

[1027] E de Maat, R Winkels, "Automated Classification of Norms in Sources of Law" in E Francesconi et al. (eds) *Semantic Processing of Legal Texts* (Berlin, Heidelberg: Springer Verlag, 2010) 171.

[1028] de Maat/Winkels, ibid, at 171.

rules and provisions in a normative text requires an analytic effort, in which all the possible distinctions among the elements, understood as rules that constitute the legislative text, are made, and the nature and function of each one is identified where possible.[1029] This includes, according to Biagioli et al. among other things:[1030]

- Viewing the legal order as a rule-based system and the text as a set of rules;
- Clearly defining the rule functions in terms of provision types;
- Individuate the logically necessary components of each individual provision;
- Analyse the recurring and privileged relationships among the different rules.

A brief (simplified) example can better illustrate this translation process from natural language legislation to formal representation.

Taking the above example of the definition of "Theft" according to S.1(1) *UK Theft Act 1968*:

> "A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it".

The following relevant elements and rules can be identified:

Addressee: "a person"
Action: "dishonestly appropriating property belonging to another"
Intention: "permanently depriving the other"

Target semantic translation to First-order logic:

$$\text{Thief x} \left[\left(\left(\neg \text{person(x)} \rightarrow \text{dishonestly\_appropriating (property,X}_{\text{belonging to y}}\text{)} \wedge \text{intention(permanently\_depriving\_y} \right]\right)\right)$$

This can be read as "a thief is person x if he dishonestly appropriated property x, which belongs to y, and has the intention to permanently depriving y.

Thus the conclusion is, that it is generally feasible to translate natural language laws into formal, computer-processable format. Bain and Subirana show that this is also true

[1029] Biagioli et al., note 1024, at 7.
[1030] Biagioli et al., note 1024, at 7.

for autonomous agent software (and thus for MIA tools), explaining that logic programming languages enable agents to incorporate legal rules.[1031]

However, the process of translating laws into a formal language is extremely labour-intensive and time-consuming.[1032] Considering the amount of legislation that MIA tools need to incorporate it becomes clear that the manual translation of all this legislation would be an enormous task.

To circumvent this problem, several researchers have developed methods to automate the translation process, or some part of it.[1033]

State-of-the-art applications are capable of autonomously translating not only codified laws but even complex syntactic constructions, such as judgments of appellate courts and other legal documents.[1034] These methodologies are based on the development of so called parsers[1035] that produce output, which can be processed automatically. The technical details of these approaches are not relevant for this thesis.[1036] However, relevant is the finding that the automatic translation of natural language legal texts into formal, machine-processable format is possible and feasible.

[1031] M Bain, B Subirana, "Towards legal programming: the incorporation of legal criteria in software agent design – Current proposals and future prospects" (2004) 20:1 *Computer Law & Security Report*, 44-52.

[1032] L T McCarty, "Deep Semantic Interpretations of Legal Texts" (2007) *Proceedings of the International Conference on Artificial Intelligence and Law '07*, 217.

[1033] See e.g. K Al-Kofahi, B Grom, P Jackson, "Anaphora resolution in the extraction of treatment history language from court opinions by partial parsing" (1999) *International Conference on Artificial Intelligence and Law '99*, 138-146; S Bruninghaus, K D Ashley, "Improving the Representation of Legal Case Texts with Information Extraction Methods" (2001) *Proceedings of the International Conference on Artificial Intelligence and Law '01*, 42-51; J J Daniels, E L Rissland, "Finding Legally Relevant Passages in Case Opinions" (1997) *Proceedings of the International Conference on Artificial Intelligence and Law '97*, 39-46; P Jackson et al., "Information extraction from Case Law and Retrieval of Prior Cases By Partial Parsing and Query Generation" (1998) *Proceedings of the International Conference on Artificial Intelligence and Law '98*, 60-67; M-F Moens, C Uyttendaele, J Dumortier, "Abstracting of Legal Cases: The SALOMON Experience" (1997) *Proceedings of the International Conference on Artificial Intelligence and Law '97*, 114-122; P Quaresma, I P Rodrigues, "A Question-Answering System for Portuguese Juridicial Documents" (2005) *Proceedings of the International Conference on Artificial Intelligence and Law '05*, 256-257; T M van Engers, et al., "POWER: Using UML/OCL for Modelling Legislation – An Application Report" (2001) *Proceedings of the International Conference on Artificial Intelligence and Law '01*, 157-167; C Biagioli et al., note 1025, 133-140; de Maat/Winkels, note 1029, 170-191; E de Maat, R Winkels, "Suggesting Model Fragments for Sentences in Dutch Law" (2010) *Proceedings of the Third International Workshop on Juris-informatics*, 19-28.

[1034] McCarty, note 1032, at 217; see also M Collins, "Head-driven Statistical Models for Natural Language Parsing" (2003) 29:4 *Computational Linguistics*, 589-637.

[1035] A parser is a computer program that breaks down text into recognised strings of characters for further analysis, *Merriam-Webster Dictionary* , available online at http://www.merriam-webster.com/dictionary/parser.

[1036] See for further details, references in footnotes 1015, 1016.

To conclude it can be summarised that combined with the capabilities of software to be rule-complicit, and reason about circumstances and adapt their actions according to situations, the incorporation of laws into MIA tools to enable these to act law-complicit seems possible.[1037]

However, some problems remain. In particular, as Hildebrandt and Koops point out, machine language will encounter difficulties dealing with open norms like "reasonable care" or "reasonable suspicion", which need to be interpreted with considerable attention to the context of a concrete case.[1038] Overcoming this problem will require detailed refinements, specifying relevant circumstances and the weight that must be attributed to them. MIA tools are particularly suited for such refinements, because the use of these tools is clearly defined, thus the relevant open legal norms and concepts could be determined before the design of these tools.

The previous two sections have shown that it is technically feasible to develop law-abiding MIA tools. However, the analysis of the technical requirements involved has also highlighted that these rely on state-of-the-art research, which is still developed at the moment. This means that incorporating these techniques into MIA tools might give rise to problems of robustness and reliability of the tools. However, the clear restriction of the use of these tools for specific purposes, i.e. investigative actions, provides a frame for the design of the necessary technical requirements, and therefore adds to the reliability of the techniques, and eventually the tools.

[1037] The focus of this chapter has been on the ability of software to behave rule-complicit, and the translation of natural language laws into formal language. However, in addition to these requirements, for software to act law-complicit and enable it to fully "understand" the meaning of incorporated rules, meaning needs to be ascribed to concepts and rules, e.g. "dishonestly" and "appropriating" in the above example. This can be achieved through ontologies that are incorporated into the software. See for a general introduction to the concept of ontology e.g. B Smith, C Welty, "FOIS Introduction: Ontology – Towards a New Synthesis" (2001) *Proceedings of the International Conference on Formal Ontology in Information Systems*, 3-9; B Smith, "Beyond Concepts: Ontology as Reality Representation" in A C Varzi, L Vieu (eds) Formal Ontology in Information Systems (Amsterdam: IOS Press, 2004) 73-84. See for an application of ontologies to the legal domain e.g. J Breuker, R Winkels, A Valente, "A Core Ontology for Law" in K van Marcke, W Daelemans (eds) *Proceedings of the 9th Dutch AI Conference* (Antwerpen: NVKI, 1997), 115-126; R Hoekstra et al., "The LKIF Core Ontology of Basic Legal Concepts" (2007) *Proceedings of the Workshop on Legal Ontologies and Artificial Intelligence Techniques (LOAIT 2007)*, 43-63.

[1038] Hildebrandt/Koops, note 939, at 453.

Nevertheless, these technical challenges also prompt concerns of a political-legal nature, as discussed above.[1039] Developing and implementing the technical requirements is likely to be very cost-intensive. However, as discussed above, outsourcing these tasks to private industry could lead to a loss of objective law making and therefore negatively impact the principles of a democratic society. Given the fact that these tools are designed for use by law enforcement agencies, and therefore a need for confidentiality of the exact details of the design exists, the outsourcing of the development of these tools is not without risks. This was confirmed during the interviews by representatives of both, the UK and the German government.[1040] It was explained that the preferred –albeit not always realisable approach- is the development of such tools internally. This would diminish concerns that industry demands and needs could influence the development of the tools negatively.

It can be concluded, that the development of a MIA Law, i.e. the design of law-complicit tools, to enable their governance through design, is possible.

8.5 Assessing the Risks of a MIA Law

So far, the focus of this chapter has been on the legal and technical feasibility of regulating MIA technologies through code. However, a notion of MIA Law, meaning the incorporation of laws into MIA technologies to enable law-complicit behaviour, is not without problems of a legal and conceptual nature. Assessing these risks is important for the consideration of the implementation of this approach.
This section considers the risks that can be deduced from the above analysis, and the envisaged use of the tools. This is therefore by no means a discussion of all possible risks involved in the implementation of a MIA law.

As discussed above, the technical challenges of this approach as a regulatory instrument arise from the novelness of the relevant techniques. This prompts two somewhat connected risks: (1) the risk of developer failure, and (2) the risk of design-failure.
The development of law-abiding MIA tools requires the incorporation of state-of-the-art techniques, and scientific findings. This necessarily requires that the developers are

[1039] See p. 269 for details.
[1040] See p. 67ff.

capable of dealing appropriately with these novel technologies, and able to apply and modify these to the specific requirements of MIA tools. As such, it becomes clear that there is a significant risk that developers could fail to achieve this, and thereby negatively impact the accurate functioning of the MIA tools. Therefore, thorough selection of suitable IT specialists is mandatory for the successful implementation of this design-based regulatory approach.

Another risk that arises from the novel technologies required for the realisation of law-abiding MIA tools is the potential for design-failure. These can occur in two ways: firstly through the mal-functioning and unreliability of the tool in its entirety, and, secondly, through the failure of implementing the relevant laws effectively.
Generally, the robustness and reliability of information systems and technologies depends on the stability and robustness of their components.[1041]

Robustness can be considered as a degree to which a system can function correctly in the presence of inputs different from those assumed, alternatively it guarantees the maintenance of desired system characteristics despite fluctuations in the behaviour of the system components or its environment.[1042] It also includes resilience and measured degradation in the event of failures, attacks, faulty assumptions, and erroneous use.[1043] Given the intended use of MIA tools, fluctuations of the network environment are likely. To ensure robustness and reliability of technologies, the different components need to be validated.[1044] The problem is that different components each have different characteristics, so the challenge is to compose heterogeneous components to ensure their correct interoperation.[1045]
Robustness therefore requires a broad spectrum of properties, such as safety, security, and availability.[1046] These properties need to be developed for the specific applications, and sufficiently tested before using the tool. Nevertheless, there is always the risk of system failure, particularly when new technologies are used.

[1041] M Burgin, "Robustness of Information Systems and Technologies" (2009) *Proceedings of the 8th WSEAS International Conference on Data Networks, Communications, Computers*, 67.
[1042] S Ali et al., "Definition of a Robustness Metric for Resource Allocation" (2003) *Proceedings of the 17th International Symposium on Parallel and Distributed Processing*, 42.
[1043] T A Henziger, J Sifakis, "The Discipline of Embedded Systems Design" (2007) *IEEE Computer Society*, 37.
[1044] Burgin, note 1041, at 67.
[1045] Burgin, note 1041, at 67.
[1046] Henziger/Sifakis, note 1043, at 38.

The other potential design-failure relates to the successful embedding of the relevant laws. The problem here is that despite careful attention to the translation of laws, these may nevertheless fail to bring about the desired policy objectives and results. This can be due to the imperfect match of traditional laws and new technologies. Traditional legislation has been drafted with the parameters of the physical world, and a human interpreter in mind. Translating these into machine-processable format can lead to undesired imperfections between the rule and its purpose, and the interpretation and execution of this by the MIA tool. This could be the case because of the fundamental differences between the online and offline sphere.

Koops also discusses this point in his work, asking how rules that are implemented into technology should be assessed, given that technology has special characteristics when it enforces or establishes legal norms.[1047] Thus it might be necessary that those responsible for the selection of the relevant legislation adapt this appropriately, without changing the intention of the law. This requires as highlighted by Flanagan et al.,[1048] collaboration between lawyers and scientists. The reason why this has not happened more frequently in the past is that in both areas knowledge and methodologies are traditionally far-flung and self-contained. However, this state needs to be overcome, as collaboration is essential for the successful implementation of laws into technologies. In addition, a test-run phase is necessary, where legal experts assess the outcome of the engineering efforts. Again, collaboration is an essential factor at this stage.

However, despite the best efforts of experts from both disciplines, in particular because both design-failure options can trigger each other, these are risks that remain.

In addition to technology-inherent risks, there are legal risks that arise from the translation of the legislation into machine-processable format.

The rules embedded into the technology are unlikely to be exactly the same as the original rules established by legislature. This is not only because the translation process from natural into formal language by default changes the rule, but also because, as discussed above, rules might have to be changed before they are incorporated into technologies. Thus, in the translation process, choices and reductions take place, and these choices are not necessarily made by the responsible legislative public authorities

[1047] Koops, note 876, at 159.

[1048] Flanagan/Howe/Nissenbaum, note 920, at 324.

subject to democratic checks and balances, but by technology developers who are at best subject to EDP auditors.[1049] The regular checks and balances of law making therefore risk to be circumvented by MIA tools, and democratic and constitutional criteria are thus *a fortiori* relevant for these technologies.

It is therefore essential to develop a systematic approach for the evaluation of the translation process, and the formal rules embedded into MIA tools. Asscher has developed a still fairly rough and tentative set of criteria, presented in the from of questions for the evaluation of "code rules", and thus MIA law:[1050]

1. Can code rules be understood? If so, are they transparent and accessible to the general public?
2. Can the rules be trusted? Are they reliable in the sense of predictability?
3. Is there an authority that makes the code rules?

Koops summarises this set as: transparency, reliability, and accountability.[1051]

A system to evaluate the translation of laws into formal format needs to take these criteria into account.

The last risk to be discussed in this chapter can be derived from the previously discussed one, and the fact that MIA tools operate clandestinely.

If the formal rules of MIA law cannot be evaluated appropriately, and the tools are deployed in a way that targeted suspects and other citizens cannot directly observe the investigative actions, this may lead to a lack of trust of people in the integrity of the Internet, and arguably more seriously, the integrity of law enforcement. Suspects and third parties (such as lawyers) can observe traditional investigative actions (such as the search of a premise), and therefore verify the adherence of law enforcement to relevant legislation governing the investigative actions.

This is not the case if a MIA tool undertakes the investigative actions without the knowledge of the suspect. If the laws implemented into MIA tools are not evaluated through a democratic and public system of checks and balances, this can lead to the

---

[1049] Koops, note 876, at 161. An EDP audit is an analysis of an organisation's computer and information system in order to evaluate the integrity of its production system as well as potential security cracks (EDP audit, The Free Dictionary, available online at: http://encyclopedia2.thefreedictionary.com/EDP+audit).

[1050] L F Asscher, note 962, at 85.

[1051] Koops, note 876, at 164.

impression that the state potentially deploys investigative tools that violate privacy and data protection rights of the targeted suspects, and do not abide appropriately to other legislation regulating investigative actions.
This would lead to a lack of trust in the use of the Internet, since MIA tools might potentially be present at all times to monitor user behaviour, as well as a lack of trust in the democratic system in general, since governments would undermine the main pillars of democratic law-making through the use of these technologies.

The risks discussed in this section have highlighted that the introduction of a MIA Law is tied to fundamental technical and legal problems. These need to be addressed and balanced against the benefits of the design of law-abiding technologies before these can be introduced.

8.6 Conclusion

This chapter has covered a wide range of issues relating to the regulatory challenges analysed in the previous chapters. The hypothesis that the technical abilities of MIA tools can be used to design these to be law-complicit has been confirmed.

This is an important finding for the development of a sustainable governance model for MIA tools, and the new cyber-policing system as a whole. Given the highly intrusive nature of investigations by MIA tools and the relevance of the virtual living space, developing such a model is an urgent matter.

The discussion of the regulatory modality code has confirmed what the previous two chapters have indicated: that it is difficult to regulate ICT technologies through law alone.
Code, or the technology's architecture, plays a crucial factor in its regulation. Code can be modified to manipulate human behaviour, however, it can also be modified to influence technology behaviour, and thereby assist the traditional regulatory modality law in adequately regulating ICT technologies.

This chapter has developed the notion of MIA law. This notion is premised on Lessig's finding that code is a regulatory modality, the work of Nissenbaum et al. that rules can be implemented into code, as well as the notion of Ambient law developed by Koops

and Hildebrandt. However, these works have remained entirely theoretical and did not explore in how far these notions are technically feasible. This thesis has closed this gap for the specific notion of MIA law.

The analysis of the technical requirements for implementing relevant legislation into MIA tools has indicated that the necessary techniques are state-of-the art research. This means that only specialists are capable of developing MIA law and issues of reliability and robustness of the MIA tools arise. This makes an immediate implementation of this governance model doubtful.

However, these risks need to be addressed in the near future to enable the successive implementation of this approach, and therefore the lawful use of MIA tools.

9 SOFT MIA LAW NOTION

The previous chapter (8) has developed the notion of MIA law as a regulatory model for MIA tools, and the cyber-policing system as a whole. This notion is premised on the findings that code is a regulatory modality,[1052] and natural language laws can be translated and implemented into software code to endow technologies with legal reasoning capabilities. [1053]

The notion of MIA law constitutes a sustainable solution for the governance of MIA tools. The new cyber-policing system and its software-based investigative tools have so far lacked a structured governance approach, which has caused insecurity about the tools legality and rights violations of affected persons.

However, as analysed in the previous chapter, the notion of MIA law is a technically complex model, and necessary techniques are not yet standardised and therefore unreliable. Implementing these into governmental investigative tools would prompt further legal issues and increase the lack of trust and legal certainty into the cyber-policing system. Additionally, the urgent legal problems linked to the use of MIA tools discussed in this thesis,[1054] and particularly the problem of evidential value of the data seized by MIA tools would remain unsolved. This would impair the usability and legality of MIA tools during investigations of the virtual living space.

This chapter therefore develops a variation of MIA law, a "soft MIA law", which still relies on endowing software with legal reasoning capabilities but focuses more on the outcomes of, rather than the replicating of the legal reasoning process.
While this approach in some ways lacks the level of abstraction deployed by Sartor et al. in their work and introduced in the previous chapter, it is a solution that can provide greater impact and robustness of MIA tools in the short term than the more complex and state-of-the-art MIA law developed in the previous chapter.

[1052] See Lessig (1999), note 24; Lessig (2006), note 627.
[1053] See p 274ff; Sartor, note 982; Gelati/ Rotolo/Sartor/Governatori, note 982.
[1054] See chapters 6 and 7.

The notion of soft MIA law equally relies on legal reasoning abilities of the software and the translation of laws and legal norms into machine-readable format. However, the reasoning and decision-making demands on the software tool are reduced, and thus the required level of programming complexity.

This means that the robustness and reliability of the MIA tools is increased, as well as the demands on the operator. This simplifies the development and design of MIA tools, and therefore also reduces the costs.[1055] This also means that capable software developers can be contracted more easily. In addition, this approach requires less technical knowledge from the operator of the tool. This means that personnel can be trained more easily and problems due to operating mistakes avoided.[1056]

The proposed system is, in short, a firewall type protocol that serves as an intermediary between the MIA tool and the operating authority to filter data and communication that cannot be lawfully transmitted, and communicate commands and requests to the MIA tool. This system, which is standardised and can be operated by any officer requiring the use of a MIA tool can be regarded as a quasi digital judge, making decisions about the usability and admissibility of data collected, and depending on for example the type of warrant underlying the search and seizure action, making decisions regarding the permissible actions.
Thus the firewall is acting as an information gateway between the MIA tool and the operating authority.

The first part of this chapter reviews in section 9.1 the particular technical problems identified in the previous chapter, and introduces three short case scenarios that highlight how the nature of MIA tools causes, at this stage, problems for reliability and robustness if a strong notion of MIA law is implemented. The second part introduces in section 9.2 the soft MIA law notion in more detail, and depicts how this can serve to overcome the technical problems of the strong MIA law notion while at the same time solving the current issues linked to the policing of the virtual living space by MIA tools. Section 9.3 concludes with the main findings of this chapter.

[1055] The problem of high development costs was one of the key problems identified by the experts. See chapter 3, p. 68.
[1056] This was another key problem identified by the experts. See chapter 3, p. 68.

9.1 Problems of the Strong MIA Law Notion

The previous chapters have analysed the technical and legal issues of the use of MIA tools for the policing of the virtual living space.[1057] This analysis, as well as the empirical research results, have evidenced that MIA tools challenge in particular existing privacy and data protection rights, sovereignty principals, and evidence principals and laws. Solving these problems through the traditional regulatory modality law alone is insufficient due to the nature of MIA tools. These investigative tools police the virtual living space autonomously and replace human investigators for core policing tasks. This means that these tools must adhere to existing legislation, which requires, as shown in the previous chapter, a regulation through code approach.

The analysis of the technical foundations of MIA law has however evidenced that the required technical standard for a successful implementation of this regulatory approach relies on state-of-the-art technology, which is not yet available as "off the shelf" products, and particularly not for the legal domain.
This creates further problems for the regulation of the most pressing legal issues identified above.

Three short case scenarios tailored to these legal issues (violations of privacy and data protection rights, sovereignty rights, and evidence principles and laws) are presented below. These case scenarios serve to highlight the particular technical problems of the implementation of the strong MIA law notion. This analysis is important for the development of the soft MIA law, which is focused on avoiding the technical problems of the strong MIA law.
The case scenarios focus is on the case study of this thesis, the online searching of ICTs,[1058] as a confirmed investigative measure of the virtual living space.

> ***Scenario a****.: A search warrant is granted for a remote search of the computer and other ICT devices of suspect X. He is suspected to be member of a group in Germany, which is planning to attack a mosque. The evidence linking him to the group is strong but no urgency is indicated. The search warrant allows for the search of relevant documentation stored on the ICT devices, as well as the monitoring of relevant communication.*

[1057] See particularly chapters 6 and 7.
[1058] See chapter 2.

> ***Variation aa****.: The evidence linking X to the group suggests that the attack is imminent, and therefore urgent measures are required. Thus the search warrant allows for the search of all documentation stored on the ICT devices, as well as the monitoring of all communication.*

In case scenario a. the MIA tool needs to be capable of selecting, copying and transmitting solely data that is directly relevant and linked to the planned attack. Due to German data protection rights, the operating authority is not allowed to view and use any other material, and in particular not material from the core area of private life.[1059]

In the case variation aa. the MIA tool may copy any data stored on the ICT devices, and monitor any communication by the suspect.

