كلية التدريب

قسم البرامج التدريبية

الأساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية

إعداد

اللواء.د. محمد الأمين البشرى

المستشار بوزارة الداخلية ـ دولة الإمارات العربية المتحدة

محاضرة مقدمة في الحلقة العلمية

(تحليل الجرائم المستحدثة والسلوك الإجرامي)

المنعقدة خلال الفترة من ١٣ ـ ١٤٣٢/٢/١٥هـ الموافق ١٧ ـ ٢٠١١/١/١٩م

بمقر الجامعة

١٤٣٢هـ ـ ٢٠١١م

الطبعة الأولى
٢٠١١

المحتويـات

مقدمة

العناصر الرئيسية والمحتوى العلمي لهذه الورقة من مستلات بحث موسع نفذه الباحث مع نخبة من أساتذة جامعة شيبا اليابانية كان موضوعه: الجرائم السايبرانية بمنظور عالمي Cyber Crimes in a Global Perspective،وذلك خلال عامي ٢٠٠٨-٢٠٠٩، بدعم من Japan Foundation Intellectua Scholarship Program.

وقد قدم البحث الذي أعدت معظم أجزائه باللغة اليابانية في سلسلة محاضرات في كلية القانون والاقتصاد بجامعة شيبا ،كما تمت مناقشته في سمنارات نظمتها الجمعية اليابانية لقانون المعلومات في قاعة جامعة هوكايدو اليابانية خلا أبريل ٢٠٠٩.

يُعد هذا البحث مساهمة في الجهود المبذولة لمواجهة ظاهرة الجرائم المستحدثة المرتكبة بوسائل التقنية العالية التي أصبحت تعرف الآن بالجرائم السايبرانية، ومعالجة جوانبها القانونية وإجراءات التحقيق والإدعاء والمحاكمة ومعاملة المدانين فيها ، وكيفية التعامل مع أطرافها داخل نظام العدالة الجنائية التقليدي وذلك بهدف تحفيز المهتمين بهذا الميدان على التعمق في مثل هذه الدراسات وطرح الحلول.

في البدء كان البعض يعتقد أن التعامل مع الجرائم السايبرانية لا يختلف عن غيرها من الجرائم ، إلا أن تطور هذا النوع من الجرائم أقنع الكثيرين بأهمية التخصص والمهنية، بل جعلنا نذهب أبعد من ذلك بالدعوة إلى إنشاء نظام خاص للعدالة، يعرف بنظام العدالة الجنائية الإلكتروني، يعنى بالجرائم السايبرانية ومرتكبيها وضحاياها ، في سياق الحوسبة الشاملة لعمليات نظام العدالة الجنائية.

يتناول هذا العمل الجرائم المستحدثة ذات الطابع السايبراني بالتعريف وبيان تشريعاتها الموضوعية والشكلية ، مع التركيز على الأساليب العلمية اللازمة لإكتشافها والتحقيق و التعامل مع الجناة فيها داخل نظام العدالة الجنائية.و تنقسم الورقة إلى فصلين، الفصل التمهيدي الذي يتناول موضوع البحث وأهدافه وبيان المصطلحات، والفصل الثاني الذي يتناول التعامل مع الجرائم السايبرانية المستحدثة في مختلف مراحل عمليات نظام العدالة الجنائية.

الفصل الأول
تمهيد

١,١ - موضوع الحث و أهدافه

تشكل ظاهرة الجرائم السايبرانية المستحدثة – التي نحن بصددها – تحديا حقيقيا للسياسات الجنائية السائدة و أجهزتها التشريعية و التنفيذية و القضائية. نحن اليوم أمام سيل من أنماط الجرائم التي لانجد لها نصوصا قانونية، موضوعية كانت أم شكلية، في كثير من التشريعات الجنائية ، خاصة في الدول العربية، مما غل أيدي القائمين على أجهزة العدالة الجنائية في إتخاذ الإجراءات الرادعة حيال كثير من الممارسات المستحدثة.

هذه محاولة لإلقاء الضوء على مسألة الجرائم السايبرانية المستحدثة والأساليب العلمية اللازمة للتعامل معها شكلا و موضوعا من قبل أجهزة الشرطة والنيابة

و القضاء، ومرحلة تنفيذ الأحكام ، ونولي عناية خاصة لمراحل التحقيقات الأولية و جمع الإستدلالات ، بإعتبارها أكثر المراحل تعقيدا.

إن انتقال الجرائم التقليدية إلى طابعها العلمي المستحدث الذي يُسخر التقنيات العالية والذكاء الاصطناعي والمعلومات الرقمية في التخطيط والتنفيذ والقضاء على آثار الجريمة ، لا يشكل معضلة قانونية حقيقية من حيث التجريم والعقاب أو من حيث تصنيف الأنماط وتحديد العناصر والأركان كما يعتقد البعض فحسب، بل تكمن المعضلة الحقيقية التي تفرزها ظاهرة الجرائم المستحدثة في صعوبة عمليات الرصد والمتابعة وتعقيدات الاكتشاف والضبط ومخاطر جمع الأدلة والتحقيق مع فئة المجرمين الأذكياء ، بجانب ضعف التشريعات الشكلية وتخلف القواعد العامة للبينة.

لا تقتصر أهمية موضوع الدراسة على أهمية التعامل العلمي مع هذه الظاهرة و علاقتها بالعدالة الجنائية و حماية حقوق الإنسان فحسب، بل هنالك عوامل عديدة تضاعف من اهمية مثل هذه الموضوعات منها :

- سرعة وإستمرارية التطور في ميدان التكنولوجيا و تقنية المعلومات و الإتصالات .
- اهتمام المجتمعات المعاصرة بظاهرة الجرائم السايبرانية المستحدثة ، لأنها تمس – في الغالب – مصالح أكثر من مجتمع وأكثر من دولة ، إذ أن الأطراف المنفذة للجريمة والأطراف المتضررة منها تضم رعايا دول ومؤسسات متعددة الجنسيات ، أي إنها جريمة عالمية.

- الحاجة الى معالجة مشكلات الإختصاص في التعامل مع الجرائم ذات الطابع السايبراني الدولي .
- إتجاه المجتمع الدولي نحو تعميم الاتفاقية الدولية لمكافحة الجريمة السايبراتية لسنة ٢٠٠٣

- ضرورة مساعدة القائمين على اكتشاف الجرائم وضبط المجرمين وفرق التحقيقات على أداء واجباتهم بأساليب علمية تلائم مستجدات الإجرام المعاصر. وينبغي في البدء التأكيد على قواعد أربعة يتطلبها التعامل مع الجرائم المستحدثة وهي:

أولاً: التركيز على التخصص في معالجة الجرائم السايبرانية المستحدثة ، بحيث تكون لكل نمط من أنماط الجرائم السايبرانية المستحدثة فرقًا متخصصة تتفرغ لرصدها وحصر وسائل ارتكابها وطرق اكتشافها.

ثانيـًا: الارتقاء بالمستوى التعليمي للعاملين في مجال التحقيقات الجنائية ومواصلة التدريب والتأهيل بالقدر الذي يمكنهم من مواكبة المتغيرات والتزود بالعلوم الحديثة.

ثالثـًا: الرصد المبكر للجريمة المستحدثة والأشخاص المحتمل تورطهم فيها وذلك عن طريق جمع أكبر قدر من المعلومات الجنائية والاجتماعية وحسن تحليلها وإعدادها للاستفادة منها عند الضرورة.

رابعـًا:بناء قنوات تبادل المعلومات مع أجهزة الشرطة والأمن في الدول الشقيقة والصديقة وحسن استغلال تلك القنوات.

خامسًا:تطوير وتحديث قوانين الإجراءات الجنائية ، قواعد البينة ، القوانين المنظمة لسلطات رجال الشرطة والنيابة العمومية والقضاء والسجون ، بالقدر الذي يحقق أهداف التعاون والتنسيق مع الأجهزة المماثلة في الدول الأجنبية ، ويستوعب متطلبات الأدلة الجنائية العلمية والتقنية.

٢,١ - مفهوم الجرائم المستحدثة وابعادها

عبارة الجرائم المستحدثة عبارة فنية كثر تداولها في الدول العربية في التسعينات مع انتشار أنماط جديدة من الجرائم التي لم تكن مألوفة من قبل.. ومن مرادفات عبارة الجرائم المستحدثة ، عبارة الجرائم المعاصرة وعبارة المشكلات الأمنية المعاصرة أو الإجرام المعاصر .

إذاً ، عبارة الجرائم المستحدثة ليست عبارة أو مصطلحًا قانونيًا يُحدد أركان وعناصر جريمة معينة يطالها القانون. بل هي عبارة تصف أنماط مختلفة من الجرائم لا يجمع بينها سوى حداثتها من حيث الأساليب والأدوات المستعملة في تنفيذها. وعلى هذا النحو يعرِّف البعض عبارة الجرائم المستحدثة بأنها أنماط من الجرائم التي لم يألفها المجتمع في السابق ، من حيث أسلوب ارتكابها ونوع الجناة فيها وحجمها. ويعِّرفها البعض الآخر بأنها الجرائم المخطط لها والتي يستعين المجرمون عند تنفيذها من معطيات العلم الحديث . وتميل فئة ثالثة من الكتاب إلى تعريف الجرائم المستحدثة بحصر جرائم بعينها واشتراط استخدام التقانة الحديثة من أجل تسهيل تنفيذها وإخفاء معالمها.