However, information from the core area of private life needs to be excluded in this case, too.

Based on the analysis in chapter 8 of ACLs and formalisation of natural language,[1060] these scenarios can be formally expressed as:

> Scenario a.: Does $_{(MIA,t)}$ [undertake search and monitoring activities of systems X] THEN^{n} Obl Does$_{MIA}$ [search only relevant data]
> THEN^{n} Obl Does$_{MIA}$ [disregard core private data]
> This can be read as "the MIA tool undertakes searching and monitoring activities of systems X at time t, and it is obligatory that MIA searches relevant data only, and disregards core private data".

In addition, such formally expressed commands require the "knowledge" of the MIA tool about certain legal concepts. In this short scenario this is "relevant data" and "core private data":

> Data [((¬ data(x) →relevant(pertaining_to_personX, topicY) ∧ disregard_core_private(medical records, diary entries, bank statementsbelonging to y)].
> This can be read as "data is any data x if it is relevant, which is data pertaining to suspect X and topic Y, and not from the core area of private life, which are medical records, diary entries, and bank statements belonging to suspect X".

[1059] See p. 47ff.
[1060] See p. 285ff.

Variation aa.: Does (MIA,t) [undertake search and monitoring activities of systems X]
THEN^{n} Obl Does$_{MIA}$ [disregard core private data]
This can be read as "the MIA tool undertakes searching and monitoring activities of systems X at time t, and it is oblifatory that MIA disregards core private data".

In addition, these formally expressed commands require the "knowledge" of the MIA tool about the legal concept "core private data":

Data [((¬ data(x) →any(ICT system of personX) ∧
disregard_core_private(medical records, diary entries, bank statementsbelonging to y)].
This can be read as "data is any data x if located on ICT systems of suspect X, and which does not pertain to the core area of private life, which are medical records, diary entries, and bank statements belonging to suspect X".

***Scenario b**. A search warrant is granted for a remote search of the computer and other ICT devices of suspect X. He is suspected to be member of a group in Germany, which is planning to attack a mosque. Shortly after the search has commenced suspect X travels to the UK.*

***Variation bb.** The UK grants German authorities the right to conduct investigative actions on their sovereignty.*

Case scenario b. requires the MIA tool to be capable of detecting when the suspect leaves German sovereignty, and stop all investigative actions while the suspect is abroad.
Variation bb. requires the MIA tool to be capable of overriding the general rule that investigative actions outside of German sovereignty are forbidden, and continue search and monitoring actions on UK sovereignty.
Based on the analysis in chapter 8 of ACLs and formalisation of natural language,[1061] these scenarios can be formally expressed as:

[1061] See 285ff.

Scenario b.: Does (MIA,t) [undertake search and monitoring activities of systems X]
Forb $Does_{MIA}$ [undertake search and monitoring activities while ICT device is outside sovereignty]
This can be read as "the MIA tool undertakes searching and monitoring activities of systems X at time t, but it is forbidden to undertake search and monitoring actions while the suspect's ICT device is outside of German territory".

In addition, these formally expressed commands require the "knowledge" of the MIA tool about the legal concept "sovereignty".[1062]

Sovereignty[((¬ geographic area(x) →authority($Germany_{supreme, independent}$) →IP address (German))]
This can be read as "sovereignty is a geographic area x, if Germany has supreme and independent authority over it, which is the case if the IP address can be assigned to Germany".[1063]

Variation bb.: Does (MIA,t) [undertake search and monitoring activities of systems X]
Forb $Does_{MIA}$ [undertake search and monitoring activities while ICT device is outside sovereignty]
Perm $Brings_{UK}$ [$Perm_{MIA}$ carry-out investigative action X]
This can be read as "the MIA tool undertakes searching and monitoring activities of systems X at time t, but it is forbidden to undertake search and monitoring actions while the suspect's ICT device is outside of German sovereignty, unless the UK has permitted that the MIA tool carries out the investigative action X on its sovereignty.

[1062] In this particular case, the legal concept "sovereignty" needs to refer to German sovereignty. Furthermore, a technical element that allows the MIA tool to autonomously detect whether an ICT device is operated in a specified sovereignty is required.
[1063] The reason for choosing an IP address as the technical element to detect where the ICT device is operated is that several open access web portals exist, where an IP address can be entered and its origin checked. An example of such a web portal is: http://software77.net/geo-ip/. Obviously, this approach has weaknesses, such as for users of virtual private networks (VPNs).

In addition, these formally expressed commands require the "knowledge" of the MIA tool about the legal concept "sovereignty".[1064]

> ***Scenario c.*** *A search warrant is granted for a remote search of the computer and other ICT devices of suspect X. He is suspected to be member of a group in Germany, which is planning to attack a mosque. All data seized by the MIA tool needs to be authentic and reliable for it to be used as evidence.*

Case scenario c. requires the MIA tool to be capable of creating bit-stream copies of all data seized, which feature time stamps so that the data can be used as evidence in court proceedings, and thus has any value for the investigation.
Based on the analysis in chapter 8 of ACLs and formalisation of natural language,[1065] these scenarios can be formally expressed as:

> Does (MIA,t) [undertake search and monitoring activities of systems X]
> Obl $Brings_{MIA}$ [create bit-stream image of data X]
> Obl $Brings_{MIA}$ [add time stamps to data X]
> This can be read as "the MIA tool undertakes searching and monitoring activities of systems X at time t, and it is obligatory that the MIA tool brings it about that a bit-stream copy of data X is created, and time stamps are added to data X.

In addition, these formally expressed commands require the "knowledge" of the MIA tool about the technical concepts "bit-stream image" and "timestamp".

> Bit-stream image[(¬ bit-by-bit copy($data_x$) →set_of_files(exact copy of hard drive X))]
> This can be read as "a bit-stream image is a bit-by-bit copy of data X if the set of files is an exact copy of the hard drive X.

> Timestamp[(¬ proof (time of which event occured) →sequence of characters(time at which event is recorded by computer))]

[1064] See above under b. for the formal expression of the legal concept "sovereignty".
[1065] See p. 285ff.

> This can be read as "a timestamp is a proof of a time at which an event occurred, if the sequence of characters is the time at which the event is recorded by the computer.

These three examples, highlighting the most pressing legal challenges arising from the use of MIA tools (violation of privacy and data protection rights, sovereignty, use as evidence) have deliberately been kept very simple. More complex scenarios would have made the formal representation far more complicated, and thus more difficult to comprehend.

The aim, however, was to depict the technical challenges arising from the implementation of the strict MIA law notion. For this, simple case scenarios are sufficient and in fact more adequate. If the arguments against the implementation of the strict MIA law notion are applicable to these simple scenarios they are, a fortiori, to more complex scenarios.

While all three scenarios (including the case modifications) are focused on a different legal problem they highlight the technical difficulties faced by software developers of MIA tools.

Chapters 4 and 5 have analysed the general technical abilities of MIA tools.[1066] The most significant being mobility, intelligence and autonomy, which enable these tools to replace human officers for policing tasks and, for example, undertake text analysis, data retrieval, link analysis, and platform migration.
Designing software tools featuring these capabilities requires a high standard of technical knowledge and sophisticated software. As shown in chapter 4,[1067] software solutions featuring some of these abilities exist and are already deployed by various authorities. This means that these systems are robust and reliable, as well as sufficiently predictable in their operations and outputs.
Reliability and robustness, as well as predictability are crucial attributes of software tools in general, but particularly if they operate autonomously and are deployed for sensitive tasks, such as the searching of ICT devices of suspects during investigations.

[1066] See p. 84ff, 123ff.
[1067] See p. 119.

The challenge for designers is thus to design "high-level programming models that expose the reaction and execution properties of a system in a way that
1. permits the programmer to express desired reaction and execution requirements and, 2. permits the compiler and run-time system to ensure that these requirements are satisfied."[1068] This in turn facilitates robustness and predictability of the software tools.

Robustness in software systems requires that the systems feature robust behaviour in the presence of perturbations.[1069] Hence, that a system is able to function correctly and coherently in a changing environment, in the presence of invalid or conflicting inputs, and in the presence of situations not considered during the design phase.[1070]
The more complex the systems the more challenging is the task of ensuring system robustness. This is because it is extremely difficult and sometimes impossible to anticipate all the possible scenarios in which these complex systems will perform so as to make the appropriate tests.[1071] Particularly challenging is the task of testing autonomic elements and verifying that they behave correctly, because it is harder to anticipate their environment, particularly if it extends across multiple administrative domains or enterprises.[1072]

Predictability in software systems refers to the ability to predict behaviour of systems.[1073] Thus predictability is closely linked to robustness of software systems, but is focused on the outputs of the software, as well as the timely execution of tasks. Predictability in dynamic systems can be summarised as the ability to predict the timing requirements of critical tasks with 100% guarantee over the life of the system, to assess overall system performance over various time frames, and to assess

---

[1068] T A Henziger, "Two Challenges in Embedded Systems Design: Predictability and Robustness" (2008) *Philosophical Transactions of the Royal Society*, 2.
[1069] Ibid, at 7.
[1070] M N Huhns, V T Holderfield, R L Z Gutierrez, "Achieving Software Robustness via Large-Scale Multiagent Systems" in C J Pereira de Lucena et al. (eds) *Software Engineering for Multi-Agent Systems II, Research Issues and Practical Applications* (Berlin, Heidelberg: Springer Verlag, 2003) 199-215, 199.
[1071] Ibid.
[1072] J O Kephart, D M Chess, "The Vision of Autonomic Computing" (2003) 36:1 *IEEE Computer*, 41-50, 41.
[1073] Huhns/Holderfield/Gutierrez, note 1070, at 3.

individual task and task group performance at different times and as a function of the current system state.[1074]

If robustness and predictability are achieved, the software tool can be considered reliable.

Given the significant legal values that are at stake, reliability, thus robustness and predictability of the MIA tool is mandatory for it usage.

However, as the brief definitions of robustness and predictability of software have shown, the more complex software is, and the higher the degree of autonomy the more difficult it is to achieve these attributes. In addition, the high complexity of a tool combined with its use on a multitude of systems and platforms complicates the anticipation and testing of all potentially possible scenarios the system will have to perform in.

The case scenarios above have shown that the strict MIA law notion requires the implementation of very complex, and state-of-the-art techniques. In addition, it has highlighted that particularly in the legal domain oftentimes unpredictable situations arise, which require the MIA tool to undertake legal reasoning on a high level. While the case scenarios have deliberately been kept simple much more complex reasoning by MIA tools is required during investigations of the virtual living space. The previous chapters have highlighted some of the pertinent legal issues.[1075]

As mentioned above, the "core abilities and functions" of MIA tools already require a high technological standard. However, given the sophistication of these techniques, and mainstream usage of tools incorporating these techniques, these tools can function under changing circumstances, as well as deal with unpredictable situations, thus feature software robustness. Their actions are also sufficiently predictable, given the amount of research undertaken in this area.[1076]

However, the required techniques to implement a strict MIA law, namely the incorporation of an advanced ACL and natural language processing abilities, are at the point of writing this chapter still very much a work in progress.

[1074] J A Stankovic, K Ramamritham, "What is Predictability for Real-Time Systems?" (1990) 2 *Real-Time Systems,* 247-254, 254.

[1075] See chapters 6 and 7.

[1076] See chapters 4 and 5 for a summary of important research results, also for the legal domain.

While the techniques already exist, for the legal domain these are currently predominantly developed in the academic arena, and therefore have not yet been implemented into a wide array of commercially available software tools.
This means that knowledge about the functioning of tools in a changing environment is very limited, if existing at all, and it is also unclear how these tools would cope with unpredictable situations.
In addition, their actions during investigations are not predictable, given the lack of appropriate tests. This is particularly true for MIA tools, due to their anticipated use for sensitive purposes.
Chapters 2 and 3 have highlighted the need for secrecy and the lack of publicly available information about the exact details of the use of MIA tools. This need for secrecy impacts on the ability of software designers to sufficiently test relevant scenarios during the development stage.
Thus, MIA tools possessing the necessary technical requirements to implement a strict MIA law can be designed, however, lack robustness and predictability, and therefore reliability. This means that their value for sensitive criminal investigations is severely impaired.
In addition to these technical concerns, there are also concerns about the sharing of the data seized by MIA tools. As briefly indicated in case scenarios a. and aa., the seized data may only be shared with authorised officers.
Authorisation, however, can vary depending on the urgency and the type of warrant. This means that the MIA tool needs to be capable of verifying whether the officer requesting the data is in fact also authorised to receive it. This adds another element to the reasoning process the MIA tool needs to accomplish, and therefore to the technical capabilities of these tools.
It is, however, of great importance that the seized data is solely shared with authorised officers. Privacy and data protection rights of the suspect would be breached if unauthorised officers would have access to the personal data. On the contrary, it can be equally important that all authorised officers receive the relevant data. Thus failure to disclose the data can be as harmful as the disclosure of data to unauthorised officers because it can negatively affect the investigative progress.
Adding this element to the reasoning process of MIA tools further complicates the technical process, and thus challenges the reliability of the tools.

Hence, the implementation of a strong MIA law to solve the legal problems of deploying MIA tools during investigations of the virtual living space is at the current stage of technological development inadvisable.[1077]

The analysis of the problems of implementing a strong MIA law has evidenced that the main issue of this notion is the high technical demand on already complex software tools. The legal domain requires absolute reliability of the tools to ensure no rights violations occur during investigations and the evidence seized can be used during court proceedings. At the current state of the art of technology research this cannot be guaranteed. This is particularly the case because MIA tools operate on different platforms and migrate on the Internet, a heterogeneous network. This unstable environment puts additional demands on the software and complicates the test phase of the software tools, and thus challenges its reliability.

However, the technical analyses in chapters 4, 5 and 8, as well as the previous section have revealed that the relevant technologies and technical applications to develop MIA tools and the MIA law exist. The problem at this stage is the implementation of MIA law into MIA tools. The governance modality code however remains the best-suited approach to ensure law-complicit behaviour of MIA tools and thus avoid rights violations and enable the awful use of these tools.

The following section therefore develops a soft MIA law notion, which still relies on endowing software with legal reasoning capabilities but avoids the technological challenges of the strong MIA law notion.

9.2 Soft MIA Law

Generally, at the core of any investigation of the virtual living space is the need for data selection and verification, as well as data sharing with authorised persons.

As highlighted by the case scenarios in the previous section,[1078] most of these requirements can be relatively well defined in advance. For example, it can be determined that as a general rule, the MIA tool is not allowed to seize data abroad without permission of the country in question. Furthermore, core private data cannot be used during investigations.

[1077] This does not mean, however, that this is generally not a suitable regulatory model. As analysed in chapter 8, principally this approach offers significant benefits over the traditional "regulation through law" approach. Hence, once the necessary technological development has been accomplished, a strict MIA law notion should be implemented.

[1078] See p. 299ff.

Thus, specific rules, derived from laws and principles that govern the investigative actions and the recording, access to, and use of the seized data can be established. The soft MIA law notion is a system that transfers the legal reasoning process about these rules to a static system, and therefore circumvents the technical problems of the strong MIA law notion analysed above. The MIA tool carries out the investigative actions,[1079] but is not burdened with the additional task of ensuring law-complicit behaviour. The reasoning about the investigative actions of the MIA tool is conducted by an additional system.
This system serves as a filter to ensure that certain data is not shared at all (e.g. core private data), specific rules are enforced (e.g. no investigative actions on foreign sovereignty), and data is only shared with authorised personnel. Hence this system assists and complements the work of the MIA tools, and at the same time guarantees reliability and legality of the results.

This is accomplished by a software agent-based "Single Point of Contact (SPoC)" model, which is implemented as software agents that serve as gateways for data control and information requests. Such a system works similarly to a firewall within a computer network, and ensures that the specified rules are adhered to.

At a basic level, firewalls use a defined set of rules to either permit or deny network traffic.[1080] Similarly, the suggested SPoC agent system validates requests for data delivery and information exchange based on rules, derived from organisational policies and legislative requirements, as defined in relevant laws and policies.
This means, for example, that the agent attempts to match the request for access to data against the rules defined in relevant data sharing regulations and implemented into the SPoC system. If the request does not match a rule, the agent will then attempt to match the request against the next rule and so on. Once a match is found, the agent will carry out the action (permit or deny), as defined by that rule, and end the searching (as a firewall would). If no matching rule is found in the set, the agent will deny the request. This is similar to the idea of an implicit deny criterion used by firewalls where

[1079] See chapter 4 p. 84ff for a discussion of these details.
[1080] See e.g M K Khan, M Mahmud, K S Alghathbar, "Security Analysis of Firewall Rule Sets in Computer Networks" (2010) *Fourth International Conference on Emerging Security Information Systems and Technologies (SECURWARE)*, 51-56.

no matching rule is found. In the case that a request is denied, the agent will return information indicating the reason for the denial.

Similarly, the agent matches data delivered by the MIA tool against the rules defined in relevant data protection and privacy legislation, implemented into the SPoC system. If the data does not match a rule, the agent will attempt to match the data against the next rule and so on.

Once a match is found, the agent will carry out the action (permit or deny), as defined by the rule, and end the searching. Contrary to the data access request however, if no matching rule is found, the data will be permitted into the system. This is based on the assumption that unlawful data (e.g. core private data) is generally filtered out by an existing rule, and additionally any data may be highly relevant, thus rejecting data because it cannot be matched to an existing rule could have serious consequences. However, similarly to red flagging of data by firewalls, such "unknown" data is red-flagged, and access to it strictly limited (for example to the investigative judge only).

The advantage of two software agent-based systems[1081] is that the communication between the systems is not an issue due to the fact that standardised ACLs can be used for communication.[1082]

The below figure provides a visualisation of the communication between the MIA tool, the SPoC agent, and the operating agency.

[1081] As discussed in chapters 4 and 5, MIA tools share crucial features with software agent technology, and particularly for the communication capabilities.

[1082] See particularly 4.3.3 p. 114, explaining multi-agent systems.

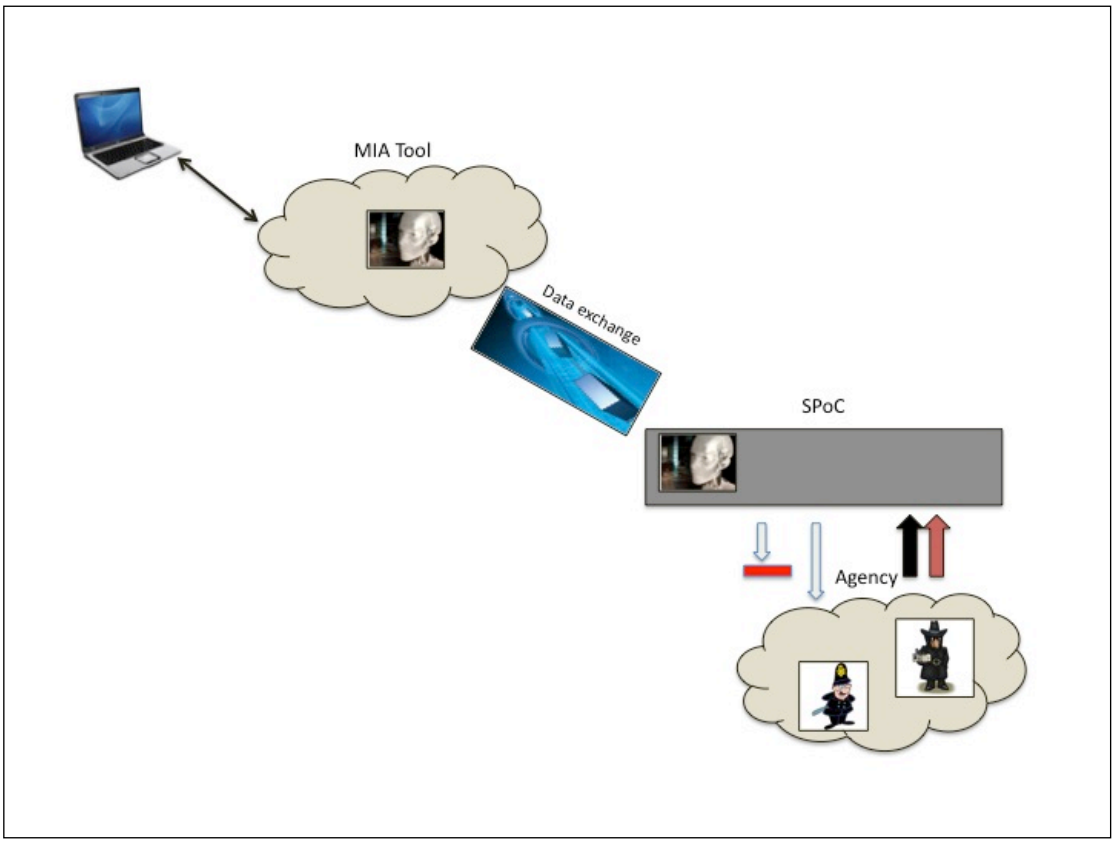

Figure 1: Overview of the architecture

9.2.1 Technical Details

As highlighted in Figure 1, the SPoC system serves as a quasi firewall, which takes on the legal reasoning task and, for example, evaluates the data seized by the MIA tool, and verifies access rights of requesting officers.

As discussed in the previous sections, adding the SPoC system to the investigation process ensures that the data seized during investigations is more reliable, and MIA tools operate lawfully. Additionally, the system ensures that only authorised officers can access the seized data, therefore ensuring that data protection and privacy rights of the suspect are maintained.

The reasons why the SPoC system is, at this stage, better suited for executing these tasks are discussed in the previous section. One of the crucial factors is that the SPoC system is more stable than MIA tools. This is the case because it does not have to function on different platforms and operates by applying pre-defined rules and filters.

Generally, firewalls are deployed on computer networks to serve as components for computer security. A firewall is essentially a filter, either a software program or a hardware device, used in a computer system to prohibit forbidden information from passing through, while allowing approved information.[1083]

"In the enterprise security environment, the *firewall* serves as the frontline security device effectively delineating the perimeter between various zones of security control within the network of an organization. These *zones of control* can range from guarding sensitive data repositories such as a large database of personnel information to separating individual departments from one another to simply protecting the internal network from outside attacks originating in the Internet."[1084]

Firewalls have gained such significance, that they have become nearly ubiquitous with deployment levels approaching 97% within modern enterprises.[1085]

While the focus of the SPoC system is not on security, the architecture is nevertheless identical to that of conventional firewalls. "Security is a complex property, and several diverse factors need to be considered to assess the security of a system's architecture."[1086] Generally, the underlying model must contain classes, attributes, and class-relationships.[1087] Hence, it is very similar in nature to the requirements for the SPoC system, where classes and class-relationships (for example the different types of data), as well as attributes of data are highly relevant.

The below figure illustrates the similarities between the proposed SPoC system and a standard firewall.

[1083] CheckPoint, "Firewall", available online at http://www.checkpoint.com/resources/firewall/.

[1084] M J Chapple, A Striegel, C R Crowell, "Firewall Rulebase Management: Tools and Techniques", in M Quigley (ed) *ICT Ethics and Security in the 21st Century: New Developments and Applications* (Hershey: IGI Global, 2011) 254-276, 255.

[1085] Ibid.

[1086] T Sommestad, M Ekstedt, P Johnson, "A Probabilistic Relational Model for Security Risk Analysis" (2010) 29:6 *Computers & Security*, 659-679, 660.

[1087] Ibid.

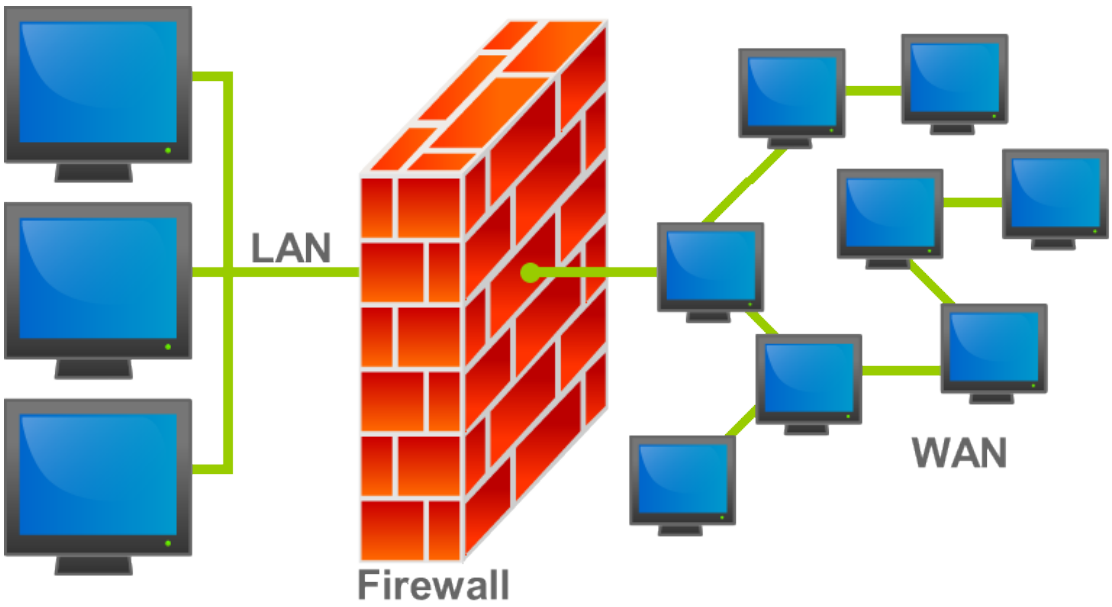

Figure 2: The location of a firewall in a computer system.[1088]

This means that all existing research into the functioning of firewalls can be applied to the SPoC system. Since firewalls are already a mainstream technology, reliability of the underlying techniques is not a matter of high concern.

Generally, firewalls are premised on a rule-based model. A so-called "policy", implemented into the firewall contains all the rules describing what traffic is allowed and what should be filtered out.[1089]

Different models have been proposed for the design of the "policy", the basis for the rule-based decision making ability of the firewall.[1090]

A discussion of all these models would go beyond the scope of this thesis, and is not relevant for this chapter. Relevant is the method applied to define the rules: the rule granularity and the rule enforcement.[1091] This is because the rules and the functioning of the rule enforcement are crucial for the success of the firewall.

[1088] Bruno Pedrozo, CC Attribution-Share alike.

[1089] K Ingham, S Forrest, "A History and Survey of Network Firewalls" (2002) *Technical Report 2002-37, University of New Mexico Computer Science Department*, 1-42, 2, available online at http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf.

[1090] See Ingham/Forrest, ibid, and Chapple/Striegel/Crowell, note 1084, for an overview of architecture designs of firewalls. Sommestad/ Ekstedt/Johnson, note 1086, discuss a probabilistic approach to rule-based decision making.

[1091] A Herzog, N Shahmehri, "Usability and Security of Personal Firewalls" in H Venter, M Eloff, L Labuschagne, J Eloff, R von Solms (eds) *IPIP International Federation for Information Processing,*

This is equally the case for the rules implemented into the SPoC system.

If, for example, a firewall policy includes anomalies, such as where a packet may match with two or more different filtering rules, this can cause malfunction of the system. Such malfunction of the SPoC system could have serious consequences, if, for example, core private data is transmitted. Hence, when the filtering rules are defined, serious attention has to be given to rule relations and interactions in order to determine the proper rule ordering and guarantee correct security policy semantics. As the number of filtering rules increases, the difficulty of writing a new rule or modifying an existing one also increases. It is very likely, in this case, to introduce conflicting rules such as one general rule shadowing another specific rule, or correlated rules whose relative ordering deter- mines different actions for the same packet. In addition, a typical large-scale enterprise network might involve hundreds of rules that might be written by different administrators in various times. This significantly increases the potential of anomaly occurrence in the firewall policy, jeopardizing the security of the protected network.[1092]

Therefore, the effectiveness and reliability of firewalls and the firewall-like SPoC system depends on the accuracy of the rules and the policy management.

Of particular relevance is the modelling of rule relations to avoid anomalies and malfunctioning of the systems. For the successful functioning of the SPoC system it is relevant that the system "knows" for example, the relation between the concept *sovereignty* and *investigative power*, to enable the system to prompt the command "stop all investigative actions" when data is being collected outside of the sovereignty of the operating authority, and thus no investigative powers exist.

Relevant is also knowledge about authorised officers asking for access to the seized data. Here, the SPoC system needs to know the relation between the rank of an officer and the type of warrant. As discussed above,[1093] perceived imminent danger leads to broader access rights to the seized data.

To express these rules and relations in a machine-readable format, these need to be formalised and formally represented.

Volume 232, New Approaches for Security. Privacy and Trust in Complex Environments (Boston: Springer, 2007) 37-48, 37.

[1092] E S Al-Shaer, H H Hamed, "Modeling and Management of Firewall Policies" (2004) *IEEE Transactions on Network and Service Management*, 2-10, 2.

[1093] See p. 306.

Generally, all relevant and possible rules and relations need to be determined and expressed formally. However, presenting a full account of all these would go beyond the scope of this thesis. In any case, relevant for this chapter is not the representation of all existing rules and relations but the presentation of the functioning of the SPoC system in general. For this, it is important and sufficient to discuss the basic functioning of the policy and present examples of selected scenarios.

On a very basic functional level, each rule in the policy is of the form:

$$\langle predicate \rangle \rightarrow \langle decision \rangle$$

where the *predicate* is a Boolean expression[1094] over the different fields of a packet of data,[1095] and the *decision* is either "a" for accept or "r" for reject.
To reach a decision concerning a packet of data, the rules in the sequence are examined one by one until the first rule, whose *predicate* is satisfied by the packet field, is found. The decision of this rule is then applied to the packet of data.
To be capable of reaching the *decision* about the various packets of data received by the SPoC system, the rules for the Boolean expression need to be determined.

These are:
Definition 1 — Rules R_x and R_y are completely disjoint if every field in R_x is not a subset nor a superset nor equal to the corresponding field in R_y.
Definition 2 — Rules R_x and R_y are exactly matching if every field in R_x is equal to the corresponding field in R_y.
Definition 3 — Rules R_x and R_y are inclusively matching if they do not exactly match and if every field in R_x is a subset or equal to the corresponding field in R_y. R_x is called the subset match while R_y is called the superset match.
Definition 4 — Rules R_x and R_y are partially disjoint (or partially matching) if there is at least one field in R_x that is a subset or a superset or equal to the corresponding field in R_y, and there is at least one field in R_x that is not a subset and not a superset and not equal to the corresponding field in R_y.

[1094] "A Boolean expression is an expression that evaluates to a value of the Boolean Data Type: True or False. Boolean expressions can take several forms. The simplest is the direct comparison of the value of a Boolean variable to a Boolean literal" (e.g. If *loginData = True* Then redirect to account); msdn Microsoft Library, Boolean Expressions (Visual Basic), available online at: http://msdn.microsoft.com/en-us/library/dya2szfk.aspx.
[1095] Packet of data refers to data seized and submitted by the MIA tool and requests made by officers.

Definition 5 — Rules R_x and R_y are correlated if some fields in R_x are subsets or equal to the corresponding fields in R_y, and the rest of the fields in R_x are supersets of the corresponding fields in R_y.

These basic functions of the SPoC system highlight the need for clear and non-ambiguous rules for the policy. It has been highlighted in previous chapters however,[1096] that legal rules and regulations are particularly prone to ambiguities and problems with interpretation. In addition, the vast number of various authorities (national and international) and (software and hardware) platforms involved in the investigation of the virtual living space can cause difficulties relating to translation of the rules and thus result in misunderstandings and malfunctioning of both, the SPoC system and the MIA tool.
The result, often, is that valuable semantics can be lost in the exchange, which degrades the efficiency of the decision-making mechanism. It is therefore crucial to find the best approach for the translation of those rules, which adequately translates the rules into formal, machine-readable language and ensures that no information gets lost or misinterpreted.
Important is in particular that common logical definitions, which constrain possible interpretations of any given concept to a finite set are agreed upon before communication can occur.

A syntactic approach to the concept of information exchange between the SPoC system, the MIA tool and the authorities simplifies the creation and implementation of rules, and is therefore the best suited approach for the translation of the rules in the policy. The focus of syntactic systems is not simply on the interpretation of data but mainly on deeper reasoning and an attempt at the computer analysis and understanding of the data.[1097] This is relevant for the SPoC system because it needs to be capable of reasoning about the data delivered by the MIA tool to properly classify and match it with data access requests from authorities, or formulate commands for the MIA tool (such as stop all investigative actions in case of cross-border activities).

[1096] See particularly p. 285ff.
[1097] L Ogiela, "Syntactic Approach to Cognitive Interpretation of Medical Patterns" in C Xiong et al. (eds) *Intelligent Robotics and Applications: First International Conference, ICIRA 2008* (Berlin, Heidelberg: Springer, 2008) 456-462, 457.

Generally, the system attempts to capture syntactic characteristics of the machine-level byte sequence of the incoming data, and matches and then classifies it with existing syntactic rules.[1098] Thus, in essence it is a translation of queries between heterogeneous sources. Syntactic rules are used to map selection predicates from one database to that of another.[1099]

Figure 3 below outlines the syntax of the rule request and of the policy rule, which provide a close match to each other. Most of the fields within these rules are defined within, and generated from, the relevant legislation, but the [Subject] field is kept as a free format field, so that the structure of the databases within the domain does not have to be exposed to other domains. All of the other fields within the rules are thus used to match the request.

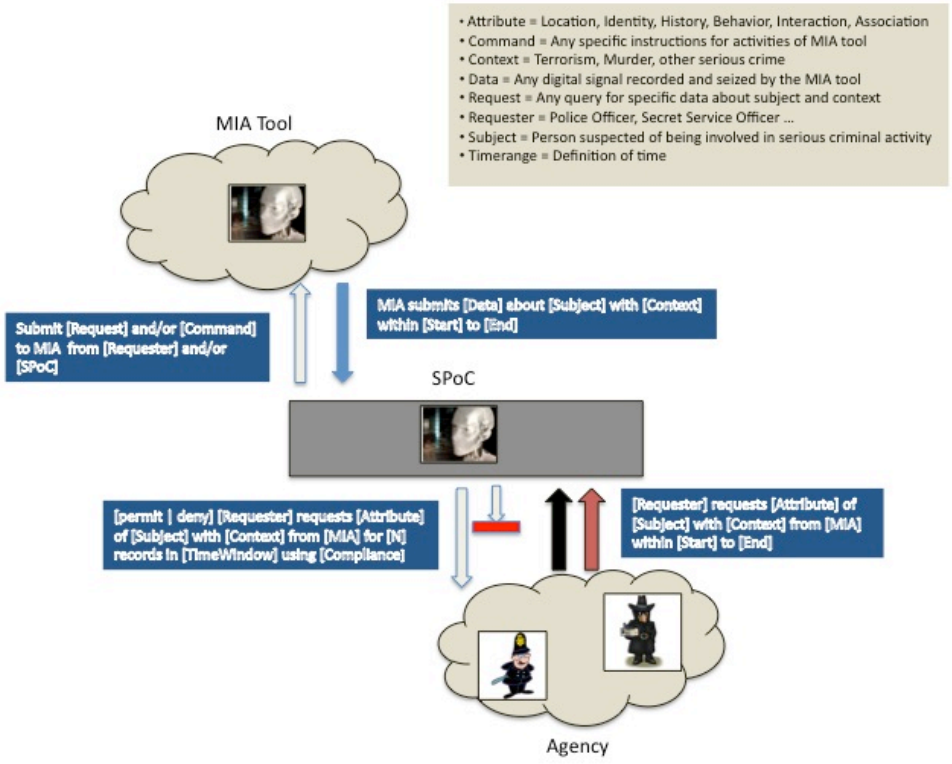

Figure 3: Overview of the request and policy implementation syntax

[1098] M Dalla Preda et al., "A Semantics-based Approach to Malware Detection" (2007) *Proceedings of the 34th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, 377-388, 377.

[1099] A Kementsietsidis, "Data Sharing and Querying for Peer-to-Peer Data Management Systems" in W Lindner et al. (eds) *Current Trends in Database Technology – EDBT 2004 Workshops* (Berlin, Heidelberg: Springer, 2004) 177-186, 181.

Adding key security elements to this structure yields the proposed syntax for policy rules, which are implemented into the SPoC:

1. For communication with the operating agency:

    [permit | deny] [Requester] requests [Attribute] of [Subject] with [Context] from [MIA] for [N] records in [TimeWindow] using [Compliance]

2. For communication with the MIA tool:

    Submit [Request] and/or [Command] to MIA from [Requester] and/or [SPoC]

A similar matching syntax can then be applied to the request messages:

    [Requester] requests [Attribute] of [Subject] with [Context] from [MIA] within [Start] to [End]

And to submission messages from the MIA tool:

    MIA submits [Data] about [Subject] with [Context] within [Start] to [End]

Elements of this syntax are defined as:

- **[permit | deny]:** This part of the rule syntax indicates the action of the rule and defines whether a message meeting the rule criteria will be permitted or denied.
- **Requester:** This identifies an exposed role defined in applicable legislation and regulations. For example, this role might be a Detective Constable (DETCST) in the Police Services (POL) domain, a Judge (JGE) in the Judicial services (JUD) domain, or a Secret Service Agent (SSA) in the Law Enforcement Services (LES) domain.
- **Subject:** This refers to any person suspected of being involved in serious criminal activities. It is a free-form field.
- **Data:** Any digital signal recorded and seized from ICT devices of suspects during investigative actions by the MIA tool.
- **Attribute:** This is a unit of information describing an object. Attributes may include details about location (address, mobile phone tracking), identity (name, insurance number), history (prior convictions, documented allegations), behavior (calm, violent) and association (group memberships, known associates).

- **Context:** This identifies the reason why data is being seized and shared. The context also governs the level of access and permissions associated with information exchange and, hence, affects the priority accorded to information requests. For example, a terrorism investigation poses a potential threat to life and will require a higher priority allocation than a vandalism context.
- **[N]** records in **[TimeWindow]** This is a part of the rule syntax that defines the number of records permitted over a period of time, where [N] can be any positive integer, and[TimeWindow] uses the ISO 8601 Coordinated Universal Time (UTC) format (YYYY-MM-DD). In practice, it prevents fishing expeditions
- **[Compliance]:** This is part of the rule syntax that refers to policies and legislative requirements that affect the exchange of information. Such as the Data Protection Act, the Human Rights Act, the Freedom of Information Act, and so on.
- **[Start]:** This is part of the request that identifies the start of the date/time period over which sharing is requested, such as for ISO 8601 (UTC) standard.
- **[End]:** This is part of the request that identifies the end of the date/time period over which sharing is requested.

9.2.2 Context Information

A key feature in the proposed system is the use of context information for a request. Here the relevant regulations and laws define access rights based on the context of the request. For example, the access rights to data are stricter within the context of a terrorism investigation than for a vandalism investigation. Equally, the seriousness of a crime to be investigated determines the amount of core private data transmitted to authorised officers.[1100]

It is therefore important that the context levels and associated rights are clearly defined. Hence, context information about the seriousness of the suspected criminal activity is animportant factor for the classification of a request.

Generally, determining crime seriousness is a complex issue, and one that cannot be discussed here in its entirety. On a basic level, "two conceptual issues exist in crime seriousness research: the meaning of seriousness and the representation of crimes."[1101]

[1100] See above p. 306 for a more detailed explanation of this.

[1101] Y K Kwan, L L Chiu, W C Ip, "Measuring Crimes Seriousness Perceptions: Methods and Demonstration" in K T Froeling (ed) *Criminology Research Focus* (New York: Nova Science Publishers, Inc, 2007) 7-19, 8.

A standard definition of seriousness does not exist, however, Rossi et al. find that participants of relevant experiments understand the concept of seriousness without any difficulty.[1102]

Based on the use of MIA tools, the codified, and hence highly conceptual, German Criminal Law proffers itself as a basis for a conceptual hierarchy of seriousness. While this hierarchy is tailored to the German legal system, this does not mean that it is inapplicable to other legal systems. In fact, the hierarchy of the German system can be detected in common-law systems, too, albeit not in codified form. For example, murder[1103] is classified as more serious than manslaughter[1104] in both the German (codified) system, as well as the UK system.

In addition to this hierarchical classification of seriousness of crimes, a proxy to weight severity within a category (e.g. murder vs. manslaughter as "offences against the life") by the minimum punishment that the crimes carry should be adopted.[1105]

This additional context element serves as a further guarantee that privacy and data protection rights, sovereignty and evidence principles are adhered to. It can be regarded as an enabler for the SPoC system to better "understand" and thus classify requests from both, the relevant agency and the MIA tool.

9.2.3 Documentation

The above-discussed features of the proposed syntax and incorporated SPoC system are crucial to ensure that robustness and reliability of the technical components of the soft MIA law notion are maintained. However, the mere promise of a technical ability of the syntax is insufficient to ensure legally binding reliability and thus legal certainty of the approach and the data seized during online searches. It is therefore crucial that the syntax is capable of creating legally binding documentation about all requests submitted, and its reasoning process and decisions.

This also ensures that any abuse of the system (e.g. labelling a minor offence as a terrorism suspicion) can be traced.

Creating such documentation is relatively straightforward, and thus easily incorporated into the syntax. In fact, most operating systems already automatically

---

[1102] P H Rossi, E Waite, C E Bose, R E Berk, "The Seriousness of Crimes: Normative Structure and Individual Differences" (1974) 39:2 *American Sociology Review*, 224-237.

[1103] Murder is regulated by §211 German Penal Code.

[1104] Manslaughter is regulated by §212 German Penal Code. Thus in the same section, "offences against the life", but in hierarchical order.

[1105] See Kwan/Chiu/Ip, note 1101, for an analysis of such a proxy solution.

create records of all computer activity. Microsoft Windows, for example, features an application called "Security Log", which is a log that contains records of login/logout activity and other security-related events specified by the system's audit policy.[1106] In addition, free software programs and web tools are available that enable users to record all computer activity including the websites visited, the applications run on the computer etc.[1107]

Thus the technology to create such documentation and records is commercially available, and therefore sufficiently robust and reliable. Implementing such an application into the syntax is therefore technically feasible and provides the necessary documentation to ensure that the use of the syntax produces legally binding results.

9.3 Conclusion

The proposed soft MIA law provides a solution to the current technical challenges and problems of incorporating explicit legal reasoning capacities into MIA tools. It serves as an intermediary between the MIA tool and the relevant authorities. It complements the key features (mobility, intelligence and autonomy) of the MIA tool by ensuring that relevant regulations, principles and rights, such as privacy and data protection rights of suspects, as well as best evidence principles and sovereignty rights of affected states, and applicable legislation, such as evidence laws and criminal procedure laws are adhered to.
Due to the static nature of the syntax as opposed to the fluctuant nature of the MIA tool compliance with these regulations, principles, rights and laws is technically realisable. As discussed above, the MIA tool would suffer from a lack of robustness and reliability if explicit legal reasoning capacities that are required for the strong MIA law notion were implemented at this stage. This would mean that MIA tools would have no or only very limited legal value.

The proposed soft MIA law notion, based on the suggested syntax offers the required level of robustness and reliability, and thus provides a unique solution to the strong MIA law notion developed in the previous chapter.

[1106] R F Smith, The Windows Security Log Encyclopedia (North Charleston, SC: Booksurge Llc, 2007).
[1107] See for a list of such programs and a discussion of these, http://www.labnol.org/software/organize/record-computer-usage-online-activity/3817/.

The SPoC agents incorporated into the syntax ensure compliance with legislation and domain policies, and ensure that only valid requests for data sharing and permissible information are transmitted between the MIA tool and the authorities.
Ultimately, the interaction between the MIA tool and the syntax should ensure that a) only data protection compliant information is transmitted, b) records of all requests and activities are created to ensure that sufficient documentation is available and abuse can be traced, and c) offer a robust and reliable enough solution to produce legally valid data and results.
For this it is necessary to prove abstractly that only law compliant interactions are permitted by the system. For this purpose in particular, incorporating an explicit representation of legal concepts along the lines of Sartor et al.,[1108] as discussed and shown above, is particularly promising.

However, the soft MIA law notion has disadvantages caused by its static syntax. While this static syntax on the one hand facilitates the development of a technically feasible governance approach for MIA tools, it hinders MIA tools to reach their full potential during investigations on the other hand.
The syntax is a separate software layer, which needs to be installed on all computers used to operate the MIA tools. This requirement constrains the flexible use of MIA tools during investigations and restricts their use to agencies and operators with the relevant software in place.
The syntax also adds another step to the investigative process, which is potentially time-consuming depending on the required amount of communication between the SPoC system, MIA tool and the requesting agency, and the amount of legal reasoning the SPoC system needs to undertake. As discussed above,[1109] time can be a crucial factor for investigations of the virtual living space. Data can be shifted within seconds to external storage media.
Furthermore, MIA tools are designed to operate as autonomous entities, or cyber-cops, during investigations. Their real potential lies in the fact that these tools are not dependent on operator commands, and have the potential to govern and regulate their own actions. This makes them so predestined for the investigation of the virtual living space, which is difficult to govern from the physical world by human officers alone.