إن العنصر المشترك في تعريفات الجرائم المستحدثة الواردة أعلاه هو استخدام التقنيات العالية والمتجددة تباعًا High-technology في تنفيذ جرائم تقليدية كانت معروفة من قبل. فالاستحداث عائد إلى الوسيلة وأسلوب ارتكاب الجريمة. إذ أن جرائم القتل ، الإرهاب ، الاتجار في المخدرات وإخفاء عائداتها أنشطة إجرامية عرفت منذ القدم. إلا أن المستحدث هو استخدام العلوم والتقانة الحديثة

في التخطيط والتنفيذ وإخفاء معالم الجريمة Oldest crimes committed in new ways[1] .

كما أنه من الصعب القول بحداثة إحدى التقنيات العالية ، طالما كانت أمامنا تقنيات عالية تولد كل يوم وكل ساعة.

ونحن بصدد الحديث عن أساليب التعامل مع الجرائم السايبرانية المستحدثة، علينا أن نركز علي العنصر الرئيس لهذا النوع من الجرائم ، ألا وهي تقنيات المعلومات والاتصالات والشبكات العنكبوتية التي تشكل البيئة الخاصة بأخطر أنماط الجرائم المستحدثة ، والتي أجمع المجتمع الدولي على تسميتها بالجرائم السايبرانية وإعتمد للتعامل معها إتفاقية دولية. . وتتجه معظم التشريعات والاتفاقيات الدولية إلى التركيز على جرائم السايبرانية Cyber Crimes،والتي تنقسم إلى جرائم سايبرانية عادية و جرائم السايبرانية الفضائية Cyber Space Crimes ، لأسباب عدة منها ما يلي(١):-

- جرائم السا يبرانية هي الجرائم الأكثر خطورة وتعقيدًا.
- طابعها الافتراضي Virtual Crime المتد على مساحات جغرافية غير محدودة، يثير تساؤلات قانونية يصعب الإجابة عليها في ظل الفكر التقليدي للقانون الجنائي.
- تنتشر على نطاق واسع من الشبكات العالمية والمحلية Wide Area Network.

---

[1] [1] John R . Vacca , Computer Forensic (2.nd ed) . Massachusetts , Charles River Media , 2005 . p.737

(1) **John Pratt and Peter Grabosky, Crime in the Digital Age: Controlling Telecommunications and Cyber Space Illegalities, Sydney, Federation Press, 1998.**

- يصعب ملاحقة الجناة فيها والحصول على الأدلة بسبب مسرحها الافتراضي virtual scene of crime
- مازالت التشريعات عاجزة عن مواكبتها.

يصعب التعامل معها بواسطة نظم و أجهزة العدالة الجنائية التقليدية ، لإمتدادها خارج دائرة الإختصاص وعبر الحدود الدولية. فما هي الجرائم السايبرانية؟ ومن أين جاءت هذه العبارة التي طغى إستخدامها على المصطلحات الأخرى ذات العلاقة بالجرائم السايبرانية؟

٣.١ – تعريف الجرائم السايبرانية

وفقاً لقاموس أكسفورد Illustrated Oxford Dictionay عبارة سايبر cyber هي أداة مقدمة Prefix توضع في بداية الكلمات التي تتعلق بشبكة الاتصالات الإلكترونية أو الصورة أو البيئة الناتجة عن البرامج الحاسوبية التي تمكن المستخدم من التعامل مع حقائق افتراضية Cyber is a prefix forming words related to electronic communication networks and virtual reality .

عليه ، فإن إضافة عبارة سايبرانية إلى عبارة جريمة ،تنقلها من طبيعتها التقليدية إلى نمط جديد يتعلق بالإتصالات الإلكترونية وشبكاتها والبرامج الحاسوبية التي تمكن الجاني من التعامل مع الحقائق الإفتراضية المحيطة بالجريمة. و يعرف القاموس المذكور الحقيقة الإفتراضية بانها الصورة أو البيئة التي تعدها البرامج الحاسوبية المستخدمة.

يجمع البعض كافة الجرائم و الأنشطة الضارة التي تتعلق بالحاسب الآلي ونظم المعلومات والاتصالات في مصطلح الجريمة السايبرانية Cyber Crime و الجريمة السايبرانية الفضائية Cyber Space Crimes.

ومن أكثر التعريفات شيوعًا لمصطلح الجريمة السايبرانية ما يلي:-

"هي أية جريمة تُرتكب بمساعدة تقنيات الحاسب الآلي والاتصالات بغرض التأثير على وظيفة الحاسب الآلي أو نظامه"

"Cyber Crime is any Crime Committed with the help of Computer and Telecommunication Technology with the purpose[i] of Influencing the Functioning of Computer or Computer System.[1]

في ضوء ما تقدم،ولأغراض هذه الدراسة فقد رأينا الأخذ بمصطلح الجرائم السايبرانية المستحدثة لدلالتة الواسعة وإنسجامه مع المصطلحات السائدة في المعاملات اليومية وعمليات الحكومة الإلكترونية،التجارة الإلكترونية،الأبواب الإلكترونية،الرقابة الإلكترونية والبريد الإلكتروني وغيرها.

وينبغي هنا التأكيد على حقائق ثلاثة تفيد كثيرا في البحث و التحقيق والتعامل مع الجرائم السايبرانية وهي:

أولا : أكثر المساحات الإفتراضية التي قد تنمو فيها الجرائم السايبرانية هي:-

١. بيئة شبكات الإنترنت والإنترانت.
٢. قواعد البيانات للمؤسسات المالية.
٣. البريد الإلكتروني.

[1] Mishera,R.C.Cyber Crime lmpact in the New Millenrium . Delhi : Saujanya Books , 2005

٤. النقود الإلكترونية.

٥. الأعمال الإلكترونية.

٦. التجارة الإلكترونية.

٧. الأسهم والسندات.

٨. الأنظمة الأمنية الحساسة.

٩. نشر الفيروسات.

١٠. الإرهاب الإلكتروني.

ثانيا : هناك إجماع حول المنظور العالمي للجريمة السايبرانية من حيث[1] :-

- طبيعتها.
- نطاقها.
- إرتباطها بالشبكات الدولية
- أثرها على الاقتصاد العالمي.
- تأثيرها على التنمية.
- علاقتها بالجرائم المستحدثة كالإرهاب ، الجريمة المنظمة ، غسل الأموال ، التهرب الضريبي والاتجار بالبشر.
- قابليتها للانتشار السريع .

---

(1) **Collin Barry. The Future of Cyber Terrorist: Chicago University Press, 1999.**

ثالثا: ضرورة إخضاعها للمعاهدات والاتفاقيات الدولية و الإقليمية لتوحيد القوانين المنظمة للعمليات الإلكترونية وتجريم ومعاقبة الأنشطة الإلكترونية الضارة وإجراءات التعامل مع الجرائم السايبرانية العابرة للحدود،خاصة فيما يتعلق بالأدلة الجنائية وقواعدها .

ويعزى تزايد مخاطر هّذا النوع من الجرائم لأسباب عدة ومن أهمها ما يلي:

١. اتساع نطاق المعاملات الإلكترونية في بيئة الأعمال التجارية والمعاملات اليومية في القطاعين العام والخاص.

٢. الثقة والاعتماد المفرط على تقنيات الحاسب الآلي في أعمال تتصل بصحة الإنسان وحياته اليومية.

٣. انتشار ظاهرة سوء استخدام تقنيات الحاسب الآلي وشبكات الإنترنت وصفحات المواقع العالمية، مثل نشر الفيروسات الضارة والصور الفاضحة وتعميم المعلومات الإرهابية وإفشاء أسرار أسلحة الدمار الشامل.

٤. عدم الاستقرار السياسي والأمني في العالم مما يضاعف احتمالات الاعتداء على البنيات التحتية العالمية لنظم المعلومات والاتصالات ، خاصة في الدول المتقدمة التي تعتمد كثيرا على التقنيات العالية.

٥. توفر فرص القرصنة وسرقة المعلومات الشخصية والاعتداء على الحريات الخاصة من خلال شبكات الإنترنت.

٦. عدم مواكبة أجهزة وتشريعات نظام العدالة الجنائية التقليدي.

٧. صعوبة اكتشاف الجرائم السايبرانية وضبط الجناة فيها.

٨. صعوبة التحقيق والإدعاء والمحاكمة في الجرائم السايبرانية.

٩. جهل ضحايا الجرائم السايبرانية بطبيعتها.

إن مواكبة هذه التغيرات التقنية التي بدأت تهيمن على حياة الإنسان ومعاملاته ، واحتمالات نمو هذا الاتجاه في المستقبل، بايجابياته وسلبياته، تلزم المعنيين بمكافحة الجريمة والمدراء والمشرفين على أعمال مختلف الأنشطة الحكومية والأهلية القيام بما يلي:-

١. التعرف وتعريف العاملين تحت إمرتهم بالبيئة العالمية للمعلومات Global Information Environment ، التي تفرز الجرائم السايبرانية.

٢. العمل على تطوير تشريعات مكافحة الجرائم السايبرانية، بشقيها الموضوعي و الشكلي

٣. وضع برامج توعوية خاصة للوقاية من الجرائم السايبرانية.

٤. مراجعة قواعد البينة وتطوير قواعد خاصة للأدلة الرقمية لمواكبة الجرائم السايبرانية.

٥. التعرف على الجرائم ذات العلاقة بالحاسب الآلي وشبكات الإنترنت وصفحات المواقع العالمية بأنماطها المختلفة وفق المفاهيم المعتمدة في الدول المتقدمة التي تسيطر على تقنياتها .

٦. إستحداث نظم للعدالة الجنائية الإلكترونية للتعامل مع الجرائم السايبرانية والمجرم السيبراني.

٧. تعزيز التعاون الإقليمي و الدولي وتطوير آليات التعامل مع الجرائم السايبرانية عبر الوطنية.

٨. اختيار وتأهيل وتدريب موارد بشرية متخصصة، في اكتشاف الجرائم السايبرانية والتحقيق فيها والتعامل مع الأدلة الرقمية في جميع مراحل عمليات العدالة الجنائية.

٤,١ - أبعاد الجرائم السايبرانية

تتجه المجتمعات المعاصرة نحو مرحلة جديدة من مراحل نموها الاجتماعي والاقتصادي، مصحوبة بأنماط سلوكية مستحدثة تسندها المعلومات والبيانات الالكترونية المنقولة عبر الفضاء. ومن المؤكد أن العالم مقبلٌ على أكثر وأخطر مما نشهده اليوم بفضل تطور البيئة العالمية للتقنية العالية للمعلومات Global High Technology Environment التي يعيش فيها الإنسان المعاصر. فالحاسب الآلي كمحور لهذه البيئة لم يعد استخدامه قاصرًا على الميادين العلمية والحسابية البحتة ، بل أصبح الحاسب الآلي وتقنياته الحديثة عنصرًا أساسًا في كافة المعاملات والأنشطة التي يقوم بها الإنسان.

تشير الإحصاءات إلى ارتفاع عدد مستخدمي الإنترنت في العالم من (٤٠٠) مليون شخصا عام ٢٠٠٠ إلى (١,٦) مليارشخصا في عام ٢٠٠٨ ،أي بزيادة قدرها (٣٤٢٪) بينما تقدر الأموال المتحركة عبر شبكات الإنترنت بمبلغ (٤١٢,٧) بليون دولار[1]. وكل ذلك يفتح مساحات واسعة للجرائم الإلكترونية خاصة في مجال الجرائم الاقتصادية. في الولايات المتحدة الأمريكية وحدها – على سبيل المثال – سجل مركز شكاوى جرائم الإنترنت (IC3) خلال عام ٢٠٠٦ (٢٠٧٤٩٢) جريمة غش منها (٧٣ر٩٪) عبر الإنترنت و (٣٦٪) من خلال صفحات المواقع العالمية.

وتتعدد أنماط الجرائم السايبرانية بتعدد مجالات استخدام الحاسب الآلي وتقانة المعلومات والاتصالات ، وهي مجالات يصعب حصرها الآن ، ناهيك عن المستقبل القريب الذي من المؤكد أن تكون فيه تقنية المعلومات والاتصالات الإلكترونية هي الحاكمة لكافة المعاملات والأنشطة اليومية. ومن المتوقع أن تتطور تقنيات المعلومات والاتصالات وأجهزة الحاسب الآلي بسرعة لا يمكن قياسها. ولا غرابة أن تنتشر

(1) Millen Nikolov "The Destructive Effect of Electronic Hacking", Symposium on Social and Security Impact of Internet, Abu Dhabi, Center for Police Research and Studies, 2006.

وتتعدد أنماط الجرائم السايبرانية المصاحبة لهذه الثورة التكنولوجية بذات السرعة وفي مختلف الاتجاهات. الأمر الذي يقتضي التعرف على أنماط تلك الجرائم والوقوف على أبعادها واتجاهاتها .

هنالك صعوبات عديدة ومتجددة تواجه القائمين على المتعامل مع الجرائم السايبرانية من حيث اكتشافها والتحقيق وجمع الاستدلالات اللازمة لإثباتها وكيفية مباشرة إجراءات الدعوى الجنائية فيها أمام المحاكم، ومعاملة المدنبين فيها لأسباب عدة أهمها :

١. جهل ضحايا الجرائم السايبرانية من المؤسسات والهيئات والأفراد بطبيعة الجريمة التي ارتكبت في حقهم ، وعدم قدرتهم على اكتشاف التضرر وحجمه في الوقت المناسب .
٢. الذكاء والقدرات العلمية التي يتميز بها مرتكبو الجرائم السايبرانية .
٣. عدم توفر مختبرات الأدلة الجنائية الرقمية وبرامج الأدلة الاصطناعية Artificial evidence وخبراء البحث التقني القانوني للحاسب الآلي Computer forensic experts .
٤. تخلف العاملين في أجهزة العدالة الجنائية في مجال علوم الحاسب الآلي والتقنيات العالية.
٥. وقوع الجريمة الإلكترونية بجهد أقل بالقدر الذي يقلل من فرص الاكتشاف رغم أنها تسبب آثاراً كبيرة E-crime requires minimal effort for maximum impact.
٦. امتداد الجريمة على نطاق واسع ومجالات غير محددة جغرافياً أو سياسياً cyber crime is borderless
٧. ضعف الشراكة الدولية والإقليمية في التعامل مع الجرائم السايبرانية .
٨. انتقال آليات الجرائم السايبرانية إلى مجال الجرائم التقليدية

٩. تنوع أنماط الجرائم السايبرانية بالقدر الذي يجعل النصوص القانونية تقف عاجزة عن مواكبتها ومنها على سبيل المثال:

١ – اختراق نظم الاتصال لأبراج المراقبة الجوية واعطاء أوامر من شأنها تسبب كوارث جوية .

٢ – استخدام بطاقات ائتمان مزورة لتمويل العمليات الإرهابية .

٣ – اختراق النظم المصرفية وتحويل الأموال .

٤ – تزييف العملات .

٥ – استخدام الهاتف النقال للإنترنت بأسماء مشفرة .

٦ – إرسال فيروسات تعطل نظم المعلومات الحكومية .

٧ – الدخول على أنظمة المستشفيات وتعديل بيانات المرضى بما يسبب الوفاة (جرعات علاج أعلى)

٨ – اختراق أنظمة الدولة واعطاء أوامر بإصدار شيكات أو تمويل أموال للأفراد مما يضر الاقتصاد القومي .

٩ – إتلاف نظم الضرائب الحكومية .

١٠ – التلاعب بنظم القطارات السريعة مما يؤدي إلى الاصطدامات .

١١ – الاستيلاء على نظم الاتصالات أو تعطيلها .

١٢ – الاستيلاء على الاتصالات الفضائية ونشر بيانات مضللة .

١٣ – الاعتداءات السياسية الإلكترونية Political cyber attacks

١٤ – اختراق وتتبع أنظمة الحكومات Mapping government systems

١٥ – ميدان الحروب الرقمية digital battle field

١٠- مسألة الاختصاص في الجرائم السايبرانية:

من الملاحظ أن التواصل بين الأمم والشعوب ، عبر الإنترنت ومؤتمرات الفيديو Video Conferencing والمؤتمرات الهاتفية Teleconferencing يتقدم بشكل سريع في مختلف المعاملات بين الإفراد والجماعات داخل الدول وعبر الحدود.[1] وقد ترتب على ذلك أن العقود والاتفاقيات المبرمة والسلع والأموال المتبادلة ، وما يصاحبها من أنشطة إجرامية لا نجد لها في الفقه المعاصر وأحكام القضاء معالجات لمسائل الاختصاص عليها. في النظام القانوني التقليدي استقر الفقه على أن أي نشاط يتم بين طرفين في إقليم معين يخضع إما لقانون الدولة التي تم فيها النشاط أو لقانون الدولة التي تتفق عليها الأطراف المشاركة في النشاط. وإذا كان النشاط عملاً إجراميًا فإنه يخضع لأحكام قانون الدولة التي وقعت فيها الجريمة.

أجريت دراسات فقهية محدودة حول مسائل الاختصاص في الجرائم السايبرانية في بعض الدول المتقدمة مثل فرنسا ، أستراليا ، كندا واليابان دون أن تستقر على مبادئ راسخة أو موجهات عامة. غير أننا نجد دراسات فقهية أكثر عمقًا حول مسائل الاختصاص في الولايات المتحدة الأمريكية التي شهدت ساحات محاكمها العديد من النزاعات حول المعاملات الإلكترونية.

نظرت الدائرة السادسة لمحكمة الاستئناف في الولايات المتحدة الأمريكية العديد من القضايا المتعلقة بمسائل الاختصاص في المعاملات الإلكترونية ، وأصدرت أحكامًا وصفت بأنها جاءت مواكبة للمتغيرات ، إذ أقرت المحاكم الأمريكية في وقت مبكر اختصاصها على إنشاء موقع على الشبكة الدولية World Wide Web الذي يمكن الدخول عليه بواسطة أي شخص في دائرة اختصاص المحاكم

[1] I Cove . David and William Von Storch . Computer Crime : Crime Fighters Hand book . CA : Reilly Association . 2001

الأمريكية . وبذلك أصبحت المحاكم الأمريكية تميل بصفة عامة إلى اعتماد اختصاصها على المنازعات الإلكترونية المدنية والجرائم السايبرانية متى توفرت أدلة تثبت وجود علاقة بينها وبين مخالفة القوانين الأمريكية التي تتطلب استيفاء شروط خاصة تعرف بشروط اختصاص اليد الطولي Long arm Jurisdiction. وقد تبلور هذا المفهوم المستحدث بصورة واضحة في تفسيرات قانون تقنية المعلومات الهندي لسنة ٢٠٠٠.