[1108] See Sartor, note 1002.
[1109] See chapter 6, p. 170ff.

Hence the strong MIA law notion developed in the previous chapter is the preferable long-term approach. However, given the highly intrusive nature of MIA tool actions and the potential for rights violations, the relevant techniques required to implement the strong MIA law notion need to be reliable before this approach can be realised.

For the interim period, the soft MIA law notion offers an ideal solution for the governance problems of MIA tools. As highlighted by the empirical research results the most pressing problem of practitioners is the lack of adequate regulatory instruments for the new generation of cyber-cops. Given the constitutional relevance of the virtual living space, and the inability of the existing legal framework to ensure law-compliant use of MIA tools, the soft MIA law notion is an important contribution to solve these problems.

10 CONCLUSION

The aim of this thesis has been to develop a sustainable regulatory model for software-based investigative tools deployed for the policing of the virtual living space by law enforcement and secret services. In recognition of the ever increasing reliance on ICTs and the growing importance of the virtual living space for people, I argue that a solution needs to be developed while these technologies are still in its infancy, to avoid rushed and ill-drafted legislation, as well as illegitimate use of investigative powers.

Looking back at past technology regulation, the preferred methodology of legal practitioners is either to reason by analogy from traditional legal concepts to new, technology-based phenomena, or to "black box" the entire process, categorise it as a purely technical issue and to put their trust in the computer forensics experts. This thesis has argued that neither approach is satisfactory when it comes to the deployment of autonomously operating software by the state.

"Black boxing" circumvents potentially necessary legal safeguards put in place to protect citizens. In this case a technocratic discourse supplements necessary political debates that are to be had about civil rights. It also can result, as was argued in chapter 7, in a degree of blind trust that prevents lawyers from evaluating the strength and reliability of the evidence in a sufficiently open, accountable, and reliable way.

Reasoning by analogy by contrast is a necessary and crucial instrument of lawyers. Any regulation that tries to be so detailed as to prevent it altogether is, as argued above, likely to have very limited shelf life, as with necessity it has to be very specific to the technology that is regulated. Even though some respondents to the interviews felt deeply uneasy with using analogical reasoning in the field of computer forensic evidence, this thesis argues that the problem is mainly due to their insecurity with the technology – they do not know if the analogies are valid.

However, this approach is indeed much more likely to fail when:

- the difference between the traditional, real world, and the new, digital counterpart is wide, and
- when in addition inevitable security concerns have to hide some of the technical features from open debate, and
- the specific field of law is structured adversarial, through irreconcilable conflicts between parties.

The solution to which this thesis hopes to contribute does not try to prevent analogous reasoning, but rather wants to prepare the conditions to enable it. Regarding point a) above, it did so by analysing the pertinent features of the technology and their legal relevance. Looking at c), in the first chapter this thesis took note of the parallel debate regarding autonomous agents for commercial applications. There too, the academic debate had initially suggested far reaching analogies that in some cases would have given the software the status of a legal person. We can see here how strong our tendency to anthropomorphise autonomously operating software code is. The emerging consensus in that discussion however seems to be that much less radical analogies are necessary, and that very simple equivalents between offline and online behaviour can be found. However, I argue that this was enabled by the convergence of interests in the private law setting – ultimately, it is in nobody's interest to prevent valid contract formation due to formalistic worries about the concept of "acceptance" or "intent" in agent negotiated transactions.

This, however, is radically different in criminal law settings, where the asymmetric distribution of power means that the interests of the state and that of suspects are less likely to be reconcilable easily. In such an environment, regulation through markets is bound to fail. Here, our tendency to anthropomorphise software code, to think of them not just metaphorically as cyber-cops, but to use this as a hook to enable legal argumentation about the respective rights and duties of citizens vis-à-vis that technology, is something we may need to exploit. This is reflected by the current policy system, which is premised on legislation rooted deeply in legal concepts tailored to the analogue world. The thesis therefore tried a three-pronged approach:

- increase our understanding of the technology and match its features to legal problems,
- show how we can "make the metaphor real", by embedding directly into the software code features that mimic reasoning of real, biological police officers,
- highlight where even this will still leave conceptual gaps between technological reality and the legal metaphors that may be in need for formal legislation, but on a suitably abstract level

Taken together, these measures should help lawyers to reason about the legal issues raised by the use of autonomously operating software tools in investigations more confidently, but also more accurately.

Deeper technological knowledge is therefore essential for the development of a regulatory model for software-based investigative tools. This thesis brought together in an interdisciplinary approach insights and findings from law, computer science, and artificial intelligence. This interdisciplinary approach has guaranteed that the research in this thesis is well grounded.

10.1 Research Goals and Answers Developed

This interdisciplinary approach was also reflected in the structure of this thesis. Chapters 4 and 5 constituted the technical foundation of this work and addressed the first research goal of this thesis, to develop a generic concept of current and future software-based investigative tools that identified the family of legal issues that every technology in this class will inevitably face.

In chapter 4 I determined in detail the technical specifics of the software tool of the case study of this thesis: the online searching of ICTs. This has so far been neglected in existing research on the topic. It was established that this comparatively task-oriented and simple technology already exhibits all the regulatory problems that also much more intelligent future tools will also face.

I argued in chapter 5 that to enable future-proof regulation of cyber-cops, the policy system needs to move away from the currently deployed approach of regulating single technologies. Instead, regulation needs to focus on classes of technology that share key concepts and attributes. Based on this finding, I developed a new category of software-based investigative technologies – mobile, intelligent, and autonomous (MIA) policing tools. The development of this class is a significant contribution to existing research, and can facilitate future policy making on this topic.

Chapters 6 and 7 formed the legal foundation of this thesis. These chapters addressed the second research goal of this PhD project, the evaluation of the existing legal framework regulating police investigations in the light of MIA policing tools. This part is influenced by the empirical research results and the focus was on those topics identified as most pressing by the legal experts involved in the use of current MIA tools. In chapter 6, I analysed the problems of cross-jurisdictional investigations by MIA tools for traditional concepts of sovereignty and territoriality. In chapter 7, I examined the problems of digital data as evidence, and particularly the “double digital paradigm”, i.e.

digital evidence seized from live systems by software tools, and the problems this causes for traditional evidence concepts and the admissibility of this evidence for court proceedings.
The analysis in these chapters evidenced that reasoning by analogy is difficult, and often unsuccessful for these specific legal issues. In answering the overarching question of this thesis, whether existing legislation is sufficient to regulate the use of MIA policing tools, these chapters found that existing legislation is limited to deal with the new class of software tools, and a new regulatory model is required.

Chapters 8 and 9 addressed the third research goal of this thesis, and developed the outline of a novel regulatory model for the governance of MIA policing tools. The proposed regulatory model is a direct result of the interdisciplinary research approach. Building on existing research in the field of technology regulation, and particularly the notion of "code is law" by Lessig, and research into computational legal reasoning, in chapter 8 I developed a model of MIA law. This strong MIA law notion proposes the implementation of legal reasoning capabilities into the software code of MIA tools to design law-abiding software. This ensures that on the one hand, these software tools are likely to perform in a law abiding way, moving away from the traditional rule of law to address rule violations and to ensure compliance as a design feature. At the same time, this approach gives traction to traditional legal reasoning skills and makes it easier to bring these technologies under the existing conceptual framework. This strong MIA law notion relies on state-of-the-art research, which makes this model timely, but also causes problems for its instant implementation.
In chapter 9 I therefore developed a soft MIA law model, which addresses the current implementation problems of the strong MIA law notion. It still relies on legal reasoning capacities of software tools, but by introducing a static syntax, distributes the responsibility for the legal reasoning process. This model relies on established research, and as a result, is robust and therefore reliable.

Although the implementation of a MIA law model (strong and soft) would be a novel development for regulators, I believe that this is a necessary step for the adequate regulation of these intelligent and autonomously operating policing tools. This regulatory approach reflects and addresses the current problems of those directly involved in the use of these tools, and legal practitioners in general. I further believe that an implementation of the soft MIA law model into the current, comparatively

simple tools is essential to facilitate a future implementation of a strong MIA law notion into more sophisticated and complex MIA policing tools.

10.3 Future Work

A novel research topic always prompts a mirage of issues that are interesting and crucial. This one is no different. There are, however, limitations to what can be discussed in a PhD thesis.

The selection of topics in this thesis was influenced by the empirical research results to ensure that this work in addition to the pure academic value also has a practical value for those stakeholders directly involved in the use of MIA tools. This has meant that some issues could only be mentioned but not fully elaborated in this work.

Particularly, the point of legal status of intelligent and autonomous software that replaces human beings for crucial policing duties is one that deserves more scrutiny in the future. I argue in this thesis that in the future, much more intelligent and autonomously operating cyber-cops will execute core policing tasks of the virtual living space. This means that the actions and their consequences of these software tools will not be distinguishable to those of human police officers. Hence, rights and duties, usually reserved for a specifically educated group of people, will be conferred to these software tools. How the law can and should deal with this situation is a question that needs to be addressed in future research. What the thesis had largely to ignore, regrettably, are therefore the wider ethical and jurisprudential implications of the solution suggested here.

It is as a result "conservative" in two ways: Firstly, it tries to ensure that our existing framework regulating police activities and providing the necessary protection for suspects, continues to work in the new, digital age, without depriving unnecessarily the police of needed tools. That assumes of course that the regulation of traditional, offline police work is adequate. Maybe we get the balance wrong already, and any attempt to project our present approach to regulate police activity into cyberspace is therefore the continuation of a failed approach. Secondly, it also takes for granted that we can remove the personal element of police work without a serious loss of "quality" of the human interaction. Being questioned by a physical police officer can be intimidating and worrying. But at least one interacts with another human being, can plead, scream or complain about him. To interact instead with a machine may look superficially attractive, as it removes some of the threatening physicality from the interaction – who

really wants a squad of coppers going through one's living room? But by reducing a police officer to his legal function (and only that is what even the most ambitious software programs can aim at), we may also diminish further the humanity of the interaction. In this new world, the "officer" and we are quite literally only a number. Whether this is desirable would require a different study with different tools. The only thing this thesis could hope to accomplish is to ground this debate in what is technologically possible.

10.4 Closing Remarks

In this thesis I developed a regulatory model for a newly defined class of software-based investigative tools.

This "code-based" model is a result of the interdisciplinary nature of this thesis. The empirical research has shown that the introduction of ever more intelligent and autonomously operating investigative software tools requires ongoing collaboration between the different relevant disciplines and practitioners. This ensures that early stage research is developed with practical issues and problems in mind, and the different disciplines can voice their respective needs.

I hope that this thesis serves as an incentive for future collaboration on this topic.

BIBLIOGRAPHY

Note: all weblinks were accurate when last visited between 25 and 30 August 2012.

Legislation and instruments (in chronological order by country)

Germany

Strafprozessordnung 1877

Grundgesetz für die Bundesrepublik Deutschland 1949

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses 1968

Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei 1990

Polizei- und Ordnungsbehördengesetz – POG Rheinland-Pfalz 1993

Gesetz über den Verfassungsschutz in Nordrhein-Westfalen 1994

Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten 1997

Gesetz zur Bekämpfung des internationalen Terrorismus 2002

Landtagsdrucksache – LTDrucks 14/2211 03.07.2006

Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen 2010

European Community

The Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950

The European Convention on Mutual Assistance in Criminal Matters (CETS No. 030) 1959

The Europol Convention

Council of Europe Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology 1995

Council of Europe Convention on Cybercrime 2001

United Kingdom

Police and Criminal Evidence Act 1984

Criminal Justice Act 1988

Computer Misuse Act 1990

Criminal Justice and Public Order Act 1994

EC telecommunications framework 1998

Human Rights Act 1998

Regulation of Investigatory Powers Act 2000

Anti-Terrorism, Crime and Security Act 2001

E-communications framework 2003

UK Criminal Justice Act 2003

Prevention of Terrorism Act 2005

Terrorism Act 2006

Digital Economy Act 2010

United Nations

United Nations Charter 1945 59 Stat. 1031, T.S. 993, 3 Bevans 1153

United States

USA Patriot Act 2002

Treaties, Declarations, Resolutions and Proposals

Treaty with the Swiss Confederation on Mutual Assistance in Criminal Matters, Senate Executive Report 94-29, 94th Cong, 2d Sess 1 (1976)

Treaty on Mutual Assistance in Criminal Matters, US-Switzerland, 27 UST 2019, TIAS No 8302 (1977)

Council of the European Union, 'Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime', 2987th Justice and Home Affairs Council meeting, 27 – 28 November 2008, available at http://www.ue2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf

European Commission, "Proposal for a Directive on Attacks against Information Systems, repealing the Framework Decision 2005/222/JHA, 30 September 2010, available online at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463&format=HTML&aged=0&language=EN&guiLanguage=en

Cases (by country in alphabetical order)

Australia

Trimcoll Pty Ltd v Deputy Commissioner of Taxation [2007] NSWCA 307

Belgium

X (Belgian Citizen) v Swiss Fed. Prosecutor's OFfuce, 10 EuGRZ 435 (Judgment of 15 July 1982) (Swiss Federal Tribunal, Lausanne, P1201/81/fs 1983)

France

LICRA v *Yahoo! Inc and Yahoo France* (Tribunal de Grande Instance de Paris, 22 May 2000)

LICRA and UEJF v *Yahoo! Inc and Yahoo France* (Tribunal de Grande Instance de Paris, 20 November 2000)

Germany

BGH, Beschluss vom 21.02.2006 – Az. 3 BGs 31/2006, http://www.hrr-strafrecht.de/hrr/3/06/3-bgs-31-06.php

BGH, Beschluss vom 25.11.2006 - Az. 1 BGs 184/2006, http://medien-internet-und-recht.de/volltext.php?mir_dok_id=486

BGH, 17.08.2011 - I ZR 57/09

BGH, NJW 2005, 1442

BGH, NJW 2007, 930

BGHSt NJW 1960, 1582

BGHSt, 18, 51

BVerfGE, 113, 29

BVerfGE NJW 1971, 2299

BVerfGE NJW 1973, 747

BVerfGE NJW 1984, 419

BVerfGE NJW 1985, 121

BVerfGE NJW, 1991, 2411

BVerfGE NJW 1992, 1875

BVerfGE NJW 1993, 2035

BVerfGE NJW 2001, 1121

BVerfGE, NJW 2002, 3619

BVerfGE NJW 2003, 1787

BVerfGE, NJW 2004, 999

BVerfGE NJW 2005, 2603

BVerfG, NJW 2008, 822

OLG Celle, NJW 1976, 2030

Italy

Romano, 706F.2d370 (2d Cir. 1983)

Jurisdictions of the United Kingdom

Al Amoudi v Brisard and JCB Consulting International SARL [2006] EWHC 1062 (QB)

Bobo v State, 2008 WL 2191159

Boyle v Wiseman (1855) 11 Ex. 360

Dow Jones v Jameel, [2005] EWCA Civ 75

DPP v Kilbourne [1973] AC 729, 756

G and G v Wikimedia Foundation [2009] EWHC 3148 (QB)

Kajala v Noble [1982] 75 Cr App R 149

Masquerade Music Ltd v Springsteen; *Springsteen v Flute International Ldt; sub nom. Springsteen v Masquerade Music Ltd* [2001] EWCA Civ 563; [2001] C.P. Rep. 85; [2001] C.P.L.R. 369 [2001] E.M.L.R. 25, CA (Civ Div)

R v Chalkley [1998] QB 848, [1998] 2 All ER 155

R v Ciantar [2005] EWCA Crim 3559

R v Dallagher [2002] EWCA Crim 1903

R v Early [2002] EWCA Crim 1904

R v Emu [2004] EWCA Crim 2296

R v Fellows; R v Arnold [1997] 1 Cr App R 244; [1997] 2 All E.R. 548

R v Hartz [1967] AC 760, 785

R v Hodges [2003] EWCA Crim 290

R v Hoey [2007] NICC 49

R v Gilham [2009] EWCA Crim 2293, 173 CL & J 749

R v Grant [2005] EWCA Crim 1089, [2006] QB 60

R v Grimer [1982] Crim LR 674, 126 SJ 641

R v Guney [1998] 2 Cr App R 242, 265

R v Khan [1994] 4 All ER 426

R v P [2002] 1 AC 146; *Attorney-General's Reference (No. 3 of 1999)* [20011 2 AC 91

R v Robb [1991] 93 Cr App R 161

R v Robson [1972] 1 WLR 651

R v Saward [2005] EWCA Crim 318

R v Skinner [2005] EWCA Crim 1439

R v Stevens [2002] All ER (D) 34 (Jun)

R v Stubbs [2002] EWCA Crim 2254

R v Thomas (Stephen) [1986] Crim LR 682

R v Tolson (1864) 4 F & F 103, 176 ER 488

R v Walsh (1989) 91 Cr App R 161 at 163, CA and *R v Ryan* [1992] Crim LR 187, CA

R v Wood [1983] 76 Cr App R 23

Teper v R [1952] AC 480, 486

United States

Daubert v Merrell Dow Pharmaceuticals 509 US 579

Frye v United States 293 F 1013

United States v Aluminium Co of America (1945) 148 F 28 147

United States v Alvarez-Machain, 946 F.2d 1466 (9th Cir. 1991), rev'd, 112 S. Ct. 2188 (1992)

United States v Gorshkov, 2001 WL 1024026

United States v Ivanov, 175 F. Supp. 2d 367

Yahoo! Inc. v LICRA and UEJF, 145 F Supp 2d 1168

Yahoo! Inc. v LICRA and UEJF, 169 F Supp 2d 1181

Yahoo! Inc. v LICRA and UEJF, 379 F 3d 1120

Yahoo! Inc. v LICRA and UEJF, 433 F 3d 1199

LICRA v Yahoo! Inc., 126 S.Ct 2332 (Mem)

Articles

Abel, W, Schafer, B, “Big Browser Manning the Thin Blue Line - Computational Legal Theory Meets Law Enforcement” (2008) 2 *Problema*, 51

Abel, W, Schafer, B, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822", (2009) 6:1 *SCRIPTed* 106 – 123

Adams, W, “Machine Consciousness: Plausible Idea or Semantic Distortion?” (2004) 11:9 *Journal of Conscious Studies*, 46-56

Adelstein, F, “Live Forensics: Diagnosing Your System Without Killing it First” (2006) 49:2 *Communications of the ACM*, 63

Ahlert, C, "Technology of Control: How Code Controls Communication" (2003) in Organization for Security and Co-operation in Europe (OSCE), *Spreading the Word on the Internet*, 119

Al-Kofahi, K, Grom, B, Jackson, P, "Anaphora resolution in the extraction of treatment history language from court opinions by partial parsing" (1999) *International Conference on Artificial Intelligence and Law '99*, 138-146

Al-Shaer, E S, Hamed, H H, "Modeling and Management of Firewall Policies" (2004) *IEEE Transactions on Network and Service Management*, 2-10

Albus, J S, "Outline for a Theory of Intelligence" (1991) 21:3 *IEEE Transactions on Systems, Man, and Cybernetics*, 473-509

Albus, J S, "The Engineering of Mind" (1999) 117 *Information Science*, 3

Ali, S, et al., "Definition of a Robustness Metric for Resource Allocation" (2003) *Proceedings of the 17th International Symposium on Parallel and Distributed Processing*, 42

Allan, J, "To Exclude or Not to Exclude Improperly Obtained Evidence: Is a Humean Approach More Helpful?" (1999) 18 *University of Tasmania Law Review,* 263

Allen, C J W, "Discretion and Security: Excluding Evidence Under Section 78(1) of the Police and Criminal Evidence Act 1984" (1990) *Cambridge Law Journal,* 80

Anderson, A R, "The Logic of Hohfeldian Propositions" (1971-72) 33 *University of Pittsburgh Law Review*, 29

Anderson, R J, Kuhn, M G, "Soft Tempest – An Opportunity for NATO" (1999) *Protecting NATO Information Systems in the 21 Century, IST Symposium, Washington DC, USA, 25–27 Oct*, available online at http://www.cl.cam.ac.uk/~rja14/Papers/nato-tempest.pdf

Arco, A, "Police Monitor Internet for Threats Against the Pope During his Visit" (2010) *Catholic Herald*, available online at http://www.catholicherald.co.uk/news/2010/07/21/police-are-monitoring-internet-for-threats-against-the-pope/

Armbrust, M, et al., "A View of Cloud Computing" (2010) 53:4 *Communications of the ACM*, 50-58

Ashworth, A J, "Excluding Evidence As Protecting Rights" (1977) *Criminal Law Review,* 723

Attfield, P, "United States v Gorshkov: Detailed Forensics and Case Study; Expert Witness Perspsective" (2005) *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering* (SSADFE'05), 3

Backes, M, Dürmuth, M, Unruh, D "Compromising Reflections – or – How to Read LCD Monitors Around the Corner" (2008) *Proceedings IEEE Symposium on Security and Privacy*, 158-169

Bain, M, Subirana, B, "Towards legal programming: the incorporation of legal criteria in software agent design – Current proposals and future prospects" (2004) 20:1 *Computer Law & Security Report*, 44-52

Balganesh, S, "Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass" (2006) 12 *Michigan Telecommunications and Technology Law Review*, 265

Barbuceanu, M, Gray, T, Mankovski, S, "The Role of Obligations in Multiagent Coordination" (1999) 13:1-2 *Applied Artificial Intelligence*, 11-38

Barlow, J P, "A Declaration of the Independence of Cyberspace" (1996) available online at http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration

Barnes, S J, "The Mobile Commerce Value Chain: Anlysis and Future Developments" (2002) 22:2 *International Journal of Information Management*, 91-108

BBC News, "BT and TalkTalk to Appeal Digital Economy Act" (2011) available online at: http://www.bbc.co.uk/news/technology-15212651

Beaumont, P, "The Truth about Twitter, Facebook and the Uprisings in the Arab World" *Guardian*, 25 February 2011, online at: http://www.guardian.co.uk/world/2011/feb/25/twitter-facebook-uprisings-arab-libya

Bechtel, W, "Connectionism and The Philosophy of the Mind: An Overview" (1987) *The Southern Journal of Philosophy*, Supplement, 17-41