في تأكيد لاتجاه الفقه المعاصر نحو مفهوم الاختصاص الإقليمي الإضافي في قضايا التقنيات الإلكترونية ، يطرح "جونسون وبوست"[١] مناقشة مبررة لمسألة الاختصاص في الجرائم والمعاملات الإلكترونية وهما يتوقعان تفاقم مشكلة الاختصاص ، مع اتساع نطاق الاتصالات الإلكترونية المتحركة الناجم عن انتشار استخدام الإنترنت بالهاتف المتحرك مما يجعل مكان النشاط الإلكتروني نشاطًا متحركًا يصعب تحديد موقعه الجغرافي. وبناءً على ذلك ينادي "جونسون وبوست" بإنشاء نظام للاختصاص خاص بالمعاملات والجرائم السايبرانية متوازي لنظام الاختصاص التقليدي ، ومدى علاقة النشاط الإجرامي بالأقاليم والأراضي الخاضعة لاختصاص المحاكم الأمريكية.

- حاولت بعض المحاكم الأمريكية تطبيق المفاهيم التقليدية للاختصاص على المعاملات الإلكترونية داخل الولايات المتحدة ، مما أفرز نتائج غير عادلة أو مدمرة في بعض الأحيان. كما رأت محاكم أخرى أن مرور الاتصالات الإلكترونية عبر الأراضي الأمريكية لتحدث نتائجها الضارة على حياة الناس في مناطق خارج الولايات المتحدة ، مدعاة للتقليل من شأن القانون الأمريكي ، الأمر الذي يقتضي

[1] Davicl . R. Johnson and David , G.Post . Law and Boarders . the Rise of law in cyber Space . London Bh72002,

التوسع في مفهوم اختصاص المحاكم الأمريكية فيما يتصل بالتقنيات الإلكترونية فيما يُعرف بالاختصاص الإقليمي الإضافي Extra – territorial Jurisdiction. ويشكل كل ذلك مسائل جديدة في فقه القانون الجنائي تحتاج الى دراسات معصرة.

5.1 – الوصف الوظيفي للمعنيين بالجرائم السايبرانية المستحدثة

تتفاوت الأجهزة المعنية بالجرائم السايبرانية من حيث حجمها التنظيمي وعدد العاملين فيها ، وذلك حسب الاحتياجات الفعلية للمنظمة التي تستفيد من خدمات مثل هذه الوحدات . الا أنه من الثابت أن أية وحدة أو فرقة متخصصه للتعامل في الجرائم السايبرانية لها وظائف رئيسية وهي :-

١. دعم الادارة الأمنية في مكافحة الجرائم السايبرانية .
٢. القيام بالتحقيق في الجرائم السايبرانية .
٣. القيام بالتحقيق في حالات الاخلال وانتهاك سياسات وتدابير مكافحة الجرائم السايبرانية
٤. تنفيذ مسوحات مكافحة الجرائم السايبرانية .
٥. انشاء وقيادة برامج الوقاية من الجرائم السايبرانية .

ونحن نسعي إلى اعتماد التخصص نهجاً للتعامل مع الجرائم السايبرانية في مختلف المراحل ، من الواجب التعريف بالشخص الذي يتولى التحقيق او الإدعاء او المحاكمة في الجرائم السايبرانية من حيث مهامه وقدراته وموقعه الوظيفي . ويقتضي ذلك وضع توصيف دقيق لكل منهم .

تتكون وظائف المحققين ورجال النيابة العاملين في مجال الجرائم السايبرانية من (٦) فئات لكل منها واجبات محددة ومؤهلات تمكنه من القيام بتلك الواجبات وهي :

١. المساعد الاداري في الجرائم السايبرانية .

E-crime Investigative Administrative Assistant

واجباته :

- تقديم المساعدات الفنية لوحدة التحقيق في الجرائم السايبرانية .
- حفظ الملفات .
- طباعة التقارير .
- تنظيم قواعد البيانات .
- إعداد النصوص والرسومات البيانية اللازمة للعرض .

٢. مساعد محقق في الجرائم السايبرانية E-crime Associate

واجباته :

- مساعدة المحققين بإجراء التحقيقات الادارية .
- إجراء المسوحات والاستطلاعات .
- دعم برامج التحقيق الالكتروني .
- تقديم النصح والارشاد للموظفين بأساليب الوقاية من الجرائم السايبرانية .
- تحديد إجراءات الوقاية من الجرائم السايبرانية والمساعدة على تطوير أساليب آلية لدعم تلك الاجراءات .
- المساعدة في تحليل الأعمال اليدوية الخاصة بضع الجرائم السايبرانية ، وكتابة تقارير بذلك .

٣. محلل الجرائم السايبرانية E-crime Analyst

واجباته :

- تعريف وتنظيم وإدارة وظائف تحليل الجرائم السايبرانية .

- تمثيل وحدة التحقيق في الجرائم السايبرانية في الجهات المعنية بالوقاية من الجرائم السايبرانية
- تقديم النصح والارشاد والمساعدة للمدراء والموظفين والعملاء فيما يتصل بالوقاية من الجرائم السايبرانية .
- تقديم المشورة العامة في شرح وبيان متطلبات الوقاية من الجرائم السايبرانية .
- تعريف متطلبات الوقاية من الجرائم السايبرانية .
- تعريف وتحديد الاجراءات الراهنة للوقاية من الجرائم السايبرانية وتطوير برامج لدعم تلك الاجراءات .
- تحليل الاجراءات اليدوية المعمول بها للوقاية من الجرائم السايبرانية وتقديم توصيات بشأن تعزيزها .
- الاحتفاظ بالنظم الآلية والاجراءات اللازمة للوقاية من الجرائم السايبرانية وتعديلها وتعزيز فاعليتها .
- جمع وتحرير مجموعات التقارير والمعلومات الخاصة بالوقاية من الجرائم السايبرانية لتقديمها للمدراء والعملاء .
- القيام بالتحريات اللازمة لتحديد وتحليل الجوانب السلبية في الممارسات الالكترونية وتقييم الخسائر المحتملة والتوصية بالتدابير الاصلاحية اللازمة .
- تقييم المخاطر والمهددات المحتملة في الأنظمة الالكترونية وكشف نقاط الضعف واقتراح الحلول المسبقة .
- التخطيط والتنفيذ الدوري لمسوحات الجرائم السايبرانية .
- القيام بالوظائف الأخرى التي يكلف بها من قبل إدارة التحقيقات .

٤. كبير محللي الجرائم السايبرانية E-crime senior Analyst

واجباته :

- تحديد وتقييم وقيادة تحليل الجرائم السايبرانية وإجراءات الوقاية منها والتحريات والمسموحات .
- تقديم تحليل متطلبات الوقاية من الجرائم السايبرانية اللازمة لحماية المنظمات الالكترونية وبنياتها التحتية وتطبيق السياسات والتدابير المعتمدة لذلك .
- تمثيل وحدة التحقيق في الجرائم السايبرانية في المؤتمرات والاجتماعات مع الجهات الأخرى ذات العلاقة .
- تقديم المشورة والارشاد والمساعدة للمدراء والقادة ومدراء نظم المعلومات والقائمين على التقنيات العالية للمعلومات والمستفيدين منها فيما يتصل بالوقاية من الجرائم السايبرانية .
- إجراء تحريات وتنفيذ التحليل الفني لعمليات الوقاية من الجرائم السايبرانية وكشف التجاوزات ونقاط الضعف وتقييم الخسائر المحتملة وتطبيق المعالجات .
- تنفيذ مسوحات وتحريات مسبقة في مجال الجرائم السايبرانية ورفع تقارير بنتائجها للمدراء .
- دعم التحقيقات في الجرائم السايبرانية باستخدام معدات وبرامج متطورة .
- تقديم شهادة الخبرة أمام المحاكم الجنائية

مؤهلاته:

- بكالوريوس في نظم المعلومات، إدارة أعمال، عدالة جنائية، علوم شرطة أو علوم اجتماعية.
- خبرة عملية لا تقل عن (٤) سنوات كمحلل جرائم إلكترونية.
- اجتياز امتحان محلل الجرائم السايبرانية.

٥. محلل اختصاصي في الجرائم السايبرانية E-crime Analyst

واجباته :

- القيام بدور المستشار الفني للوقاية من الجرائم السايبرانية وتدابير مكافحتها .
- تقديم الاستشارات الفنية لمجموعة من وحدات التحقيق في الجرائم السايبرانية
- تمثيل وحدات التحقيق في الجرائم السايبرانية أمام الجهات الأخرى ذات العلاقة .
- تقديم المشورة والارشاد لكبار مدراء نظم المعلومات والمستفيدين فيما يتصل بالوقاية من الجرائم السايبرانية .
- تنفيذ جميع المهام التي تحددها إدارة الوقاية ومكافحة الجرائم السايبرانية .
- تقديم شهادات الخبرة أمام المحاكم الجنائية .

مؤهلاته:

- درجة البكالوريوس على الأقل في مجال التقنيات العالية.
- خبرة عملية لا تقل عن (٦) أعوام في مجال مكافحة الجرائم السايبرانية.
- اجتياز امتحان محلل جرائم إلكترونية.

٦. مهندس أمن النظم System security Engineer

واجباته :

- القيام بدور المستشار الفني للنظم والقائد لمشروعات التحقيق والاكتشاف والوقاية من الجرائم السايبرانية .
- قيادة عمليات التحقيق في الجرائم السايبرانية في الأجهزة الحكومية ولدى المستخدمين لضمان متطلبات التحقيق السليم والتدابير الوقائية السليمة .

- تمثيل وحدات التحقيق في الجرائم السايبرانية أمام الجهات المحلية والدولية ذات لاختصاص والوكالات الحكومية .
- تقديم المشورة والنصح للقيادات الادارية فيما يتصل بتطبيق معايير أمن التقنيات العالية .
- تقديم المساعدة للمدراء والاحتفاظ ببرامج لمكافحة الجرائم السايبرانية والتحقيق فيها .
- قيادة تقييم تدابير الوقاية من الجرائم السايبرانية وفحص نظم التحقيقات الالكترونية بمختلف أنواعها Hardware , software and firmware
- تطوير وتوجيه التقنيات الرئيسية والاجراءات والبينات التحتية بالقدر الذي يقلل من الجرائم السايبرانية ومخاطرها .
- قيادة فرق التحقيق في الجرائم السايبرانية وفرق الوقاية منها .
- التحقق من أساليب وإجراءات مكافحة الجرائم السايبرانية .
- تصميم وتطوير قواعد بيانات التحقيق ومكافحة الجرائم السايبرانية .
- الاسهام في نشر الوعي العام للوقاية من الجرائم .
- قيادة وتوجيه المحققين والموظفين العاملين في وحدات مكافحة الجرائم السايبرانية .
- تقديم الخبرة أمام المحاكم .

مؤهلاته:

- درجة البكالوريوس في نظم المعلومات، العدالة الجنائية، علوم الشرطة، العلوم الاجتماعية أو العلوم النفسية.
- خبرة عملية لاتقل عن عشرة سنوات في مجال مكافحة الجرائم السايبرانية.
- اجتياز امتحان مهندس أمن المعلومات.

مما تقدم يمكننا رسم صورة مهنية لمحقق الجرائم السايبرانية [1]

Profile of E- crime Investigator

بوصفه بما يلي :

- يستمتع باللعب بأجهزة ومعدات التقنية العالية والألعاب الالكترونية .
- يحب العمل مع الأشخاص المتخصصين في مجال التقنيات المعلومات العالية .
- يهوى اصطياط لقراصنه والهاكرز .
- يتخذ من كل جريمة الكترونية تحدياً شخصياً يعتقد أن عدم انتهاء التحقيق بالنجاح يعد فشلاً منه وتفوقاً من الجناه .
- ملماً مستجدات تقنيات المعلومات والاتصالات ذات العلاقة بالجرائم السايبرانية وقادراً على استيعابها وحسن استخدامها .
- مواكباً لأخر ماو صل إليه العلم من تقنيات وأساليب التحقيق في الجرائم السايبرانية .
- عضواً نشطاً في الروابط والجمعيات العلمية والاتحادات المهنية ذات العلاقة .
- يهوى التغيير المستمر ويزعجه عدم التغيير .
- مهيأ لخدمة العملاء .
- مهيأ لمواجهة كل التوقعات .
- يقبل ويستخدم أساليب التحقيق الجديدة والمتفردة .
- يهوي العمل في البيئة العالية للمعلومات .
- يهوى التحقيق في الجرائم السايبرانية .
- يحب الحياه والمرح .

تلك هي المواصفات والمؤهلات والشروط الأساسية التي ينبغي توفرها في محققي الجرائم السايبرانية ، فكيف يتم تعزيز تلك الخصائص والارتقاء بمهارات الأشخاص الذين

[1] Fletcher N. Baldwrin . Cyber Crime and Security , N.Y:Ocean Publications ,2008

توفرت لديهم الشروط الأساسية حتى يكونوا محققين أكفاء و خبراء في التخصصات المختلفة ؟

لا شك أننا في حاجة إلى جهد منظم لتحقيق تلك الغاية ، وفق خطط ومناهج تنفذها معاهد أو مؤسسات تعليمية مؤهلة ومعتمدة .

الفصل الثاني

الأساليب العلمية للتعامل مع الجرائم السايبرانية المستحدثة

٢ . ١ - أساليب التعامل في مرحلة التحقيق الجنائي:

تعتبر الأدلة الجنائية هي الوسيلة التي تعتمد عليها أجهزة العدالة الجنائية في إثبات وتقصي الحقائق حول الوقائع والأشخاص والأشياء، وصولاً إلى العدل كغاية يتطلع إليها كل فرد في المجتمع. وقد حدد لنا علماء البحث الجنائي أنواع من الأدلة الجنائية وهي: الأدلة القانونية، الأدلة الفنية، الأدلة القولية والأدلة المادية . في هذا السياق

جاءت قوانين الإجراءات الجنائية لتضع لنا الأحكام والضوابط المنظمة لعمليات البحث عن تلك الأدلة وكيفية جمعها وتأمينها بطرق مشروعة تحفظ لجميع الأطراف حقوقها. وقد ألف رجال التحقيق العمل في هذا المجال واكتسبوا المهارات والخبرة، إلا أننا الآن أمام نوع جديد من الجرائم يتطلب إثباتها نوعاً من الأدلة التي قد لا تندرج ضمن أنواع الأدلة الجنائية التي ألفتها أجهزة العدالة الجنائية. ولهذا النوع الجديد من الأدلة خصائص ومميزات قد تتطلب قواعد وموجهات جديدة تمكننا من التعامل معها. وبالتالي نجد أن أجهزة العدالة الجنائية في حاجة إلى مهارات جديدة وتخصصات غير تقليدية للتعامل مع نوع جديد من الأدلة الجنائية تعرف بالأدلة الرقمية. وتأتي الأدلة الجنائية الرقمية كنتيجة طبيعية لتزايد استخدام تقنية المعلومات الرقمية في الحياة العامة، بعد أن أصبحت أجهزة الحاسوب وشبكات الاتصالات الرقمية تشكل مستودعاً هاماً للمعلومات والبيانات التي من شأنها أن تدعم جهود تحقيق العدالة الجنائية.

لاشك أن هنالك قدراً لا يستهان به من الأدلة الجنائية الرقمية المنتشرة حولنا، والتي قد تختزن حقائق قيمة ولا يستفيد منها رجال الشرطة والقضاء والمحققون لجهلهم بطبيعة تلك الأدلة وقنوات انسيابها. إن عدداً محدوداً من الأقراص الصلبة قد تشكل مستودعاً لمكتبة جامعية، كاميرا رقمية قد تكون مخزناً لآلاف الصور الفوتوغرافية الرقمية عالية الجودة وشبكة معلوماتية صغيرة قد تحتوي على العديد من المعلومات المتعلقة بالأشخاص وسلوكياتهم. في كل لحظة تتحرك حولنا مكالمات هاتفية خاصة، معاملات مالية، وثائق سرية وغيرها من المعلومات الرقمية التي قد تشكل مصدراً لأدلة جنائية مفيدة . ولكن هنالك القليل من الاهتمام والمعرفة بتقنيات الأدلة الرقمية وشرعيتها وسط رجال القانون، جعل العدالة الجنائية تفقد الكثير، ومن المؤمل أن

تتضاعف الخسائر في المستقبل القريب بفضل التطور السريع في مجال تقنية المعلومات، ما لم يتضاعف الاهتمام بالأدلة الرقمية لدى أجهزة العدالة الجنائية[1] .

إن التعامل مع مثل هذه المعلومات الرقمية يحتاج إلى جهود فريق من رجال الشرطة، العلوم الجنائية، النيابة، البرمجة وتحليل النظم، إذ ليس في مقدور واحد منهم أن يكون ملماً بجميع المهارات اللازمة لكشف خبايا الجرائم ذات العلاقة بالحاسب الآلي والإنترنت. ضابط الشرطة التقليدي قد يكون ملماً بالإجراءات الفنية والقانونية المعتمدة لضبط الجرائم والتحقيق فيها وحماية حقوق الإنسان، ولكن قد لا يكون ملماً بعلوم الحاسب الآلي والحوسبة والاتصالات، وبالتالي لن يدرك تماماً ماهية الأدلة الجنائية الرقمية التي يسعى لها [2] .

لأجهزة العدالة الجنائية تجارب ناجحة في التعامل مع الأدلة الجنائية ومواكبة مستجداتها منذ أقدم العصور. إلا أن النقلة التي تقبل عليها أجهزة العدالة الجنائية اليوم أكبر مما كان متوقعاً. فالانتقال من مرحلة التعامل مع الأدلة المادية الملموسة معروفة المصادر، إلى مرحلة التعامل مع الأدلة الرقمية المنتشرة في أماكن افتراضية أمر لا مُحال يثير مشكلات مهنية وأخرى قانونية، ينبغي تحديها بدقة ووضوح توطئة لوضع الحلول المناسبة لعلاجها. ويمكننا عرض تلك المشكلات في النقاط التالية:

١. معطيات التقنية المعلوماتية الحديثة أضافت إلى مشكلة الجريمة أنماطاً إجرامية على درجة عالية من التعقيد ويحتاج إثباتها إلى أسلحة وأدوات علمية نابعة من طبيعة الجريمة المعلوماتية.