Becker, J, "Rechtsrahmen für Public Private Partnerships" (2002) *Zeitschrift für Rechtspolitik*, 303-308

Bellia, P L, "Chasing Bits Across Borders" (2001) 35 *University of Chicago Legal Forum*, 80

Berlit, S, Wegewitz, T, "Mythos „Bundestrojaner" - Auf dem Weg zur legalen Onlineüberwachung – ", (2008) *1. Workshop IT-Sicherheitsmanagement*, available online at http://wi.f4.htw-berlin.de/users/messer/LV/Globals/ISM-Workshops/Workshop-WS07/Mythos%20Bundestrojaner%200.pdf

Berners-Lee, T, "The World Wide Web – Past, Present and Future" (1997) 1:1 *Journal of Digital Information*, available online at: https://journals.tdl.org/jodi/article/viewArticle/3/3

Biagioli, C, et al., "Automatic Semantics Extraction in Law Documents" (2005) *Proceedings of the International Conference on Artificial Intelligence and Law '05*, 6

Blair, "What is a Backdoor Trojan" (2007) *Geeks to Go*, available online at http://www.geekstogo.com/2007/10/03/what-is-a-backdoor-trojan/

Bleich, H, "Staatstrojaner: Mehr als 50 Einsätze bundesweit" heise, 16.10.2011, available online at http://heise.de/-1361857

Boella, G, Torre, L van der, "Regulative and Constitutive Norms in Normative Multiagent Systems" (2004) *Proceedings of 9th International Conference on the Principles of Knowledge Representation and Reasoning*, 255-265

Boella, G, Torre, L van der, Verhagen, H, "Introduction to Normative Multiagent Systems" (2006) 12 *Computational and Mathematical Organization Theory*, 71

Bradwell, P, "Judicial Review of the Digital Economy Act" (2011) European Digital Rights, available online at: http://www.edri.org/edrigram/number9.7/judicial-review-digital-economy-bill

Brazier, F, Kubbe, O, Oskamp, A, Wijngaards, N, "Are Law-Abiding Agents Realistic?" (2002) *Proceedings of the workshop on the Law of Electronic Agents (LEA02)*, 151-155

Brenner, S, "'Our'" Fourth Amendment", *CYB3RCRIM3*, 11.03.2006, available online at http://cyb3rcrim3.blogspot.com/2006/03/our-fourth-amendment.html

Briegleb, V, "30 Planstellen für den Staatstrojaner" (2012) *heise*, available online at: http://heise.de/-1414154

Brin S, Page L, "The Anatomy of a Large-Scale Hypertextual Web Search Engine", (1998) 30(1) *Computer Networks and ISDN Systems* 107

Brooks, R A, "Intelligence Without Representation" (1991) 47 *Artificial Intelligence*, 139-159

Brown, I, Korff, D, "Terrorism and the Proportionality of Internet Surveillance" (2009) 6:2 *European Journal of Criminology*, 119

Brownsword, R, "Code, Control, and Choice: Why East is East and West is West" (2005) 25:1 *Legal Studies*, 1

Brownsword, R, "Neither East Nor West, Is Mid-West Best?" (2006) 3:1 *SCRIPTed*, 15

Bruninghaus, S, Ashley, K D, "Improving the Representation of Legal Case Texts with Information Extraction Methods" (2001) *Proceedings of the International Conference on Artificial Intelligence and Law '01*, 42-51

Brunnstein, K, "From AntiVirus to AntiMalware Software and Beyond: Another Approach to the Protection of Customers from Dysfunctional System Behaviour" (1999) *Proceedings of the 22nd National Information Systems Security Conference*

Buermeyer, U, "Die 'Online-Durchsuchung' – Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme", (2007) 4 *Höchstrichterliche Rechtsprechung im Strafrecht* 154

Bundesministerium des Inneren, "Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien", 22.08.2007, available online at http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf

Bundesministerium des Inneren, "Fragenkatalog des Bundesministeriums der Justiz",22.08.2007, available online at http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf

Burgin, M, "Robustness of Information Systems and Technologies" (2009) *Proceedings of the 8th WSEAS International Conference on Data Networks, Communications, Computers*, 67

Burk, D L, "Jurisdiction in a World Without Borders" (1997) 1:3 *Virginia Journal of Law and Technology* 1522

Bush, J A, "How Did We Get Here? Foreign Abduction after Alvarez-Machain" (1993) 45:4 *Stanford Law Review*, 939

Buskirk, E van, Liu, V T, "Digital Evidence: Challenging the Presumption of Reliability" (2006) 1:1 *Journal of Digital Forensic Practice*, 19-26

Camp, L J, Syme, S, "Code as Governance, Governance of Code" (2001) *John F. Kennedy School Government Faculty Research Working Paper Series*

Chaos Computer Club, *Analyse einer Regierungs-Malware*, 08.10.2011, available online at: http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf

Calverley, D J, "Imagining a Non-Biological Machine as a Legal Person" (2008) 22 *Artificial Intelligence & Society*, 523-537

K M Carley, D S Kaufer, "Semantic Connectivity: An Approach for Analyzing Symbols in Semantic Networks" (1993) 3:3 *Communication Theory*, 183-213

Carrier, B, "Defining Digital Forensic Examination and Analysis Tool Using Abstraction Layers" (2003) 1:4 *International Journal of Digital Evidence*, 4

Carrier, B, Spafford, E, "Getting Physical with the Digital Investigation Process (2003) 2 *International Journal of Digital Evidence*, 1-20

Carrier, B, *"Risks* of live digital forensic analysis" (2006) 49:2 *Communications of the ACM*, 56

Case, A et al., "FACE: Automated digital evidence discovery and correlation" (2008) 5 *Digital Investigation* 65

Casey, E, Stanley, A, "Tool Review – Remote Forensic Preservation and Examination Tools" (2004) 1 *Digital Investigation*, 284

Castelfranchi, C, "Guarantees for Autonomy in Cognitive Agent Architecture" (1995) 890 *Intelligent Agents: Theories, Architectures, and Language*, 57

Castelfranchi, C, et al., "Deliberative Normative Agents: Principles and Architecture" (2000) 1757 *Intelligent Agents VI. Agent Theories Architectures, And Languages. Lecture Notes in Computer Science*, 364-378

Chaib-Draa, B, Dignum, F, "Trends in Agent Communication Language" (2002) 18:2 *Computational Intelligence*, 89-101

Chen H, Hsu, F, Li, J, Ristenpart, T, Su, Z, "Back to the Future: A Framework for Automatic Malware Removal and System Repair", (2006) *Proceedings 22nd Computer Security Application Conference* 257-268, 257

Chenwei, Z, "In Code, We Trust? Regulation and Emancipation in Cyberspace" (2004) 1:4 *SCRIPTed*, 585

Cohen, F, "Computer Viruses – Theory and Experiments" (1987) 6:1 *Computer Security*, 22-35

Collins, M, "Head-driven Statistical Models for Natural Language Parsing" (2003) 29:4 *Computational Linguistics*, 589-637

Colman, A, Han, J, "On the Autonomy of Software Entities and Modes of Organisation" (2005) *Proceedings of the 1st International Workshop on Coordination and Organisation* (CoOrg 2005)

Cook, D J, Augusto, J C, Jakkula, V R, "Ambient Intelligence: Technologies, applications, and opportunities" (2009) 5:4 *Pervasive and Mobile Computing*, 277

Cornelius, K, "Anmerkung zum Beschluss des BGH zur verdeckten Online-Durchsuchung", (2007) 62:15/16 *Juristenzeitung* 285-295

Dalla Preda, M, et al., "A Semantics-based Approach to Malware Detection" (2007) *Proceedings of the 34th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, 377-388

Daniels, J J, Rissland, E L, "Finding Legally Relevant Passages in Case Opinions" (1997) *Proceedings of the International Conference on Artificial Intelligence and Law '97*, 39-46

Dickey, K, "Tales of Trojan Horses – Why You Should Beware of Those Bearing Gifts" 9:2 *Smart Computing* 12-16

Deflem, M, "Bureaucratization and Social Control: Historical Foundations of International Police Cooperation" (2000) 34:3 *Law & Society Review*, 739-778

Deflem, M, "Europol and the Policing of International Terrorism: Counter-Terrorism in a Global Perspective" (2006) 23:3 *Justice Quarterly*, 336-359

Dellapenna, J W, "The Internet and Public International Law: Law in a Shrinking World: The Interaction of Science and Technology with International Law" (1999-2000) 88:4 *Kentucky Law Journal*, 809

Delic, K A, Dayal, U, "AI Re-Emerging as Research in Complex Systems" (2006) 7:38 *Ubiquity*

Dikaiakos, M D, Stassopoulou, A, Papageorgiou, L, "An investigation of web crawler behavior: characterization and metrics", (2005) 28:8 *Computer Communications*, 880–897

Doctorow, C, "Britain's New Internet Law -- As Bad as Everyone's Been Saying, And Worse. Much, Much Worse", (2009) *boingboing*, available at http://www.boingboing.net/2009/11/20/britains-new-interne.html

Dörges, T, "Why Protection against Viruses, Bots, and Worms is so hard- Malware seen as Mobile Agents" (2007) *PRESECURE Consulting GmbH*, 2 available online at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.4657&rep=rep1&type=pdf.

Doyle, E, "Not All Spyware is as Harmless as Cookies: Block it or Your Business Could Pay Dearly", (2003) *Computer Weekly*, available online at http://www.computerweekly.com/Articles/2003/11/26/198884/not-all-spyware-is-as-harmless-as-cookies.htm

Dreier, T, "Law and Information Technology – An Uneasy Marriage, Or Getting Along With Each Other?" (2005) 14:3 *Information & Communications Technology Law*, 207-216

Duncan, G, "China to Mandate Internet Filtering Software on PCs" (2009) *Digitaltrends*, available online at http://www.digitaltrends.com/international/china-to-mandate-internet-filtering-software-on-pcs/

Dunn, J E, "Israeli Police Uncover Massive, Trojan Horse-Based Industrial Spy Ring", (2005) *Techworld.com*, available online at http://www.pcworld.com/article/121081/israeli_police_uncover_massive_trojan_horsebased_industrial_spy_ring.html

Easterbrook, A H, "Cyberspace and the Law of the Horse" (1996) 207 *University of Chicago Legal Forum*, 209

Edwards, L, "The Changing Shape of Cyberlaw" (2004) 1:3 *SCRIPTed*, 363;

Edwards, L, "Mandy and Me: Some Thoughts on the Digital Economy Bill", (2009) 6:3 *SCRIPTed*, 534, available at http://www.law.ed.ac.uk/ahrc/script-ed/vol6-3/editorial.asp

Ellis, A, Pisani, R L, "The United States Treaties on Mutual Assistance in Criminal Matters: A Conparative Analysis" (1985) 19 *International Lawyer*, 189

Emert, M, "Münchener Koalition beschließt Änderungen beim 'Bayerntrojaner'" (2009) *heise*, available online at http://heise.de/-5939

Emm, D, "Focus on Trojans – holding data to ransom" (2006) 6 *Network Security*, 4-7

Engers, T M van, et al., "POWER: Using UML/OCL for Modelling Legislation – An Application Report" (2001) *Proceedings of the International Conference on Artificial Intelligence and Law '01*, 157-167

Escudero-Pascual, A, Hosein, I, "The Hazards of Technology-Neutral Policy: Questioning Lawful Access to Traffic Data" (2004) 47 *Communications of the ACM* 77-82

Eskridge, W N, "Public Values in Statutory Interpretation" (1989) 137:4 *University of Pennsylvania Law Review*, 1007

Etzioni, O, Levy, H M, Segal, R B, Thekkath, C A, "The Softbot Approach to OS Interfaces" (1995) 12:4 *IEEE Software*, 42-51

Etzioni, O, Weld, D S, "Intelligent agents on the internet: Fact, fiction and forecast", (1995) 12:4 *IEEE Expert* 41-51

Evers, J, "The future of malware: Trojan horses" (2006) CNETnews.com, available online at http://www.zdnetasia.com/news/security/0,39044215,61960021,00.htm

Farmer, D, Venema, W, "Forensic Computing Analysis: An Introduction" (2000) *Dr.Dobb's*, available online at: http://www.drdobbs.com/184404242;jsessionid=UUDPHDMG32RETQE1GHPSKH4ATMY32JVN

Federal Trade Commission, "Public workshop: monitoring software on your PC: spyware, adware, and other software" 2004, available online at: http://www.ftc.gov/bcp/workshops/spyware/extension.pdf

Ferber, J, Gutknecht, O, Michel, F, "From Agents to Organizations: an Organizational View of Multi-Agent Systems" in P Giorgini, J Müller, J Odell (eds.) *Agent-Oriented Software Engineering (AOSE) IV* (LNCS 2935, 2004) 214-230

Fitzpatrick, B, Taylor, N, "Human Rights and the Discretionary Exclusion of Evidence" (2001) 65 *Journal of Criminal Law* 349

Freiling, F C, "Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07", 29.09.2007, available online at http://pi1.informatik.uni-mannheim.de/filepool/publications/stellungnahme-online-durchsuchung.pdf

Fox, D "Realisierung, Grenzen und Risiken der 'Online-Durchsuchung'" (2007) 31:11 *Datenschutz und Datensicherheit*, 827-834

Fox, D, Secorvo Security Consulting GmbH, "Stellungnahme zur ‚Online-Durchsuchung' Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07", 29.09.2007, 1-17, at 7, available online at http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf

Galligan, D J, "More Scepticism About Scepticism" (1988) 8 *Oxford Journal of Legal Studies* 249

Garcia-Camino, A, Noriega, P, Rodriguez-Aguilar, J A, "Implementing Norms in Electronic Institutions" (2005) *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*, 667-673

Gardner, H, Hatch, T, "Multiple Intelligences Go to School: Educational Implications of the Theory of Multiple Intelligences" (1989) 18:8 *Educational Researcher* 4-10

Gardner, D, Shepherd, G M, "A gateway to the future of Neuroinformatics" (2004) 2:3 *Neuroinformatics* 271–274

Garson, J, "Connectionism" (2007) Stanford Encyclopedia of Philosophy, available online at: http://plato.stanford.edu/entries/connectionism/

Gelati, J, Totolo, A, Sartor, G, Governatori, G, "Normative Autonomy and Normative Co-ordination: Declarative Power, Representation, and Mandate" (2004) 12:1-2 *Artificial Intelligence and Law*, 53-81

George, E, "UK Computer Misuse Act – The Trojan Virus Defence Regina v Aaron Caffrey, Southwark Crown Court, 17 October 2003" (2004) 1:2 *Digital Investigation*, 89

Gercke, M, "Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit" (2007) *Computer und Recht*, 245

Gibbons, L J, "No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace" (1997) 6 *Cornell Journal of Law and Public Policy*, 475

Gilbert, D, et al., "IBM Intelligent Agent Strategy", (1995) *IBM Corporation*
Hansen, M, Pfitzmann, A, "Technische Grundlagen von Online-Durchsuchung und – Beschlagnahme" (2007) 8 *Deutsche Richterzeitung*, 225-228

Goldsmith, J L, "The Internet and the Abiding Significance of Territorial Sovereignty" (1998) 5 *Indiana Journal of Global Legal Studies* 475

Goldsmith, J L, "Against Cyberanarchy" (1998) 65 *University of Chicago Law Review* 1199

Goldsmith, J L, E A Posner, "A Theory of Customary International Law" (1999) 66:4 *The University of Chicago Law Review*, 1113

Goldsmith, J L, "The Internet and the Legitimacy of Remote Cross-Border Searches" (2001) *The University of Chicago Legal Forum* 103

Goldsmith, J, "Unilateral Regulation of the Internet: A Modest Defence" (2000) 11 *European Journal of International Law*, 135

Goldstein, E, "Photographic and Videotape Evidence in the Criminal Courts of England and Canada" (1987) *Criminal Law Review* 384

Governatori, G, Rotolo, A, "BIO Logical Agents: Norms, Beliefs, Intentions in Defeasible Logic" (2007) *Dagstuhl Seminar Proceedings 07122*, 1-34

Graf, J P, "Befugnisse und Grenzen der Ermittlungsbehörden" *Deutsches Polizeiblatt* 4/2001, 6

Greenleaf, G, "An Endnote on Regulating Cyberspace: Architecture vs Law?" (1998) 21:1 *University of New South Wales Law Journal*, 593

Groom, J, "Are 'Agent' Exclusion Clauses a Legitimate Application of the EU Database Directive?" (2004) 1:1 *SCRIPTed*, 83-118, available online at http://www.law.ed.ac.uk/ahrc/script-ed/docs/agents.asp

Hage, J, "A Theory of Legal Reasoning and A Logic to Match" (1996) 4 *Artificial Intelligence and Law*, 199-273

Hahn, C, et al., "Self-regulation through social institutions: A Framework for the Design of Self-Regulation of Open Agent-based Electronic Marketplaces" (2006) 12:1-2 *Computational & Mathematical Organization Theory.* Special Issue on Normative Multiagent Systems, 181-204

Hansard, House of Lords 28th June, 2000 (Committee Stage), Column 1012

Hansen, J, Pigozzi, G, Torre, L van der, "Ten Philosophical Problems in Deontic Logic" (2007) *Normative Multi-agent Systems*, *Dagstuhl Seminar Proceedings 07122*, 2

Hayes Weier, M, "Hewlett-Packard Data Warehouse Lands In Wal-Mart's Shopping Cart" *InformationWeek*, 4 August 2007, available online at: http://www.informationweek.com/news/storage/showArticle.jhtml?articleID=201203024

Heise, "Bayern will Regelung zu Online-Durchsuchungen vorantreiben" (2007) *heise*, available online at http://heise.de/-142981

Heiser, J G, "Understanding today's malware" (2004) 9:2 *Information Security Technical Report*, 56

Helsinki Times, "Finnish government wants police to have spyware powers" (2011) *Helsinki Times*, available online at: http://www.helsinkitimes.fi/htimes/domestic-news/politics/14409-finnish-government-wants-police-to-have-spyware-powers.html

Henziger, T A, Sifakis, J, "The Discipline of Embedded Systems Design" (2007) *IEEE Computer Society*, 37

Henziger, T A, "Two Challenges in Embedded Systems Design: Predictability and Robustness" (2008) *Philosophical Transactions of the Royal Society*, 2

Hert, P de, et al., "Legal Safeguards for Privacy and Data Protection in Ambient Intelligence" (2009) 13 *Personal Ubiquitous Computing*, 435

Hexmoor, H, "Case Studies of Autonomy" (2000) *Proceedings of FLAIRS*, 2000

Hildebrandt, M, Koops, B-J, "The Challenges of Ambient Law and Legal Protection in the Profiling Era" (2010) 73:3 *Modern Law Review*, 428

Hoekstra, R, et al., "The LKIF Core Ontology of Basic Legal Concepts" (2007) *Proceedings of the Workshop on Legal Ontologies and Artificial Intelligence Techniques (LOAIT 2007)*, 43-63

Hoffman, F G, "Complex Irregular Warfare: The Next Revolution in Military Affairs" (2005) 105:1 *The Military Balance* 411-420

Hoffmann-Riem, W, "Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme" (2008) *Juristenzeitung* 1009-1022

Hofmann, M, "Die Online-Durchsuchung – staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?" (2005) 25:3 *Neue Zeitschrift für Strafrecht* 121

Hohfeld, W N, "Some Fundamental Legal Conceptions As Applied in Judicial Reasoning" (1913-1914) 23 *Yale Law Journal*, 16

Hoppfield, J J, "Neural Networks and Physical Systems with Emergent Collective Computational Abilities" (1982) 79:8 *Proceedings of the National Academy of Science*, 2554

Hornung, G, "Ermächtigungsgrundlage für die Online-Durchsuchung und – Beschlagnahme" (2007) 31 *Datenschutz und Datensicherheit*, 575

Hornung, G, " Ein neues Grundrecht. Der verfassungsrechtliche Schutz der "Vertraulichkeit und Integrität informationstechnischer Systeme"", (2008) 5 *Computer und Recht*, 299

Hornung, G, Schnabel, C "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention" (2009) 25:2 *Computer Law & Security Review* 115-122

Hosmer, C, "Digital Evidence Bag" (2006) 49:2 *Communications of the ACM*, 69

House of Lords, European Union Committee, *Europol: Coordinating the Fight Against Serious and Organised Crime*, 29th Report of Session 2007-2008

Hughes, L A, DeLone, G J, "Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both?" (2007) 25 *Social Sciences Computer Review*, 78-97

Huhns, M N, "Agent Societies: Magnitude and Duration" (2002) *IEEE Internet Computing* 2-4

Hunton, P, "The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model" (2009) 25:6 *Computer Law & Security Review*, 528

Insa, F, "The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against Hight-Tech Crime – Results of a European Study" (2007) 1:4 *Journal of Digital Forensic Practice*, 285-289

Interpol, "General Secretariat 2002 Activity Report", available online at http://www.interpol.int/content/download/773/6131/version/5/file/agn72r01.pdf

Jaafar, J, McKenzie, E, "Decision Making Method Using Fuzzy Logic for Autonomous Agent Navigation" (2011) 3:1 *Electronic Journal of Computer Science and Information Technology*, 8-18

Jackson, P, et al., "Information extraction from Case Law and Retrieval of Prior Cases By Partial Parsing and Query Generation" (1998) *Proceedings of the International Conference on Artificial Intelligence and Law '98*, 60-67

Jennings, N R, Faratin, P, Johnson, M J, Norman, T J, O'Brien, P, Wiegand, M E, "Agent-based business process management" (1996) 5:2&3 *International Journal of Cooperative Information Systems*, 105-130

Jennings, N R, Sycara, K, Wooldridge, M, "A roadmap of agent research and development" (1998), 1:1 *Autonomous Agents and Multi-Agent Systems* 275-306

Johnson, D, Post, D, "Law and Borders – The Rise of Law in Cyberspace" (1996) 48 *Stanford Law Review* 1367

Jøsang, A, Bondi, V A, "Legal Reasoning with Subjective Logic" (2000) 8:4 *Artificial Intelligence and Law*, 289-315

Jul, E, Levy, H, Hutchinson, N, Black, A, "Fine-Grained Mobility in the Emerald System" (1988) 6:1 *ACM Transactions on Computer Systems*, 109-133

Kanger, S, "Law and Logic" (1972) 38 *Theorica*, 105-132

Karresand, M, "Seperating Trojan Horses, Viruses, and Worms – A Proposed Taxonomy of Software Weapons" (2003) *Proceedings of 2003 IEEE Workshop on Information Assurance*, 127-134