---

[1] Turvey. Brent, Criminal Profiling: An Introduction to Behavioral Evidence Analysis, London: Academic Press, 1999, P.31

[2] محمد الأمين البشرى، التحقيق في جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية والتدريبية(العدد ٣٠)، الرياض : أكاديمية نايف العربية للعلوم الأمنية ٢٠٠٠ ، ص ٣١٧

٢. كانت الأدلة الجنائية التي ألفتها أجهزة العدالة الجنائية في السابق أدلة مادية ملموسة أو مرئية أو مسموعة يمكن أن يتعامل معها الرجل العادي. وتأتي الجرائم الرقمية اليوم وتفرض على الواقع أدلة جنائية ذات طبيعة معلوماتية غير ملموسة ولا يستطيع التعامل معها إلا من كان بارعاً في استيعاب تقنية المعلوماتية.

٣. كان مسرح الجريمة وملحقاتها المستودع للأدلة الجنائية التقليدية. أما مستودع الأدلة الجنائية الرقمية فهو محيط واسع من الشبكات المعلوماتية والبرامج وأجهزة الحاسوب المنتشرة على نطاق قضائي غير محدود.

٤. نظمت القوانين وقواعد البينة المستقرة كيفية التعامل مع الأدلة الجنائية التقليدية سواء كانت مادية أو فنية أو قولية، أما الآن فنحن أمام نوع جديد من الأدلة الجنائية لم تنظمها القوانين ولم تتوفر بشأنها الأدبيات التي تعين أجهزة العدالة الجنائية.

٥. الكادر البشري المتوفر في نظام العدالة الجنائية يجهل الكثير عن الأدلة الجنائية الرقمية وقنوات انسيابها وكيفية التعامل معها الشيء الذي قد يضع العدالة في أيدي بعيدة عن نظام العدالة الجنائية.

٦. في كثير من أنحاء العالم، وفي الدول العربية على وجه الخصوص، لم تكتمل حتى الآن التشريعات أو الأطر القانونية والفقهية الضابطة للجريمة السايبرانية Cyber crime أو الأدلة الرقمية المتصلة بها،والتي تعتبر أهم الخصائص المميزة للتحقيق في الجرائم السايبرانية.

ولكن ما الأدلة الجنائية الرقمية وإلى أي نوع تنتمي؟ أين توجد تلك الأدلة؟ من المكلف بجمع الأدلة الجنائية وتأمينها؟ ما استخدامات الأدلة الجنائية الرقمية في مجال العدالة

الجنائية؟ وما حكمها شرعاً وقانوناً؟ وما مدى كفاءة رجال الشرطة و النيابة والقضاة على التعامل معها؟

يُعرِّف "كيسي" الأدلة الجنائية الرقمية بأنها تشمل جميع البيانات الرقمية التي يمكن أن تثبت أن هنالك جريمة قد ارتكبت ، أو توجد علاقة بين الجريمة والجاني أو توجد علاقة بين الجريمة والمتضرر منها. والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة ، الرسومات ، الخرائط ، الصوت أو الصورة.

"Digital evidence encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator" [1]

أما مجموعة العمل العلمية للأدلة الرقمية The Scientific Working Group on Digital Evidence فقد عرفت الدليل الرقمي عام ١٩٩٩، بأنه معلومات ذات قيمة إثباتية مخزنة أو منقولة في شكل ثنائي Information of probative value stored or transmitted in binary form [٢] إذاً ، الأدلة الجنائية الرقمية. في رأينا هي: معلومات يقبلها المنطق والعقل ويعتمدها العلم ، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الاتصال ، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه.

يرى البعض أن الأدلة الجنائية الرقمية ما هي إلا مرحلة متقدمة من الأدلة المادية الملموسة التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان إلى الاستعانة بجميع ما يبتكره العلم من أجهزة مخبرية ووسائل التقنية العالية ومنها الحاسوب محور الأدلة

[1] Eoghan Casey, Digital Evidence and Computer Crime, London: Academic Press, 2000, P. 260.

[2] J. Philip Craiger, "Law Enforcement and Digital Evidence". Handbook of Information Security, New York, John Wiley & Sons, 2005

الرقمية. فالأدلة الجنائية الرقمية في منظور أنصار هذا الاتجاه لا تختلف عن آثار الأسلحة والبصمات الوراثية D.N.A [2].

ولكن الحقيقة – في رأينا – غير ذلك. إن الأدلة الرقمية هي نوع متميز من وسائل الإثبات ولها من الخصائص العلمية والمواصفات القانونية ما يؤهلها لتقوم كإضافة جديدة لأنواع الأدلة الجنائية الأربعة آنفة الذكر ، وذلك للأسباب التالية :

أ ـ الأدلة الرقمية تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة ، ولا يدكها الرجل العادي بالحواس الطبيعية للإنسان.

ب ـ الأدلة الرقمية ليست – كما يقول البعض – أقل مادية من الأدلة المادية فحسب ، بل تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعين.

ج ـ يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها ذات القيمة العلمية والحجية الثبوتية الشيء الذي لا يتوفر في أنواع الأدلة الأخرى.

د ـ يمكن التعرف على الأدلة الرقمية المزورة أو التي جرى تحريفها بمضاهاتها مع الأدلة الأصلية بالقدر الذي لا يدع مجالاً للشك.

هـ ـ من الصعب الإتلاف أو القضاء على الأدلة الجنائية الرقمية التي يمكن استرجاعها من الحاسوب بعد محوها.

و ـ علاوة على تواجد الأدلة الرقمية في مسرح الجريمة التقليدي يمكن تواجدها أيضًا في مسرح أو مكان افتراضي Virtual Scene of Crime.

ز ـ تتميز الأدلة الجنائية الرقمية عن غيرها من أنواع الأدلة بسرعة حركتها عبر شبكات الاتصالات.

وقد قضت المحاكم بإمكانية اعتماد مثل تلك الأدلة غير الملموسة لأنها تتميز عن غيرها من أنواع الأدلة المادية الأخرى بما يلي :

أ ـ يمكن استخراج نسخ منها مماثلة ومطابقة للأصل ولها ذات الحجية.

ب ـ يمكن بالأساليب العلمية الملائمة تحديد وتأكيد ما إذا كانت الأدلة الرقمية قد تعرضت لتعديل أو تحريف.

ج ـ من الصعب إتلاف الأدلة الجنائية الرقمية ، وفي حالة محوها أو إتلافها يمكن استرجاعها من ذاكرة الحاسوب.

د ـ إذا حاول المتهمون إتلاف الأدلة الرقمية يمكن الاحتفاظ بنسخ منها في أماكن آمنة. علمًا بأن للنسخ قيمة الأصل.

٢ .١. ١- بداية التحقيق في الجرائم السايبرانية

عند وصول بلاغ إلى جهة التحقيق بأية وسيلة من وسائل الاتصال المباشر أو غير المباشر، ويفيد بوقوع جريمة الكترونية ، على متلقي البلاغ أن يوجه للمبلغ عدداً من الأسئلة ، ويحاول بالتعاون مع المبلغ إيجاد إجابات واضحة عليها . فيما يلي نشير إلى أهم الأسئلة التي ينبغي توجيهها للمبلغ ، علماً بأن هذه الأسئلة تغطي مختلف أنماط الجرائم السايبرانية ، ويمكن لمتلقي البلاغ أن يختار منها ما يناسب موضوع البلاغ الذي وصل إليه . والأسئلة هي [١] .

١. هل لديك نظام كشف الاختراق Intrusion Detection system وإذا كانت الاجابة بنعم .
٢. من هو أول من لا حظ الحادث ؟
٣. هل الجاني مازال على اتصال Online
٤. هل هنالك أي مشتبه فيه ؟
٥. هل نظم وإجراءات الأمن عاملة ؟
٦. هل تم أي اتصال بمقدم خدمة الانترنت أو أية سلطات قانونية ؟

[1] Britz , M.T. computer forensics and computer crime , New Jersey Pearson Prentice hall . 2003 .

٧. ماسبب اعتقادك بأن هنالك اختراق أو دخول غير مصرح به ؟

٨. كم عمر جهاز الحاسب الآلي ؟

٩. هل يمكنك تزويدي عاجلاً بنسخة الكترونية من مخطط شبكتك وبوسيلة آمنة ؟

١٠. ما هي البرامج التشغيلية المعمول بها لديك ؟

١١. هل لديك نظام NT وهل القرص الصلب Drivers ، FAT أو NTFS ؟

١٢. ما هي أنواع الأجهزة المستعملة لديك Intel , Sparc , Dell .....ألخ ؟

١٣. هل للنظام ملحقات CD-ROM ، أقراص أخرى ؟

١٤. هل هذه النظم مصنفة ، وهل الجزء الذي سوف أدخل فيه مصنف ؟ وأي درجة ؟ أين أبعث نتائج عملي ؟

١٥. ما حجم أجهزة الحاسب الآلي في النظام ؟

١٦. هل سيكون مدير النظام موجوداً عند وصولي ؟ وهل لديك أي خبراء أو مختصين سيتواجدون عند وصولي ؟

١٧. ما نوع المعلومات الموجودة على نظامك ؟ وهل هي معلومات مهمة لأعمالك؟

١٨. هل يمكن أن يوجد تحت تصرفي أحد خبراء البنيات التحتية لشبكاتك عند وصولي ؟

١٩. هل لديك حراس أمن لتأمين المكان ومنع الدخول إليه ؟ إن لم يكن أرجو العمل على ذلك .

٢٠. هل يُحظر في مكان الحادث استعمال أجهزة الاتصالات الالكترونية كالهاتف المتحرك أو البيجر ؟

٢١. هل يمكنك تحضير نسخه من محفوظات النظام backup للأيام الثلاثين السابقة ؟

٢٢. أرجو تحضير قائمة بجميع الموظفين العاملين في النظام أو في المشاريع التي لها صلة بالنظام ؟

٢٣. أرجو مراجعة الدخول في النظام ، وتحضير قائمة بالدخول الذي تم خلال ال ٢٤ ساعة الماضية .