Katyal, N K, "Digital Architecture as Crime Control" (2003) 112 *The Yale Law Journal*, 2261

Kerr, O, "Cybercrime's Scope: Interpreting Access and Authorization in Computer Misuse Statutes" (2003) 78:5 *New York University Law Review* 1596-1668

Kelly, J P, "The Twilight of Customary International Law" (2000) 40:2 *Virginia Journal of International Law*, 449

Kemper, M, "Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten" (2007) 40:4 *Zeitschrift f*ür *Rechtspolitik,* 105-109

Kenneally, E E, "Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection" (2005) 9:2 *UCLA Journal of Law and Technology*, 3

Kephart, J O, Chess, D M, "The Vision of Autonomic Computing" (2003) 36:1 *IEEE Computer*, 41-50

Kesan, J P, Shah, R C, "Deconstructing Code" (2003-04) 6 *Yale Journal of Law & Technology*, 277

Khan, M K, Mahmud, M, Alghathbar, K S, "Security Analysis of Firewall Rule Sets in Computer Networks" (2010) *Fourth International Conference on Emerging Security Information Systems and Technologies (SECURWARE)*, 51-56

Killback, K D, Tochor, M D, "Searching for Truth but Missing the Point" (2002) 40 *Alberta Law Journal Review*, 333

Kirk, P L, "The Ontogeny of Criminalistics" (1963) 54:2 *The Journal of Criminal Law, Criminology, and Political Science*, 235-238

Knopp, M, "Rechtliche Perpektiven zur digitalen Beweisführung" (2009) Proceedings of GI Jahrestagung'2009, 1552-1566

Knott, G D, "A proposal for certain process management and intercommunication primitives" (1974) 8:4 *ACM SIGOPS Operating Systems Review*, 7-44

Kornblum, J, "Preservation of Fragile Digital Evidence by First Responders" (2002) *Digital Forensics Research Workshop*, 1, available online at: http://dfrws.org/2002/papers/Papers/Jesse_Kornblum.pdf

Krebs, V E, "Uncloaking Terrorist Networks" (2002) 7:4 *First Monday*

Krempel, S, "Bundesregierung gibt zu: Online-Durchsuchungen laufen schon" (2007) *heise,* available online at http://www.heise.de/newsticker/meldung/88824

Krempl, S, "Bayrischer Landtag setzt den 'Bayerntrojaner' frei" (2008) *heise*, available online at http://heise.de/-183633

Krempl, S, "Bundestag verabschiedet BKA-Gesetz mit heimlichen Online-Durchsuchungen" (2008) *heise*, available online at http://heise.de/-216645

Krempl, S, "SPD legt Verfassungsbeschwerde gegen den 'Bayerntrojaner' ein" (2008) *heise*, available online at http://heise.de/-207807

Krempl, S, "Rheinland-Pfalz lässt den Landestrojaner von der Leine" (2011) *heise*, available online at http://heise.de/-1178650

Krogh, A, "What are artificial neural networks?" (2008) 26:2 *Nature Biotechnology*, 195

Krogh, C, Herrestad, H, "Hohfeld in Cyberspace and Other Applications of Normative Reasoning in Agent Technology" (1999) 7 *Artificial Intelligence and Law*, 81-96

Koger, J L, "You Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace As Primary Legislator Of Electronic Signatures" (2001) 11 *Transnational Law and Contemporary Problems*, 491-516

Kohl, U, "Yahoo! – But No Hooray! for the International Online Community" (2001) 75 *Australian Law Journal* 401

Koops, B J, Vedder, A, "Criminal Investigation and Privacy: Opinions of Citizens" (2002) 18:5 *Computer Law & Security Report* 322-326

Kuhn, M G, "Electromagnetic Eavesdropping Risks of Flat-Panel Displays" (2004) *Workshop on Privacy Enhancing Technology, 26–28 May 2004, Toronto, Canada*, available online at http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf

Kuhn, T, *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 1962)

Kupchinsky, R, "Intelligence and Police Coordination in the EU" (2004) 4:11 *RFE/RL Organized Crime and Terrorism Watch*

Kutscha, M, "Verdeckte 'Online-Durchsuchung' und Unverletzlichkeit der Wohnung" (2007) *Neue Juristische Wochenschrif*t, 1169

Kutscha, M, "Mehr Schutz von Computerdaten durch ein neues Grundrecht?", (2008) 15 *Neue Juristische Wochenschrift*, 1042

Kuri, J, "Staatstrojaner: Von der 'rechtlichen Grauzone' zur Grundrechtsverletzung" *heise*, 10.10.2011, available online at http://heise.de/-1357873

Labrou, Y, Finin, T, "Semantics for an Agent Communication Language" (1998) 1365 *Intelligent Agents IV Agent Theories, Architectures, and Languages*, 209-214

Labrou, Y, Finin, T, Peng, Y, "Agent Communicaction Languages: The Current Landscape" (1999) *IEEE Intelligent Systems*, 45-52

Labrou, Y, Finin, T, "History, State of the Art and Challenges for Agent Communication Languages" (2000) *Swiss Federation of Information Processing Societies*, 1-16

Lange, D B, Oshima, M, "Seven Good Reasons for Mobile Agents" (1999) 42:3 *Communications of the ACM*, 88-89

Leipold, K, "Die Online-Durchsuchung", (2007) 4 *Neue Juristische Wochenschrift Spezial* 135

Leppard, D, "Police set to step up hacking of home PCs" (2009) *The Sunday Times*, available online at http://www.timesonline.co.uk/tol/news/politics/article5439604.ece

Leroux, O, "Legal Admissibility of Electronic Evidence" (2004) 18:2 *International Review of Law, Computers & Technology*, 193

Lessig, L, "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 *Harvard Law Review* 501

Levine, B N, Liberatore, M, "DEX: Digital Evidence Provenance Supporting Reproducibility and Comparison" (2009) *DFRWS Annual Conference*

Leyden, J, "Computer Virus turns 25", (2007) *The Register*, available online at http://www.theregister.co.uk/2007/07/13/virus_silver_jubilee/

Lippman, M, "Genocide: The Trial of Adolf Eichmann and the Quest for Global Justice" (2002) 8 *Buffalo Human Rights Law Review*, 45

Luck, M, McBurney, P, Preist, P, "Agent Technology: Enabling Next Generation Computing. A Roadmap for Agent-Based Computing" (2003) AgentLink II, IST-1999-29003, available online at http://eprints.ecs.soton.ac.uk/7309/

Lüders, S, "Verfassungsbeschwerde gegen BKA-Gesetz" (2009) *Humanistischer Presseverband*, available online at http://hpd.de/node/6228

Luethi, N, "Cybercops nehmen Dienst wieder auf" (2003) *Telepolis*, http://www.heise.de/tp/r4/artikel/13/13911/1.html

Lynch, C, Authenticity and integrity in the digital environment: An exploratory analysis of the central role of trust" (2000) *Authenticity in a Digital Environment*, Council on Library Information Resource

Maat, E de, Winkels, R, "Suggesting Model Fragments for Sentences in Dutch Law" (2010) *Proceedings of the Third International Workshop on Juris-informatics*, 19-28

Makison, D, "On the Formal Representation of Rights Relations" 15 *Journal of Philosophical Logic*, 403-425

Maudet, N, Chaib-Draa, B, "Commitment-baswd and dialogue-game-based Protocols: New Trends in Agent Communication Languages" (2002) 17:2 *The Knowledge Engineering Review*, 157-179

Maes, P, "Artificial Life Meets Entertainment: Life like Autonomous Agents" (1995) 38:11 *Communications of the ACM*, 108-114

Maier, H G, "Extraterritorial Jurisdiction at a Crossroads: an Intersection Between Public and Private International Law" (1982) 76 *American Journal of International Law*, 280

B Markesinis, "Judicial Mentality: Mental Disposition or Outlook as a Factor Impeding Recourse to Foreign Law" (2006) 80 *Tulane Law Review* 1325-1375.

Matorin, M J, "Unchaining the Law: The Legality of Extraterritorial Abduction in Lieu of Extradition" (1992) 41:4 *Duke Law Journal*, 907

McBurney, P, Parsons, S, "Games That Agents Play: A Formal Framework for Dialogues between Autonomous Agents" (2002) 11 *Journal of Logic, Language and Information*, 315-334

McBurney, P, Parsons, S, Wooldridge, M, "Desiderata for Agent Argumentation Protocols" (2002) *Proceedings of the First International Conference on Autonomous Agents and Multiagent Systems (AAMAS-02)*, Bologna, Italy

McCarty, L T, "Deep Semantic Interpretations of Legal Texts" (2007) *Proceedings of the International Conference on Artificial Intelligence and Law '07*, 217

McCarthy, J, Hayes, P J, "Some Philosophical Problems from the Standpoint of Artificial Intelligence" (1969) 4 *Machine Intelligence*, 464

McClelland, D C, "Testing for Competence rather than for 'Intelligence'" (1973) 28:1 *American Psychology*, 1-14

McClelland, J L, "Connectionist Models and Psychological Evidence" (1988) 27 *Journal of Memory and Language*, 107-123

McDowell, K, "Now That We Are All So Well-Educated about Spyware, Can We Put the Bad Guys out of Business?" (2006) *Proceedings of the 34th annual ACM SIGUCCS conference on User services*, 235 – 239

Mell, P, Grance, T, "The NIST Definition of Cloud Computing" (2011) *Computer Security*, available online at http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf

Meyers, M, Rogers, M, "Computer Forensics: The Need for Standardization and Certification" (2004) 3:2 *International Journal of Digital Evidence*, 6

Marrow, P, "Scalability in Multi-Agent Systems: The DIET Project" (2001) *Agents'01 Workshop on Infrastructure and Scalability for Agents*, ACM Press, New York

Milojicic, D S, LaForge, W, Chauhan, D, "Mobile Objects and Agents (MOA)" (1998) *Distributed Systems Engineering Journal*, 179-194

Milojicic, D, S, "Trend Wars - Mobile agent applications" (1999) 7:3 *EEE Concurrency* [see also IEEE Parallel & Distributed Technology] 80-90

Moens, M-F, Uyttendaele, C, Dumortier, J, "Abstracting of Legal Cases: The SALOMON Experience" (1997) *Proceedings of the International Conference on Artificial Intelligence and Law '97*, 114-122

Mowbray, M, "The Fog over the Grimpen Mire: Cloud Computing and the Law", 6:1 *SCRIPTed* 132-146

Mühlbauer, P, "Wie verlässlich sind digitale Beweise?" (2007) *Telepolis*, available online at http://www.heise.de/tp/r4/artikel/24/24638/1.html

Nachbar, T B, "Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character" (2000) 85 *Minnesota Law Review*, 215

Newell, A, Simon, H A, "Computer Sciences as Empirical Inquiry: Symbols and Search" (1976) 19:3 *Communications of the ACM*, 113-126

Nguy, N, "Using Architectural Contraints and Game Theory to Regulate International Cyberspace Behaviour" (2004) 5 *San Diego International Law Journal*, 431

Nickles, M, Rovatsos, M, Weiß, G, "A Schema For Specifying Computational Autonomy" (2002) *Proceedings of the Third International Worksop on Engineering Societies in the Agents World (ESAW)*

Nikkel, B J, "Improving Evidence Acquisition from Live Network Sources" (2006) 3 *Digital Investigation*, 89

Nissenbaum, H, "How Computer Systems Embody Values" (2001) 3 *IEEE Computer*, 120

Nowostawski, M, Purvis, M, "The Concecpt of Autonomy in Distributed Computation and Multi-Agent Systems" (2007) *2007/6 The Information Science Discussion Paper Series*, 3

Nuttall, M, "A brief survey of systems providing process or object migration facilities" (1994) 28:4 *ACM SIGOPS Operating Systems Review*, 64-80

Nwana, S, "Software Agents: An Overview" (1996) 11:3 *Knowledge Engineering Review*, 1-40

Oppliger, R, Rytz, R, "Digital Evidence: Dream and Reality" (2003) 1:5 *IEEE Security and Privacy*, 44
Out-Law, "Digital Economy Act to be Reviewed by Courts and Parliament" (2010) *out-law* http://www.out-law.com/page-11538

Paes, R, et al., "Specifying Laws in Open Multi-Agent Systems" (2009) 82:4 *Journal of Systems and Software*, 629-649

Pagallo, U, "Killers, Fridges, and Slaves: A Legal Journey in Robotics" (2011) 26:4 *AI & Society*, 347-354

Parsons, S, Klein, M, "Towards robust multi-agent systems: Handling communication exceptions in double auctions" (2004) *Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multiagent Systems*, 1482-1489

Pattenden, R, "Authenticating 'things' in English law: Principles for adducing tangible evidence in common law jury trials" (2009) 12 *The International Journal of Evidence & Proof*, 273

Paust, J J, "Federal Jurisdiction Over Extraterritorial Acts of Terrorism and Nonimmunity for Foreign Violators of International Law Under the FSIA and the Act of State Doctrine" (1983) 23 *Virginia Journal of International Law*, 191

Perkins, R M, "The Territorial Principle in Criminal Law" (1970) 22 *Hastings Law Journal* 1155.

Perritt, H H, "Cyberspace and State Sovereignty" (1997) 3 *Journal of International Legal Studies* 155

Platz, E, "Rechtliche Zulässigkeit von Remote Forensic Software in der Schweiz" (2008) *sic-online*, available online at http://www.sic-online.ch/2008/documents/838.pdf

Pohl, H "Zur Technik der heimlichen Online-Durchsuchung, (2007) 31:9 *Datenschutz und Datensicherheit*, 684-688

Popper, K, *The Logic of Scientific Discovery* (New York: Basic Books, 1959)

Popper, K, *Objective Knowledge: An Evolutionary Approach* (Oxford: Clarendon Press, 1982)

Powell, M, Miller, B, "Process Migration in DEMOS/MO" (1983) *Proceedings of the Ninth ACM Symposium on Operating Systems Principles* (ACM/SIGOPS, New York), 110-119

Pushpalatha, A, Mukunthan, B, "Automation of DNA Finger Printing for Precise Pattern Identification using Neural-fuzzy Mapping Approach" (2011) 13:3 *International Journal of Computer Applications*, 16

Quaresma, P, Rodrigues, I P, "A Question-Answering System for Portuguese Juridicial Documents" (2005) *Proceedings of the International Conference on Artificial Intelligence and Law '05*, 256-257

Randall, K C, "Universal Jurisdiction Under International Law" (1988) 66 *Texas Law Review*, 785

Rath, C, "Die Polizei als Hacker", (2006) *die tageszeitung* 11 December 2006, http://www.taz.de/index.php?id=archivseite&dig=2006/12/11/a0060

Reed, C, "The Admissibility and Authentication of Computer Evidence – A Confusion of Issues" (2005) 5th *BILETA Conference British and Irish Legal Technology Association*, 5

Reed, C, "Taking Sides on Technology Neutrality" (2007) 4:3 *SCRIPTed* 263-284

Reidenberg, J, "Lex Informatica" (1998) 76 *Texas Law Review* 553

Reidenberg, J R, "Technology and Internet Jurisdiction" (2005) 153 *University of Pennsylvania Law Review* 1951

Reiman, M, "Introduction: The *Yahoo!* Case and Conflict of Laws in the Cyberage" (2003) 24 *Michigan Journal of International Law* 663

Rejer, I, "A Method for Improving Agent's Autonomy" (2010) *Agent and Multi-Agent Systems: Technologies and Applications*, 52-61

Reith, M, Carr, C, Gunsch, G, "An Examination of Digital Forensic Models" (2002) 1:3 *International Journal of Digital Evidence*

Riecken, D, "An architecture of integrated agents" (1994) 37:7 *Communications of the ACM*, 107-116

Ringel, K, "Rechtsprobleme beim Zugriff auf EDV-Beweismittel" (1998) 3 *Deutsches Polizeiblatt*, 14

Roberts, A E, "Traditional and Modern Approaches to Customary International Law: A Reconciliation" (2001) 95:4 *The American Journal of International Law*, 757

Roßnagel, A, "Verfassungspolitische und verfassungsrechtliche Fragen der Online-Durchsuchung" (2007) 8 *Deutsche Richterzeitung*, 229-230

Rossi, P H, Waite, E, Bose, C E, Berk, R E, "The Seriousness of Crimes: Normative Structure and Individual Differences" (1974) 39:2 *American Sociology Review*, 224-237

Rotenberg, M, "Fair Information Practices and the Architecture of Privacy" (2001) *Stanford Technology Law Review* 1

Rötzer, F, "CCC entlarvt Bundestrojaner und Sicherheitspolitik" (2011) *TELEPOLIS*, available online at http://www.heise.de/tp/artikel/35/35648/1.html

Rouvroy, A, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence" (2008) 2:1 *Studies in Ethics, Law, and Technology*, Article 3

Rux, J, "Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden – Rechtsfragen der 'Online-Durchsuchung'" (2007) 6 *Juristenzeitung*, 285-295

Samuels, A, "Illegally Obtained Evidence: In or Out?" (2003) 67 *Journal of Criminal Law* 411-414

Sartor, G, "Fundamental Legal Concepts: A Formal and Teleological Characterisation", (2006) 14 *Artificial Intelligence and Law*, 101-142

Sartor, G, "Doing Justice to Rights and Values: Teleological Reasoning and Proportionality, (2010) 18:2 *Artificial Intelligence and Law*, 175-215

Scarr, S Weinberg, R A, "IQ test performance of black children adopted by white families",(1976) 31:10 *American Psychologist,* 726-739

Schaar, P, "Anmerkung zum Beschluss des BGH vom 31.1.2007 - StB 18/06 - zur verdeckten Online-Durchsuchung", (2007) 10:4 *Kommunikation und Recht* 202-205

Schachter, O, *International Law in Theory and Practice* (Dordrecht, The Netherlands; Boston: M. Nijhoff Publishers, 1991)

Schaerer, E, "Robots As Animals: A Framework for Liability and Responsibility in Human-Robot Interactions" (2009) *18th IEEE International Symposium on Robot and Human Interactive Communication*, 72-77

Schafer, B, "The taming of the Sleuth—problems and potential of autonomous agents in crime investigation and prosecution" (2006) 20:1 *International Review of Law, Computers & Technology*, 63-76

Schafer, B, et al., "Towards a Financial Fraud Ontology: A Legal Modelling Approach" (2006) 12 *Artificial Intelligence and Law*, 419-446

Schafer, B, Danidou, Y, "Trusted computing and the digital crime scene" (2011) 8 *Digital Evidence and Electronic Signature Law Review* 111-123

Schmidt, J, "Bundestrojaner: Geht was – was geht. Technische Optionen für die Online-Durchsuchung"(2007) *heise*, available online at http://www.heise.de/security/Bundestrojaner-Geht-was-was-geht--/artikel/86415

Schulz, H, "Male Captus, Bene Deditus?" (1984) 40 *Schweizerisches Jahrbuch für Internationales Rrecht*, 93

Scientific Working Group on Digital Evidence (SWGDE), "Digital Evidence: Standards and Principles" (2000) 2:2 *Forensic Science Communications*, available online at: http://www.fbi.gov/about-us/lab/forensic-science-communications/forensic-science-communications-april-2010

Searle, J R, "Minds Brains, and Programs" (1980) 3 *The Behavioral and Brain* Science, 417

Seitz, N, "Transborder Search: A new Perspective in Law Enforcement?" (2005) 23 *Yale Journal of Law and Technology*, 23

Selker, T, "Coach: A Teaching Agent that Learns" (1994) 37:7 *Communications of the ACM*, 92-99

Sergot, M, "A Computational Theory of Normative Positions" (2001) 2:4 *ACM Transactions on Computational Logic*, 581-622

Sieber, U, "Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen", 09.10.2007, 1-24, at 12, available online at http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf

Siena, A, et al., "Towards a Framework for Law-Compliant Software Requirements" (2009) *IEEE ICSE-Companion, 31st International Conference on Software Engineering*, 251

Sipior, J C, Ward, B T, "Trust, privacy, and legal protection in the use of software with surreptitiously installed operations: An empirical evaluation" (2008) 10:3 *Information Systems Frontiers*, 3-18

Site Security Policy Handbook Working Group, Site Security Policy Handbook RFC 1244, 1991, 50, available online at http://www.faqs.org/ftp/rfc/pdf/rfc1244.txt.pdf

Smith, B, Welty, C, "FOIS Introduction: Ontology – Towards a New Synthesis" (2001) *Proceedings of the International Conference on Formal Ontology in Information Systems*, 3-9

Smith, D C, Cypher, A, Spohrer, J, "Programming agents without a programming language" (1994) 37:7 *Communications of the ACM*, 55-67

Smith, J M, "A Survey of Process Migration Mechanisms" (1988) 22:3 *ACM SIGOPS Operating Systems Review*, 28-40

Smolensky, P, "Connectionist AI, Symbolic AI, and the Brain" (1987) 1:2 *Artificial Intelligence Review*, 95-109

Sofaer, A, et al., "A Proposal for an International Convention on Cybercrime and Terrorism" (2000) *Centre for International Security and Cooperation, Stanford University*, Article 6 (5), available online at http://iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf

Sokolov, D AJ, "Österreich: Arbeitsgruppe Online-Durchsuchung legt Bericht vor, (2008) *heise*, available online at: http://heise.de/-198121

Solum, L, "Legal Personhood for Artificial Intelligences" (1992) 70 *North Carolina Law Review*, 1231-1287

Sommestad, T, Ekstedt, M, Johnson, P, "A Probabilistic Relational Model for Security Risk Analysis" (2010) 29:6 *Computers & Security*, 659-679

Sorge, C, "Conclusion of contracts by electronic agents" (2005) *Proceedings of the 10th international conference on Artificial intelligence and law*, 210-214

Spatscheck, R, "Steuerhinterziehung im Internet" (2000) 28 *Strafverteidiger Forum*, 1

Stafford, T F, Urbaczewski, A "Spyware: The Ghost in the Machine" (2004) 14 *Communications of the Association for the Information Systems*, 291-306

Stamos, J, Gifford, D, "Remote evaluation" (1990) 12:4 *ACM Transactions on Programming Languages and Systems*, 537-565

Stankovic, J A, Ramamritham, K, "What is Predictability for Real-Time Systems?" (1990) 2 *Real-Time Systems,* 247-254

Steels, L, "When Are Robots Intellligent Autonomous Agents?" (1995) 15 *Robotics and Systems*, 4