٢٤. هل للنظام ارتباط مع أجهزة حاسب آلي صغيرة أو أجهزة أخرى موازية ؟

٢٥. أرجو عدم لمس أي شيء وعدم إغلاق أي نظام أو قطع الكهرباء .

٢٦. ماهي أسماء الفنادق القريبة منك التي يمكن أن أقيم فيها ؟

٢٧. وصولي سيكون الساعة كذا ، هل ستكون هنالك مطاعم مفتوحة لتناول الطعام ؟

٢٨. وصول إلى مكان الحادث الساعة (تحدد بدقة)

٢٩. أرجو عدم ذكر الحادث لآي شخص [١] .

٢,١,٢- وصول مكان الحادث :

في الطريق إلى مكان الحادث ، على المحقق أن لا يضيع الوقت ، عليه أن يراجع الاجابات التي قدمها المبلغ عند البلاغ الأول . وعلى المحقق خلال هذه الرحلة مراجعة خرائط النظام أو أي بيانات أرسلت له في ضوء الأسئلة الأولية ، كما يجب على المحقق مناقشة كل ذلك مع فريق عمله لوضع خطة عمل يتم تنفيذها فور الوصول إلى مكان الحادث .

عند الوصول إلى مكان الحادث على المحقق البدء بمقابلة المبلغ والأشخاص الذين وفرهم المبلغ لمساعدته في التحقيق . وهنا أيضاً ينبغي توجيه عدد من الأسئلة ، وفيما يلي قائمة عامة بالأسئلة اللازمة لهذه المرحلة ، وعلى المحقق الاختيار من بينها ما يتلاءم مع موضوع التحقيق والأسئلة هي :

[1] David s. Wall, cybercrime, the transformation of crime in information Age. Cambridge : polity press . 2007

١. هل كان عادياً وجود هؤلاء الأشخاص على النظام خلال ال ٢٤ ساعة الماضية ؟

٢. من هو أخر شخص كان على النظام ؟

٣. هل هذا الشخص يعمل عادة في مثل هذه الساعات ؟

٤. هل لأحد موظفيك عادة العمل أيام العطلات أو الوصول المبكر أو البقاء بعد ساعات الدوام ؟

٥. ما هي طبيعة عمل هؤلاء الموظفين ؟

٦. في أي وقت وقع الحادث ؟

٧. ماذا كان على شاشة الحاسب الآلي ؟

٨. متى تم الحفظ الاحتياطي Backup آخر مرة ؟

٩. كم مدة عمل هؤلاء الموظفين معك ؟

١٠. هل لآي من هؤلاء الموظفين سلوكاً غريباً أو علاقات سيئة مع الموظفين الأخرين ؟

١١. هل لوحظ أي شيء غير عادي على النظام خلال ال (٣٠) يوماً الماضية ؟

١٢. هل يمكنك تزويدي بما حدث ؟

١٣. ما هي البرامج أو العقود التي يعمل في النظام الآن ومن هم الأشخاص القائمين عليها ؟

١٤. هل هنالك أي تغيير في موقع النظام ؟ هل هنالك أي شيء في غير مكانه ؟

١٥. أي درجة من درجات الدخول يملك كل موظف؟

١٦. هل هنالك أي موظف غير مواطن ؟

١٧. هل هنالك أية كاميرا أو مايكروفون في المكان يمكن أن يرصد تحركات الموظفين حول النظام ؟

١٨. هل هنالك كلمات سر للدخول إلى المبنى أو المكان ؟

١٩. هل يستخدم الموظفون كلمات سر مشتركة أم يستخدمون بطاقات شخصية ؟

٢٠. هل للمنظمة أية مشاكل مالية ؟

٢١. هل قام أحد الموظفين بإجازات طويلة أو السفر خارج الدولة خلال ال (٩٠) يوماً السابقة ؟

٢٢. هل تمت مساءلة أي موظف عن اساءة استخدام النظام أو عن أي شيء آخر ؟

٢٣. هل من الموظفين من له مشاكل مالية أو أسرية ؟ وهل لآي منهم علاقات خاصة مع آخرين أو مع متعاقدين مع المنظمة ؟

٢٤. هل هنالك موظفين مؤقتين ؟

٢٥. من هم الأشخاص الأخرين المسموح لهم بالدخول ؟

٢٦. ما المستوى التعليمي ومستوى خبره الحاسب الآلي لكل من الموظفين ؟

٢٧. ماهي الأعمال التي تنفذها المنظمة الآن وفي السابق ؟

٢٨. من هو أول من شاهد الحادث ؟ ومن هو أول من أبلغ عن الحادث ؟ ومتى ؟

٢٩. هل قام الشخص الذي شهد الحادث بلمس أي شيء بعد ذلك ؟

٣٠. هل علم أي شخص في المنظمة بهذا الحدث ؟

٣١. ما هي الأوقات التي وصل فيها الموظفون اليوم ؟

٣٢. إذا كان أحدهم قد وصل مبكراً ، هل كان هنالك من وصل قبله ؟ وهل كان ذلك عادياً ؟

٣٣. أرجو تزويدي بقائمة تواجد الموظفين على النظام خلال ال (٣٠) يوماً الماضية ما بين اليوم والوقت لكل منهم ؟

٣٤. ما الغرض من هذا النظام ؟

٣٥. هل تم إنهاء عمل أي موظف خلال ال (٩٠) يوماً الماضية ؟

٣٦. هل يمكنك تزويدي بنسخه من الاجراءات الأمنية المتبعة ؟

٣٧. لماذا تعتقد أن هنالك اختراقاً ؟

٣٨. هل يمكنك تزويدي بسجل أعمال النظام ؟ وأي تعديلات أو مشاكل مرت به ؟

٣٩. هل يمكنك تزويدي بخرائط الشبكة ؟

٤٠. هل جميع الخبراء المرتبطين بالنظام حاضرون ؟ (الأسماء وأرقام الهواتف لو أمكن)

٤١. أفصح عن خطتك للبحث عن الأدلة للفريق ؟

٤٢. هل استلمتم نسخ من المحفوظات الاحتياطية Backup ؟ هل عملتم الحفظ الاحتياطي (لأعضاء الفريق)

٤٣. هل تمت صيانة النظام مؤخراً ؟ وبواسطة من ؟

٤٤. هل تمت اضافة برامج جديدة للنظام مؤخراً ؟

٤٥. هل تمت ترقية النظام أو توسعته مؤخراً ؟

٤٦. هل تواجد أي شخص مشبوه حول النظام أو في المنطقة خلال ال (٣٠) يوماً الماضية ؟

٤٧. هل مُنح تصريح دخول غير عادي لآي شخص خلال ال (٩٠) يوماً الماضية .

٤٨. هل هنالك أي موظف أو متعاقد غاضب على المنظمة ؟

٤٩. هل هنالك موظفين أو متعاقدين جُدد تم استيعابهم خلال الشهر الماضي ؟

٥٠. هل هنالك أية سياسات أو تعليمات خاصة بالموظفين أو الاتحادات أو المنظمات علينا الالتزام بها في التحقيق في هذا الحادث [1] ؟

٢.٢– العمل في مسرح الجريمة السايبرانية

وفقاً للمعايير والقواعد المعتمدة من قبل الفريق العلمي العامل في الأدلة الرقمية (SWGDE) Scientific Working Group on Digital Evidence ، والمنظمة الدولية للأدلة الرقمية (IOCE)International

[1] Debra Little Schneider. Cybercrime; Computer forensics Handbook, Rockland; Syngress Publishing, 2002.

Organization on Digital Evidence ، تتكون الأدلة الجنائية اللازمة لإثبات الجرائم السايبرانية من الآتي:[1]

- الأدلة الرقمية، وهي معلومات مفيدة للتحقيق في الجريمة الإلكترونية مخزنة أو منقولة في شكل رقمي.
- بيانات موضوعية Data Object ، وهي معلومات مفيدة للتحقيق في الجريمة الإلكترونية مرتبطة بشيء مادي.
- أشياء مادية، وهي الوسائط المادية التي تخزن فيها أو تنقل عبرها المعلومات الرقمية.
- ويُجمع معظم خبراء الأدلة الرقمية والأدلة العلمية الخاصة بالحاسب الآلي Computer Forensic حول المعايير الخاصة بالتعامل مع الأدلة الرقمية وهي:
- يجب حفظ الأدلة الأصلية على حالتها التي وجدت عليها .
- أخذ نسخ لأصل الأدلة والتعامل معها لأغراض البحث والتحليل حتى لا تتأثر الأدلة الأصلية.
- يجب أخذ النسخ على وسائط جديدة ومؤمنة ولا تحمل أية بيانات سابقة .
- يجب حفظ جميع الأدلة مرقمة وموثقة مع توثيق جميع مراحل ضبطها ونقلها وحفظها.