Sukthankar, G, Sycara, K, "Policy Recognition for Multi-Player Tactical Scenarios" (2007) *Proceedings of the 6th International Joint Conference on Autonomous Agents and Multiagent Systems* (AAMAS '07), ACM, New York, 1-8

Sunner, M, "The Rise of the Targeted Trojans" (2007) 12 *Network Security* 4-7

Sussmann, M, "The Critical Challenges from International High-Tech and Computer-related Crime at the Millenium" (1999) 9 *Duke Journal of Computer & International Law*, 451

Swafford, L L, "Admissibility of DNA Genetic Profiling Evidence in Criminal Proceedings" (1990) 18:1 *Pepperdine Law Review*, 123

Swimmer, M, "Malicious Software in Ubiquitous Computing" in M Petkovic, W Jonker (eds.) *Security, Privacy, and Trust in Modern Data Management* (Berlin Heidelberg: Springer, 2007) 451-466

Tinnefeld, M-T, "Online-Durchsuchung : Menschenrechte vs. virtuelle Trojaner", (2007) 10:3 *MultiMedia und Recht* 225-228

Torre, L van der, "Contextual Deontic Logic: normative agents, violations and independence" (2003) 37 *Annals Mathematics and Artificial Intelligence* 33

Tupman, B "Where has all the money gone? The IRA as a profit-making concern" (1998) 1:4 *Journal of Moneylaundering Control*, 32-40

Turing, A, "Computing Machinery and Intelligence" (1950) 236 *Mind*, 433-460

Turner, P, "Digital provenance – interpretation, verificaton and corroboration" (2005) 2 *Digital Investigation*, 45

Turner, P, "Selective and intelligent imaging using digital evidence bags" (2006) 3 *Digital Investigation*, 59

Urbach, R R , Kibel, G A, "Adware/Spyware: An Update Regarding Pending Litigation and Legislation", (2004) 16:7 *Intellectual Property and Technology Law Journal*, 12-16

Valeri, M, "Europe's first 'Online Police Station'", (2006) presented at *6th Computer Law World Conference*, Edinburgh

Vazquez-Salceda, J, et al., "From Human Regulations to Regulated software Agents' behavior: Connecting the abstract declarative norms with the concrete operational implementation" (2008) 16 *Artificial Intelligence and Law*, 73-87

Walker, C, "Computer Forensics: Bringing the Evidence to Court" (2007) *infosecwriters*, available online at http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf

Walker-Morgan, DJ, "CCC Cracks Government Trojan" (2011) *The H Security*, available online at: http://h-online.com/-1357755

Wall, D S, "Digital Realism and the Governance of Spam as Cybercrime" (2005) 10 *European Journal on Criminal Policy and Research*, 309

Wallach, W, Franklin, S, Allen, C, "A Conceptual and Computational Model of Moral Decision Making in Human and Artificial Agents" (2010) 2 *Topics in Cognitive Science*, 455

Watt, H M, "Yahoo! Cyber-Collision of Cultures: Who Regulates?" (2003) 24 *Michigan Journal of International Law* 673

Wegener, C, "Hintergründe zum Vorhaben 'Online-Durchsuchung'" 15. Workshop "Sicherheit in vernetzten Systemen", 3 available online at: http://www.wecon.net/files/14/DFN2008-HzVOD-ARTIKEL.pdf

Weinberg, R A, "Intelligence and IQ" (1989) 44:2 *American Psychology*, 98-104

Weitzenböck, E, "Electronic Agents and the Formation of Contracts" (2001) 9:3 *International Journal of Law and Information Technology*, 204-234

Weitzenböck, E, "Good faith and fair dealing in contracts formed and performed by electronic agents" (2004) 12:1-2 *Artifical Intelligence and Law*, 83-110

Welch, C H, "Flexible Standards, Deferential Review: Daubert's Legacy of Confusion" (2006) 29:3 *Harvard Journal of Law and Public Policy*, 1085

Wheate, R M, Jamieson, A, "A Tale of Two Approaches – The NAS Report and the Law Commission Consultation Paper on Forensic Science" (2009) 7:2 *International Commentary on Evidence*, 3

Wilske, S, Schiller, T, "International Jurisdiction in Cyberspace: Which States May Regulate the Internet?" (1997) 50 *Federal Communications Law Journal*, 171.

Wong, D, Paciorek, N, Moore, D, "Java-based Mobile Agents" (1999) 42:3 *Communications of the ACM*, 92-101

Wooldridge, M, Jennings, N R, "Intelligent Agents: Theory and Practice" (1995) 10:2 *The Knowledge Engineering Review*, 115-152

Wooldridge, M, "Semantic Issues in the Verification of Agent Communication Languages" (2000) 3 *Autonomous Agents and Multi-Agent Systems*, 9-31

Wooldridge, M, "Intelligent Agents: The Key Concepts" (2001) Vol. 2322 Lecture Notes in Computer Science, Proceedings of the 9th ECCAI-ACAI/EASSS, 3-43

Wu, T, "When Code Isn't Law" (2003) 89 *Virginia Law Review* 679

Zadeh, L A, "Fuzzy Sets" (1965) 8 *Information and Control*, 338-353

Zadeh , L A, "Fuzzy Logic and Approximate Reasoning" (1975) 30:3-4 *Synthese*, 407-428

Zadeh, L A,"Fuzzy Sets as a Basis for a Theory of Posibility" (1978) 1:1 *Fuzzy Sets and Systems*, 3-28

Zadeh, L A, "Fuzzy Logic" (1988) 21:4 *Computer*, 83-93

Zadeh, L A, "Fuzzy Logic, Neural Networks, and Soft Computing" (1994) 37:3 *Communicatioins of the ACM*, 77-84

Zadeh, L A, "A Summary and Update of Fuzzy Logic" (2010) *2010 IEEE International Conference on Granular Computing*, 42-44

Zelinsky, A, Shubik, M, "Terrorist Groups as Business Firms: A New Typological Framework" (2009) 21:2 Terrorism and Political Violence, 327-336

Zetter, K, "Researchers Connect Flame to US-Israel Stuxnet Attack" (2012) *Wired*, available online at: http://www.wired.com/threatlevel/2012/06/flame-tied-to-stuxnet/

Books

Anonymous, *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network* (Canada: SAMS, 2002)

Arbib, M A, Grethe, J S, *Computing the Brain: A Guide to Neuroinformatics* (San Diego: Academic Press, 2001)

Arend, A C, Beck, R J, *International Law and the Use of Force: Beyond the UN charter Paradigm* (London: Routledge, 1993)

Bankowski, Z, Del Mar, M, Maharg, P, (eds) *Beyond Text, vol 1: The Arts and the Legal Academy* (Farnham, Surrey: Ashgate Publishing, 2012)

Bär, W, *Der Zugriff auf Computerdaten im Strafverfahren* (Köln: Heymanns Verlag, 1992)

Bentham, J, *Rationale of Judicial Evidence, Specially Applied to English Practice*, Vol 1 (London: Hunt and Clarke, 1827)

Beulke, W, *Strafprozessrecht* (Heidelberg, München: C.F. Müller, 2010, 11th ed)

Bing, J, Sartor, G, (eds) *The Law of Electronic Agents* (Oslo: Norwegian Research Center for Computers and Law, 2003).

Böckenförde, T, *Die Ermittlung im Netz* (2003, Tübingen: Mohr Siebeck)

Boczek, B A, *International Law: A Dictionary* (Lanham, Md.: Scarecrow Press, 2005)
Bontchev, V V, *Methodology of Computer Anti-Virus Research*, Unpublished Doctoral Thesis, University of Hamburg, 1998.
Braun, P, Rossak, W, *Mobile Agents: Basic Concepts, Mobility Models, and the Tracy Toolkit* (Morgan Kaufman Publishers Inc., San Francisco, CA: 2004)

Brenner, S W, *Cybercrime: Criminal Threats from Cyberspace* (Santa Barbara, CA: Greenwood, 2010)

Briel, O G von, Ehlscheid, D, *Steuerstrafrecht* (Bonn: Deutscher Anwaltverlag, 2001)

Casey, E, *Digital Evidence and Computer Crime: Forensic Science, Computers and The Internet* (Amsterdam: Elsevier Academic Press, 3rd edition, 2011)

Choo, A L-T, *Evidence* (Oxford: Oxford University Press, 2006)

Cignoli, R, D'Ottaviano, I, Mundici, D, *Algebraic Foundations of Many-Valued Reasoning* (Dordrecht: Kluwer, 2000)

Cleary, E W, (ed), *McCormick on Evidence*, 3rd ed. (St. Paul: West, 1984)

Clough, J, *Principles of Cybercrime* (Cambridge, UK; New York: Cambridge University Press, 2010)

Deaver, J, *Roadside Crosses* (New York: Simon & Schuster, 2009)

Dennis, I, *The Law of Evidence* (London: Sweet & Maxwell, 2010)

d'Inverno, M, Luck, M, *Understanding Agent Systems* (Berlin: Springer, 2004)

Dworkin, R, *A Matter of Principle* (Havard: Havard University Press, 1985)

DeForest, P, Gaensslen, R, Lee, H, *Forensic Science: An Introduction to Criminalistics* (New York: McGraw Hill: 1983)

Doehring, K, *Völkerrecht* (Heidelberg: C.F. Müller, 2004)

Eberhart, R C, Shi, Y, *Computational Intelligence: Concepts to Implementation* (Burlington: Morgan Kaufmann Publishers, 2007)

Eisenberg, U, *Beweisrecht der StPO* (München: C.H. Beck Verlag, 2011)

Feyerabend, P, *Against Method* (London: Verso, 1993)

Finnis, J, *Fundamentals of Ethics* (Washington: Georgetown University Press, 1983)

Foucault, M, Discipline and Punish (New York: Pantheon, 1977)

Francesconi, E, Montemagni, S, Peters, W, Tiscornia, D, (eds) *Semantic Processing of Legal Texts: Where the Language of Law Meets the Law of Language* (Berlin, Heidelberg: Springer, 2010)

Gardner, H, *Frames of Mind* (New York: Basic Books, 1983)

Gercke, M, *Rechtswidrige Inhalte im Internet: eine Diskussion ausgewählter Problemfelder des Internet-Strafrechts unter Berücksichtigung strafprozessualer Aspekte* (Aachen: Hochschulschrift, 2000)

Gercke, M, Brunst, P W, *Praxishandbuch Internetstrafrecht* (Stuttgart: Kohlhammer, 2009)

Germann, M, *Gefahrenabwehr und Strafverfolgung im Internet* (Berlin: Duncker & Humblot, 2000)

Gillham, B, *Research Interviewing: The Range of Techniques* (Berkshire: Open University Press, 2005)

Gottfredson, L S, "Mainstream sciences on Intelligence: An Editorial with 52 Signatories, History, and Bibliography" (1997) 24:1 *Intelligence*, 13-25

Gottwald, S, *A Treatise on Many-Valued Logic* (Baldock: Research Studies Press, 2001)

Hajek, P, *Metamathematics of Fuzzy Logic* (Dordrecht: Kluwer, 1998)

Haller, K, Conzen, K, *Das Strafverfahren* (Heidelberg, München: C.F. Müller, 2008)

Hellmann,U, *Strafprozessrecht* (Berlin, Heidelberg: Springer, 2006, 2nd ed)

Hempel, C, *The Philosophy of Carl G.Hempel: Studies in Science, Explanation and Rationality* (Oxford: Oxford University Press, 2001)

Herrmann, C, *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität – Entstehung und Perspektiven* (Frankfurt/Main: Peter Lang, 2010)

Higgins, R, *Problems and Process: International Law and How We Use It* (Oxford: Clarendon Press; New York: Oxford University Press, 1994)

Hillier, T, *Sourcebook on Public International Law* (London; Sydney : Cavendish, 1998)

Ho, H L, *A Philosophy of Evidence Law* (Oxford: Oxford University Press, 2008)

Hohfeld, W N, *Fundamental Legal Conceptions as Applied in Judicial Reasoning and Other Legal Essays* (New Haven: Yale University Press, 1923)

Horty, J, *Agency and Deontic Logic* (Oxford: Oxford University Press, 2001

Inman, K, Rudin, N, *Principles and Practices of Criminalistics: The Profession of Forensic Science* (Boca Raton, Florida: CRC Press, 2001)

Jennings, N R, Wooldridge, M, *Agent Technology, Foundations, Applications and Markets* (Berlin:Springer, 1998)

Jennings, R, Watts, A, (eds.), *I Oppenheim's International Law* (9th edition, Longmans, 1992)

Jofer, R, *Strafverfolgung im Internet: Phänomenologie und Bekämpfung kriminellen Verhaltens in internationalen Computernetzen* (Frankfurt am Main: Lang, 1999)

Joubert, C, *Judicial Control of Foreign Evidence in Comparative Perspective* (Amsterdam, Netherlands: Rozenberg Publishers, 2005)

Joyner, C C, *International Law in the 21st Century: Rules for Global Governance* (Lanham, MD: Rowman & Littlefield Publishing, 2005)

A Keane, *The Modern Law of Evidence* (Oxford, New York: Oxford University Press, 7th edition, 2008)

Klemke, O, Elbs, H, *Einführung in die Praxis der Strafverteidigung* (Heidelberg, München: C.F. Müller, 2010)

Klir, G J, Yuan, B, (eds) *Fuzzy Sets, Fuzzy Logic and Fuzzy Systems: Selected Papers by Lotfi A Zadeh* (Singapore: World Scientific, 1996)

Kohl, U, Jurisdiction and the Internet (Cambridge: Cambridge University Press, 2007)

Kugelmann, D, *Polizei-und Ordnungsrecht*, (Heidelberg: Springer, 2006)

Kurzweil, R, *The age of intelligent machines* (MIT Press, Cambridge, MA: 1990)

Kvale, S, *Interviews: An Introduction to Qualitative Research Interviewing* (Thousand Oaks California: Sage Publications, 1996)

Labrosse, JJ, et al., *Embedded Software* (Oxford: Elsevier, 2008)

Leflar, R, *American Conflicts Law* (3rd edition, Indianapolis: Bobbs-Merrill, 1977)

Lessig, L, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999)

Lessig, L, *Code Version 2.0* (New York: Basic Books, 2006)

Lindahl, L, *Position and Change: A study in Law and Logic* (Dordrecht: D. Reidel Publishing, 1977)

Liu, J, Jin, X, Tsui, K C, *Autonomy Oriented Computing: From Problem Solving to Complex Systems Modeling* (Dordrecht: Kluwer, 2005)

Lucas, R A, *Evolving Artificial Neural Network Controllers for Autonomous Agents Navigating Dynamic Environments* (University of Northern British Columbia: Thesis, 2008)

Luck, M, Ashri, R, D'Inverno, M, *Agent-based Software Development* (Norwoord: ArtechHouse Inc., 2004)

Malanczuk, P, *Akehurst's Modern Introduction to International Law* (London: Routledge, 1997)

Mason, S (ed), International Electronic Evidence (London: British Institute for International and Comparative Law, 2008)

Mason, S, (ed) *Electronic Evidence* (London: Lexis Nexis Butterworths, 2010)

Malek, H M (ed), *Phipson on Evidence* (London: Sweet & Maxwell, 17th ed, 2010)

Miles, M B, Huberman, A M, *Qualitative Data Analysis: A Sourcebook of New Methods* (Thousand Oaks, California: Sage Publications, 1984)

Miles, M B, Huberman, A M, *Qualitative Data Analysis: An Expanded Sourcebook* (Thousand Oaks, California: Sage Publications, 1994, 2nd ed)

Moore, D S, *The Dependent Gene: The Fallacy of the Nature versus Nurture Debate* (New York: Henry Holt, 2003)

Morse, J M, Field, P A, *Nursing Research: The Application of Qualitative Approaches* (Cheltenham: Nelson Thornes, 2002, 3rd ed)

Nelson B, et al., *Guide to Computer Forensics and Investigations* (Boston, MA: Cengage Learning, 2009)

Nemeth, C P, *Law and Evidence: A Primer for Criminal Justice, Criminology and Legal Studies*, 2nd ed (Sudburry: Jones and Bartlett, 2011)

Nguyen, H T, Noguera, C, *First Course in Fuzzy Logic* (Boca Raton: Chapman & Hall/CCRC Press, 1999, 2dn ed)

Nilsson, N J, *Artificial Intelligence: A New Synthesis* (Burlington: Morgan Kaufmann Publishers, 1998)

Novak, V, *Fuzzy Sets and their Applications* (Bristol: Adam Hilger, 1989)

Novak, V, Perfilieva, I, Mockor, J, *Mathematical Principles of Fuzzy Logic* (Dordrecht: Kluwer, 2000)

Olive, J, Christianson, C, McCary, J, (eds) *Handbook of Natural Language Processing and Machine Translation* (New York, Heidelberg, London: Springer, 2011)

Pfeifer, R, Scheier, C, *Understanding Intelligence* (MIT Press: Cambridge, MA, 1999)

Pfeifer, R, Bongard, J, Berry, D, *Designing Intelligence – Why Brains Aren't Enough* (Norderstedt: GRIN Verlag, 2011)

Pollitt, M, Bianchi, R, "Digital Evidence" in A Mozayani, C Noziglia (eds) *The Forensic Laboratory Handbook Procedures and Practice* (New York, Dordrecht, Heidelberg, London: Springer, 2011 2nd ed)

Poole, D, Mackworth, A, Goebel, R, *Computational Intelligence: A Logical Approach* (New York: Oxford University Press, 1998)

Raz, J, *The Concept of a Legal System* (Oxford: Oxford University Press, 1980, 2nd ed)

Reber, A S, Reber, E, Allen, R, *The Penguin Dictionary of Psychology* (Penguin Press: New York, US, 2009)

Reed, C, *Internet Law: Texts and Materials* (Cambridge, Cambridge University Press: 2004)

Rein, R, *Argentine Jews or Jewish Argentines?: Essays on Ethnicity, Identity, and Diaspora* (Leiden, Netherlands: Martinus Nijhoff, 2010)

Ross, A, *Directives and Norms* (London: Routledge, 1968)

Ross, T J, *Fuzzy Logic with Engineering Applications* (Chichester: John Wiley & Sons, 2004, 2nd ed)

Roxin, C, Achenbach, H, *Strafprozessrecht* (München: Beck, 2006, 16th ed)

Russel, S, Norvig, P, *Artificial Inteligence: A Modern Approach* (Prentice Hall: New Jersey: 2003)

Saferstein, R, *Forensic Science Handbook, Volume II* (Englewood Cliffs, New Jersey: Prentice-Hall, 1988)

Schermer, B W, Durinck, M, Bijmans, L, *Juridische Aspecten van Autonome Systemen* (Leidenschendam: ECP.NL, 2005)

Schermer, B W, *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance* (Leiden University Press: Leiden, 2007)

Schermer, M, *The Different Faces of Autonomy: Patient Autonomy in Ethical Theory and Hospital Practice* (Dordrecht: Kluwer, 2002)

Simon, H A, *The Sciences of the Artificial* (Cambridge: M.I.T. Press, 1969)

Smith, R F, The Windows Security Log Encyclopedia (North Charleston, SC: Booksurge Llc, 2007)

Spitz, H H, *The raising of intelligence: A selected history of attempts to raise retarded intelligence* (Hillsdale, NJ: Erlbaum, 1986)

Stair, R M, Reynolds, G W, *Principles of Information Systems* (Course Technology Press: Boston, 2009)

Stephen, J F, *A Digest of the Law of Evidence*, ed. by H L Stephen, L F Sturge (London: Macmillan, 1948)

Thierer, A, Crews, C W, (eds) *Who rules the net?: Internet governance and jurisdiction* (Massachusetts: Cato Institute, 2003)

Toepel, F, *Grundstrukturen des Sachverständigenbeweises im Strafprozessrecht* (Tübingen: Mohr Siebeck, 2002)

Turkle, S, *Life on the Screen: Identity in the Age of the Internet* (New York: Simon and Schuster, 1995)

Turkle, S, *The Second Self: Computers and the Human Spirit* (Cambridge: MIT Press, 2005)

Turkle, S, *Simulation and Its Discontents* (Cambridge: MIT Press, 2009)

Turunen, E, *Mathematics Behind Fuzzy Logic (Advances in Soft Computing)* (Heidelberg: Physica Verlag, 1999)

United States Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3rd edition, OLE Litigation series, 2009), 56, available online at http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf

Vacca, J R, *Computer Forensics: Computer Crime Scene Investigation* (Hingham, MA: Charles River Media, 2nd edition, 2005)

Vlassis, N, *A Concise Introduction to Multiagent Systems and Distributed Artificial* (Morgan & Claypool: San Rafael, CA, 2007)

Weinrib, E J, *The Idea of Private Law* (Harvard: Harvard University Press, 1995)

Weiss, G, (ed), *Multiagent systems: a modern approach to distributed artificial intelligence* (MIT Press: Cambridge, MA, 1999)

Wigmore, J H, *The Science of Judicial Proof, as given by Logic, Psychology, and General Experience, and Illustrated in Judicial Trials* (Boston: Little Brown and Co, 3rd ed, 1937)

Wigmore, J H, *Wigmore on Evidence*, 3rd ed., Vol. 7 (Boston: Chardbourn, 1940)

Wooldridge, M, *An Introduction to Multi-agent Systems* (West Sussex: John Wiley & Sons Ltd, 2002)

Zagaris, B, *International White Collar Crime: Cases and Materials* (Cambridge, UK: Cambridge University Press, 2010) 275

Zhuang, L, *Security Inference from Noisy Data*, (2008), Unpublished PhD thesis, University of California, Berkeley, available online at http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-32.pdf

Zimmermann, H-J, *Fuzzy Set Theory and its Applications* (Dordrecht: Kluwer, 1991, 2nd ed)

Chapters in Books

Alexy, R, Dreier, R, "Statutory Interpretation in the Federal Republic of Germany", in N MacCormick and R Summers (eds) *Interpreting Statutes: A Comparative Study* (Darthmouth: Aldershot, 1991)

Allen, A E, Saxon, C S, "A-Hohfeld: A language for Robust Sturctural Representation of Knowledge in the Legal Domain to Build Interpretation-Assistance Expert Systems" in J Meyer, R J Wieringa (eds) *Deontic Logic in Computer Science: Normative System Specification* (Chichester, New York: J Wiley, 1993)

Andrade, F, Novais, P, Neves, J, "Will and Declaration in Acts Performed by Intelligent Software Agents - Preliminary Issues on the Question" in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005) 53-55

Asscher, L F, "'Code' as Law – Using Fuller to Assess Code Rules" in E J Dommering, L F Asscher (eds) *Coding Regulation. Essays on the Normative Role of Information Technologies*, IT & Law Series vol 12 (The Hague: TMC Asser Press, 2006) 85

Bacon, Francis, "Meditationes Sacrae" (1597), in James Spedding, Robert Ellis, Douglas Heath (eds), *The Works of Francis Bacon* (1887-1901), Vol. 7, 253

Balkin, J M, Kozlovski, N, "Introduction" in J M Balkin, J Grimmelmann, E Katz, N Kozlovski, S Wagman, T Zarsky (eds) *Cybercrime: Digital Cops in a Networked Environment* (New York, London: New York University Press, 2007) 1-12

Bernardez, S T, "Territorial Sovereignty" in R Bernhardt (ed) *Encyclopedia of Public International Law* (4th ed., North-Holland Publishing Co.: Amsterdam, 2000) 823

J Bing, "Human Rights in the Digital Age" in M Klang, A Murray (eds) *Human Rights in the Digital Age* (London: Glasshouse Press, 2006) 203-217

Bing, J, "Building Cyberspace: A Brief History of Internet" in L A Bygrave, J Bing (eds.) *Internet Governance: Infrastructure and Institutions* (Oxford, New York: Oxford University Press, 2009) 8-48

Black, R, "Ethics and the Products of Science", in R E Spier (ed) *Science and Technology Ethics* (London: Routledge, 2002)

Böhme R, et al., "Multimedia Forensics Is Not Computer Forensics" in Z J M H Geradts, K Y Franke, C J Veenman (eds.) *Computational Forensics: Third International Workshop*, *IWCF 2009* (Berlin, Heidelberg: Springer, 2009) 90-103

Bohn, J, et al., "Ethical Implications of Ambient Intelligence and Ubiquitous Computing" in W Weber, J Rabaey, E Aarts (eds) *Ambient Intelligence* (Berlin, Heidelberg, New York: Springer, 2005), 14
Boonk, M L, de Groot, D R A, Brazier, F M T, Oskamp, A , "Agent exclusion on websites" (2005) in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005), 13-20

Braun, P, Trinh, D, Kowalczyk, R, "Integrating a New Mobility Service into the Jade Agent Toolkit" in T Magedanz et al.(eds.) *Mobility aware technologies and applications: second international workshop*, Lecture Notes in Computer Science (Berlin: Springer-Verlag, 2005), 354–363

Breuker, J, Winkels, R, Valente, A, "A Core Ontology for Law" in K van Marcke, W Daelemans (eds) *Proceedings of the 9th Dutch AI Conference* (Antwerpen: NVKI, 1997)

Brooks, R A, "How to build complete creatures rather than isolated cognitive simulators", in K VanLehn (ed) *Architectures for Intelligence* (Hillsdale, NJ: Lawrence Erlbaum Assosiates, 1991), 225-239

Brownsword, R, Yeung, , K, "Regulating Technologies – Tools, Targets and Thematics" in R Brownsword, K Yeung (eds) *Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes* (Oxford, Portland: Hart Publishing, 2008)

Calmet, J, Endsuleit, R, "An Agent Framework for Legal Validation of E -Transactions" in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005) 181-184

Chan, T S, "Spyware" in H Bidgoli (ed.) *Handbook of Information Security Volume 1* (Wiley: Hoboken, New Jersey, 2005) 136-146

Chapple, M J, Striegel, A, Crowell, C R, "Firewall Rulebase Management: Tools and Techniques", in M Quigley (ed) *ICT Ethics and Security in the 21st Century: New Developments and Applications* (Hershey: IGI Global, 2011) 254-276

Chess, D, Harrison, C, Kershenbaum, A, "Mobile agents: Are they a good idea?" in J Vitek, C Tschudin (eds), *Mobile Object Systems - Towards the Programmable Internet*, Lecture Notesin Computer Science (Springer-Verlag, Berlin Germany: 1997), 25–47

Dignum, F, et al., "A Modal Approach to Intentions, Commitments and Obligations: Intention plus Commitment yields Obligations" in M Brown, J Carmo (eds.) *Deontic Logic, Agency and Normative Systems* (Berlin: Springer Verlag, 1996) 80-97

Flanagan, M, Howe, D C, Nissenbaum, H, "Embodying Values in Technology – Theory and Practice" in J van den Hoven, J Weckert (eds) *Information Technology and Moral Philosophy* (Cambridge: Cambridge University Press, 2008) 322

Franklin, S, Grasser, A, "Is it an agent, or just a program? A taxonomy for autonomous agents" in J Miller, M Wooldridge, N Jennings (eds) *Intelligent Agents III: Agent Theories, Architectures, and Languages* (Springer Verlag, Berlin: 1997), 21 – 35

Gelati, J, Riveret, R, "DRM in a Multi-Agent System Marketplace" in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005) 123-139

Gercke, M, "Telekommunikationsüberwachung" in F Roggan, M Kutscha (eds.) *Handbuch zum Recht der inneren Sicherheit* (Berlin: Berliner Wissenschafts-Verlag, 2006) 146-182

Goodman, M, "International Dimensions of Cybercrime" in S Gosh, E Turrini (eds) *Cybercrimes: A Multidisciplinary Analysis* (Berlin, Heidelberg: Springer-Verlag, 2010) 311-339

Graca, N, Quaresma, P, "How to Model Legal Reasoning Using Dynamic Logic Programming: A Preliminary Report" in D Bourcier (ed) *Legal Knowledge and Information Systems Jurix 2003: The Sixteenth Annual Conference* (Amsterdam: IOS Press, 2003) 163-172

Hansen, M, Pfitzmann, A, "Techniken der Online-Durchsuchung" in F Roggan (ed.), *Online-Durchsuchungen – Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008* (Berlin: Berliner Wissenschafts-Verlag, 2008) 131-157

Hayashi, M, "The Rules of Jurisdiction in Public International Law" in M Dunn, S F Krishna-Hensel, V Mauer (eds) *The Resurgence of the State: Trends and Processes in Cyberspace Governance* (Aldershot: Ashgate Publishing Ltd, 2007) 59

Heesen, C, Homburg, V, Offereins, M, "LACA: An Architecture For Legal Agents" in J C Hage, T J M Bench-Capon, M J Cohen, H J van den Herik (eds) *Legal Knowledge Based Systems JURIX '95: Telecommunication and AI & Law* (Lelystad: Koninklijke Vermande, 1995) 23-32

Hert, P de, "Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace – Whose Sovereignty is At Stake?" in B-J Koops, S Brenner (eds) *Cybercrime and Jursidiction – An International Survey* (The Hague: Asser Press, 2006) 107

Herzog, A, Shahmehri, N, "Usability and Security of Personal Firewalls" in H Venter, M Eloff, L Labuschagne, J Eloff, R von Solms (eds) *IPIP International Federation for Information Processing, Volume 232, New Approaches for Security. Privacy and Trust in Complex Environments* (Boston: Springer, 2007) 37-48

Hildebrandt, M, "A Vision of Ambient Law" in R Brownsword, K Yeung (eds) *Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes* (Oxford, Portland: Hart Publishing, 2008) 175

Hörnle, J, "The Jurisdictional Challenge of the Internet" in L Edwards, C Waelde (eds) *Law and the Internet* (3rd edition Hart publishing, 2009) 121

Hornung, G, Bendrath, R, Pfitzman, A, "Surveillance in Germany: Strategies and Counterstrategies" in S Gutwirth et al (eds.) *Data Protection in a Profiled World* (Berlin Heidelberg: Springer, 2010) 139-156

Huhns, M N, Holderfield, V T, Gutierrez, R L Z, "Achieving Software Robustness via Large-Scale Multiagent Systems" in C J Pereira de Lucena et al. (eds) *Software*

Engineering for Multi-Agent Systems II, Research Issues and Practical Applications (Berlin, Heidelberg: Springer Verlag, 2003) 199-215

Jennings, N, Wooldridge, M, "Applications of Intelligent Agents" in N Jennings, M Wooldridge (eds.) *Agent Technology: Foundations, Applications, and Markets* (Berlin, Heidelberg, New York: Springer, 1998)

Johnson, D R, Post, D, "And How Shall the Net be Governed? – A Meditation on the Relative Virtues of Decentralized, Emergent Law" in B Kahin, J H Keller (eds.) *Coordinating the Internet* (Cambridge, MA: MIT Press, 1997) 62-91

Jones, R, "Architecture, Criminal Justice, and Control" in L McAra, S Armstrong (eds) *Perspectives on Punishment: The Contours of Control* (Oxford: Oxford University Press, 2005) 471

Kaspersen, H W K, "Jurisdiction in the Cybercrime Convention" in B-J Koops, S Brenner (eds) *Cybercrime and Jursidiction – An International Survey* (The Hague: Asser Press, 2006)

Kementsietsidis, A, "Data Sharing and Querying for Peer-to-Peer Data Management Systems" in W Lindner et al. (eds) *Current Trends in Database Technology – EDBT 2004 Workshops* (Berlin, Heidelberg: Springer, 2004) 177-186

Kinny, D, Georgeff, M, Rao, A, "A methodology and modeling technique for systems of BDI agents" in Y Demazeau, J-P Müller, M Tambe (eds) *Agents Breaking Away: Proceedings of the Seventh Eurpean Workshop on Modelling Autonomous Agents in a Multi-Agent World, LNAI 1038* (Berlin: Springer, 1996), 56-71

Koen, R, Olivier, M, "An Evidence Acquisition Tool for Live Systems" in I Ray, S Shenoi (eds.) *IFIP International Federation for Information Processing*, Volume 285

Koops, B J, "Should ICT Regulation Be Technology-Neutral" in B J Koops, M Lips, C Priens, M Schellekens (eds.) *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, IT&Law Series Vol. 9, (The Hague, T.C.M. Asser Press: 2006), 77-108

Koops, B-J, Brenner, S, "Cybercrime Jurisdiction – An Introduction" in B-J Koops, S Brenner (eds.) *Cybercrime and Jursidiction – An International Survey* (The Hague: Asser Press, 2006)

Koops, B-J, "Criteria for Normative Technology – The Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values" in R Brownsword, K Yeung (eds) *Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes* (Oxford, Portland: Hart Publishing, 2008)

Kowalski, R A, "Legislation as Logic Program" in G Comyn, N E Fuchs, M J Ratcliffe (eds) *Logic Programming in Action* (Berlin, Heidelberg: Springer Verlag, 1992)

Kuhn, M G, "Optical Time-Domain Eavesdropping Risks of CRT Displays" (2002) *Proceedings IEEE Symposium on Security and Privacy*, 3-18

Kuhn, M G, Anderson, R J, "Soft Tempest: Hidden Data Transmission

Using Electromagnetic Emanations" in D Aucsmith (ed.), *Information Hiding* (Berlin, Heidelberg: Springer, 1998) 124-142

Kwan, Y K, Chiu, L L, Ip, W C, "Measuring Crimes Seriousness Perceptions: Methods and Demonstration" in K T Froeling (ed) *Criminology Research Focus* (New York: Nova Science Publishers, Inc, 2007) 7-19

Maat, E de, Winkels, R, "Automated Classification of Norms in Sources of Law" in E Francesconi et al. (eds) *Semantic Processing of Legal Texts* (Berlin, Heidelberg: Springer Verlag, 2010) 171

Mac Namee, B, Cunningham, P, "A Proposal for an Agent Architecture for Proactive Persistent Non-Player Characters" in D O'Donoghue (ed) *Proceedings of the 12th Irish Conference on AI and Cognitive Science* (Dublin: Trinity College Dublin, Department of Computer Science, TCD-CS-2001-20) 221-232

Mason, S, Schafer, B, "The Characteristics of Electronic Evidence" in S Mason (ed) *Electronic Evidence* (London: Lexis Nexis Butterworths, 2010)

Mason, S, "England & Wales" in S Mason (ed) *Electronic Evidence* (London: Lexis Nexis Butterworths, 2010)

Mason, S, "Authenticating Digital Data" in S Mason (ed) *Electronic Evidence* (London: Lexis Nexis Butterworths, 2010)

Mayfield, J, Labrou, Y, Finin, T, "Evaluating KQML as an Agent Communication Language" in M Wooldridge, J P Müller, M Tambe (eds.) *Intelligent Agents II (LNAI Volume 1037)* (Berlin: Springer, 1996) 347-360

Ogiela, L, "Syntactic Approach to Cognitive Interpretation of Medical Patterns" in C Xiong et al. (eds) *Intelligent Robotics and Applications: First International Conference, ICIRA 2008* (Berlin, Heidelberg: Springer, 2008) 456-462

Pollitt, M, "Applying Traditional Forensic Taxonomy to Digital Forensics" in I Ray, S Shenoi (eds)IFIP International Federation for Information Processing, Volume 285; *Advances in Digital Forensics IV* (Boston: Springer, 2008) 17-26

Richard, G, Roussev, V, "File System Support for Digital Evidence Bags" M Olivier, S Shenoi (eds) *Advances in Digital Forensics II* (New York: Springer, 2006)

Rotolo, A, Sartor, G, Smith, C, "Formalization of a 'Normative Version' of Good Faith" in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005), 65-76

Salomon, R, "Neural Networks in the Context of Autonomous Agents: Important Concepts Revisited" in C H Dagli et al. (eds) *Proceedings of the Artificial Neural Networks in Engineering (ANNIE'96)* (New York: ASME Press, 1996)

Sartor G, et al., "Norm Modifications in Defeasible Logic", in M-F Moens (ed.) *Proceedings of Jurix 2006* (Amsterdam: IOS, 2006) 13-22

Schafer, B, Rodriguez-Rico, M, Vandenberghe, W, "Undercover Agents and Agents Provocateur- Evidence Collection by Autonomous Agents and the Law", in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005) 155-170

Shearer, I, "Jurisdiction", in S Blay, R Piotrowicz, M Tsamenyi (eds.), *Public International Law – An Australian Perspective* (2nd edition, Melbourne: Oxford University Press, 2005)

Sieber, U, in T Hoeren, U Sieber (eds) *Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs* (München: Beck, 2000)
Siena, A, et al., "Designing Law-Compliant Software Requirements" in A H F Laender et al. (eds) *Conceptual Modeling – ER 2009, Lecture Notes in Computer Science* (Berlin, Heidelberg: Springer Verlag, 2009) 472-486

Smith, B, "Beyond Concepts: Ontology as Reality Representation" in A C Varzi, L Vieu (eds) Formal Ontology in Information Systems (Amsterdam: IOS Press, 2004) 73-84

Steinberger, H, "Sovereignty" in R Bernhardt (ed.), *Encyclopedia of Public International Law* (1987), Vol.10, 397

Sun, R, "Artificial Intelligence: Connectionist versus Symbolic Approaches" in N J Smelser, P B Baltes (eds.), *International Encyclopedia of the Social and Behavioral Sciences* (Pergamon/Elsevier, Oxford: 2001), 783-789

Tien, L, "Architectural Regulatioin and the Evolution of Social Norms"in J M Balkin, J Grimmelmann, E Katz, N Kozlovski, S Wagman, T Zarsky (eds) *Cybercrime: Digital Cops in a Networked Environment* (New York, London: New York University Press, 2007) 37-58

Uzunay, Y, Incebacak, D, Bicakci, K, "Towards Trustable Digital Evidence with PKIDEV: PKI Based Digital Evidence Verification Model" in A Blyth, I Sutherland (eds.) *EC2ND 2006: Proceedings of the Second European Conference on Computer Network Defense, in conjunction with the First Workshop on Digital Forensics and Incident Analysis* (London: Springer, 2007), 105

Vitek, J, Serrano, M, Thanos, D, "Security and Communication in Mobile Object Systems" in J Vitek, C Tschudin (eds) *Mobile Object Systems: Towards the Programmable Internet* (Springer-Verlag, LNCS 1222: 1997) 177-201

Wall, David S "The Internet as a Conduit for Criminal Activity" in A Pattavina (ed) Information Technology and the Criminal Justice System (London: Sage Publications, 2005) 77-98

Weber, W, Rabaey, J, Aarts, E, "Introduction" in W Weber, J Rabaey, E Aarts (eds) *Ambient Intelligence* (Berlin, Heidelberg, New York: Springer, 2005)

Weigand, H, Dignum, V, "I am Autonomous, You are Autonomous" in M Nickles, M Rovatsos, G Weiss (eds) *Autonomy 2003, LNAI 2969* (Berlin, Heidelberg: Springer, 2004)

Wettig, S, Zehedner, E, "The electronic agent: a legal personality under German law?" in A Oskamp, E Weitzenbök *The Law and Electronic Agents (LEA 2003)* (Unipub, Oslo: 2003) 97-113

Werbos, P J, "ADP Design to Replicate/Understand Brain Intelligence" in L I Perlovsky, R Kozma, *Understanding Complex Systems* (Berlin, Heidelberg: Springer Verlag, 2007) 119

Wieringa, R J, Meyer, J-J Ch, "Applications of Deontic Logic in Computer Science: A Concise Overview" in J-J Ch Meyer, R J Wieringa (eds) *Deontic Logic in Computer Science* (Chichester: Wiley, 1993) 17

Zadeh, L A, "Preface" in R J Marks (ed) *Fuzzy Logic Technology and Applications* (New Jersey: IEEE Press, 1994) xvii

Zagaris, B, "United States Treaties on Mutual Assistance in Criminal Matters" in M C Bassiouni (ed) *International Criminal Law: Multilateral and Bilateral Enforcement Mechanisms* ((Leiden, Netherlands: Martinus Nijhoff, 2008), 385

Working Papers and Reports

Bond, M, Danezis, G, "A pact with the Devil" (2006) Technical Report 666, *University of Cambridge*, available online at http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-666.pdf

Carrier, B, "Open Source Digital Forensics Tools: The Legal Argument" (2002) *@stake Research Report*

Falliere, N, Murchu, L O E Chien, "W32.Stuxnet Dossier" (2011) Symantec, available online at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Gilbert D, et al., "IBM Intelligent Agent Strategy", (1995) White Paper, IBM Corporation.

GFI, "The corporate threat posed by email trojans" Whitepaper, available online at http://www.gfi.com/whitepapers/network-protection-against-trojans.pdf

Ingham, K, Forrest, S, "A History and Survey of Network Firewalls" (2002) *Technical Report 2002-37, University of New Mexico Computer Science Department*, 1-42, 2, available online at http://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf.

Kanger, S, "New Foundations For Ethical Theory", (1957) *Technical Report, Stockholm Unversity*

Messagelabs, "Targeted Trojans: A New Online Threat to Businesses", Whitepaper, available online at http://www.google.com/url?sa=t&source=web&ct=res&cd=6&url=http%3A%2F%2Fwww.messagelabs.com%2Fdownload.get%3Ffilename%3DUS_WP_Targeted%2520Trojans_Associate.pdf&ei=aIaWSsyFM4LQ-

Qaz4tjOCQ&usg=AFQjCNGjGTn2XMhBq2Dt65nCb55_Rc8keQ&sig2=4dX_SI0DAOV36J_3sq7MBQ

Knowledge Computing Corporation, (2004) *The COPLINK Whitepaper*, 2004/3

Zwanenburg, M, Boddens Hosang, H, Wijngaards, N, "Humans, Agents and International Humanitarian Law: Dilemmas in Target Discrimination" in A Oskamp, C Cevenini (eds) *The Law and Electronic Agents: Proceedings of the LEA 04 workshop* (Nijmegen: Wolf Legal Publishers, 2005) 45-51

Policy Reports and Recommendations

ACPO, "Guide for Computer-Based Electronic Evidence" available online at http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf
Bundesamt für Sicherheit in der Informationstechnik, Leitfaden "IT-Forensik", Version 1.0 (September 2010) available online at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile

Computer Crime and Intellectual Property Section, US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Office of Legal Education Executive Office for United States Attorneys, 2009)

Kleine Anfrage Deutscher Bundestag, "Online-Durchsuchungen" (2007) *Deutscher Bundestag Drucksache* 16/4795

Kleine Anfrage Deutscher Bundestag, "Bilanz der Online-Durchsuchung" (2010) *Deutscher Bundestag Drucksache* 17/1629

Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow, October 1999, at http://www.g7.utoronto.ca/adhoc/crime99.htm

The Law Commission (Consultation Paper No 141), *Criminal Law-Evidence in Criminal Proceedings: Previous Misconduct of a Defendant-A Consultation Paper* (1996) [6.7]-[6.9], available at http://www.lawcom.gov.uk/docs/cp141.pdf

The Law Commission (Consultation Paper 190), *The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales: A New Approach to the Determination of Evidentiary Reliability* (2009)

Appendix: Interview Questions

Overarching Questions:

1. What are the existing technology-based investigative measures for the policing of the Internet?

2. Has the remote online searching of ICTs been introduced in the respective country?

3. Did the respective government play a role in adopting the technology-based investigative measures?

4. What were the reasons for developing the technology-based investigative measures in the respective countries?

Detailed Technical Questions:

1. What are the technologies underlying the new software-based investigative tools for the policing of the Internet?

2. What are the technical details of the software used for online searches of ICTs (if this measure has been adopted in the country)?

3. Is the online searching of ICTs technically feasible?

4. What other technical investigative measures are currently feasible?

5. Is it technically feasible to infiltrate a specific ICT device of a suspect?

6. What are the capabilities of investigative software (and in particular software used for online searches of ICTs)?

7. What is the degree of autonomy of these software-based investigative tools?

8. Is the software capable of functioning without a human operator?

9. How much in known about these software tools in the hacking community?

10. What counter-measures are generally possible, and are any being discussed in the hacking community?

11. Is it possible to circumvent commercial protection software (anti-virus software, firewalls etc) with these investigative tools?

12. Will the target system be compromised by the infiltration with the investigative software and investigative actions?

13. What are the security concerns of the use of software-based investigative tools? For example, could third parties detect and utilise such tools?

14. Did the government and other organisations and institutions play a role in the development of these software-based investigative tools?

15. Who is financing the development of these software tools?

16. Who evaluates the results of these measures?

17. What are the experiences with the adopted measures?

18. What are the future technologies to be deployed?

Detailed Legal Questions:

1. How are the software-based investigative measures regulated, if at all?

2. Are these measures based on a valid legal basis?

3. Was new legislation introduced to regulate these new software-based investigative measures?

4. Was any case law generated dealing with the introduction and use of these new investigative measures?

5. What are the greatest legal concerns linked to the use of these software-based investigative tools?

6. What are the greatest legal concerns connected to the online searching of ICTs?

7. How are legal practitioners classifying these tools?

8. How is the evidence seized by these tools classified?

9. Who is involved in the regulation of these tools?