١,٢,٢- طرق التعامل مع الأدلة الرقمية:

يشارك في التعامل مع الأدلة الرقمية العديد من الأطراف والمعنيين، إلا أننا نشير هنا إلى ثلاثة أطراف رئيسية لها الدور الأكبر في حركة الأدلة الرقمية وتنظيم الأطراف الأخرى

[1] U.S> Department of Justice, F.B.I., Forensic science communications. Vol 2 No. 2. 2003

التي قد تتعامل مع الأدلة الرقمية . والأطراف الرئيسية الثلاثة هي، المتلقي الأول للبلاغ First Responder، المحقق وفني مسرح الجريمة. ولكل منهم أدوار نوجزها فيما يلي:

(١) **دور المتلقي الأول للبلاغ**

- تحديد وتعريف مسح الجريمة.
- تأمين وحماية مسرح الجريمة.
- الحفظ المؤقت للأدلة الهشة أو القابلة للتلف.

(٢) **دور المحقق**

- وضع خطة العمل في مسرح الجريمة.
- تنظيم وإدارة العمل في مسرح الجريمة.
- القيام بالبحث في مسرح الجريمة.
- تأمين الأدلة وحمايتها .
- استدعاء فني مسرح الجريمة.

(٣) **دور فني مسرح الجريمة**

- التحفظ على الأدلة الهشة الموجودة داخل أجهزة الحاسب الآلي وملحقاتها.
- إغلاق النظام ووضع خطة لنقل الأجهزة.
- تصنيف وترقيم الأدلة.
- حفظ وتغليف الأدلة.
- نقل الأدلة.
- فحص وتحليل الأدلة.

ويجب على فني مسرح الجريمة التأكد من اتخاذ الإجراءات التالية:

(١) تصوير شاشات الحاسب الآلي في مكان الحادث والتأكد من الشاشات الأ×رى المرتبطة بالحاسب الآلي.

(٢) حفظ الأدلة الموجودة داخل الحاسب الآلي.

(٣) عمل صور للأقراص الصلبة.

(٤) فحص التداخل بين الأقراص الصلبة.

(٥) إغلاق النظام بالطرق السليمة.

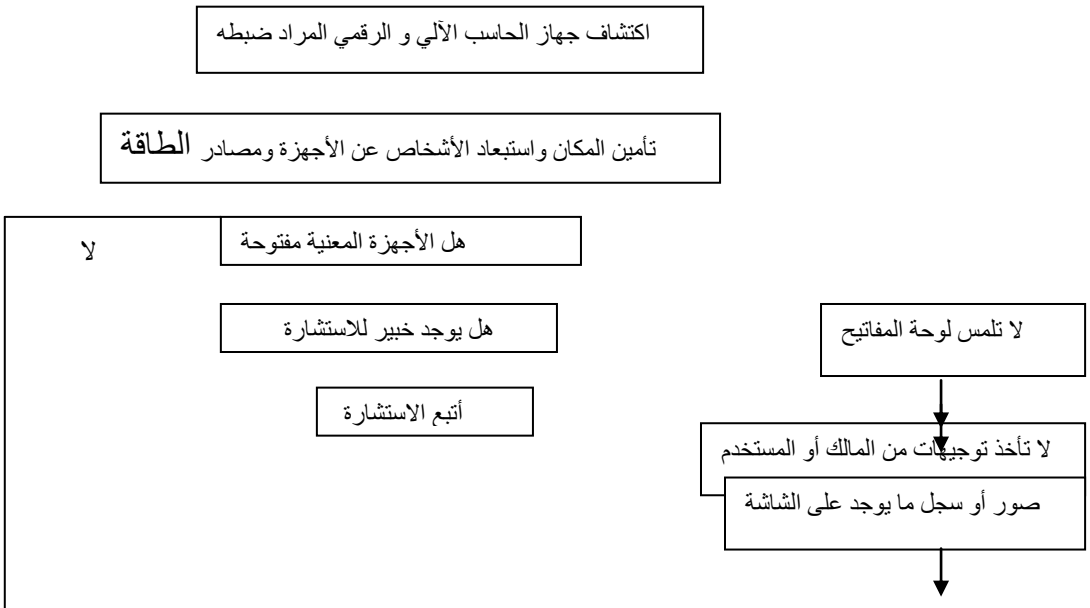
(٦) تصوير النظام قبل تحريك الأجهزة.

(٧) فصل الكهرباء عن النظام.

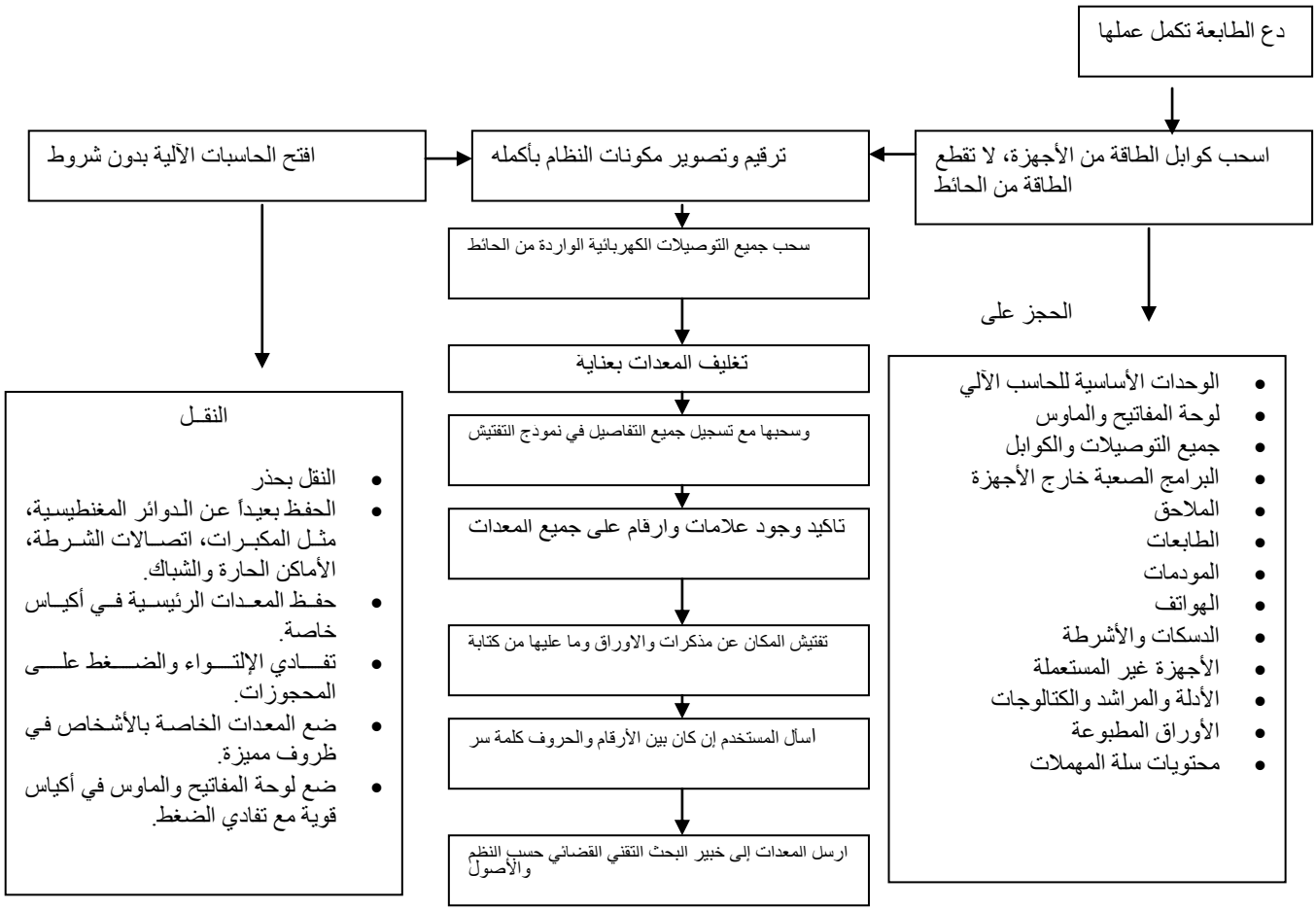
(٨) تأمين التوصيلات الكهربائية قبل تحريك الأجهزة.

(٩) جمع وحفظ كافة الملحقات والتوصيلات وحفظها بعيداً عن مصادر الحرارة أو الحقول المغنطيسية. [١]

إجراءات ضبط الأدلة الرقمية



[1] Bruce Middleton, Cyber crime Investigator's Field Guide (2nd.ed) London: Auerbach Publications, 2005



2. ٢. ٢- استرجاع الأدلة الرقمية وتوثيقها

في بعض الجرائم السايبرانية تكون الأدلـة مخزنـة ومصـنفة في ملفـات واضـحة، أمـا في جرائم أخرى قد لا يكون المحقق محظوظاً ليجد مثل هذه الأدلة بالكيفية التي يتمناها، لأن الجناة يقومون بمحو البيانات وإغلاق الملفات التي تحتوي على الأدلـة الـتي يمكـن أن تدينهم. وفي بعض الأحيان لا يتم تخزين البيانات الهامة على الديسـك تـوب ولكـن هنالك قدراً كبيراً من البيانات يـتم تخزينهـا في مواقـع أخـرى مثـل Swap page-Cache files أو الملفات المؤقتة. في هـذا الجـزء نحـاول بيـان الكيفيـة الـتي تمكـن المحقق من استرجاع مثل هذه البيانـات الـتي تم محوهـا أو تلـك الـتي تم تخزينهـا في

حقول غير تقليدية وتعرف مثل هذه البيانات أحياناً بـ Electronic dumpster diving .كثيرين من مستخدمي الحاسب الآلي ومرتكبو الجرائم السايبرانية، وحتى خبراء الحاسب الآلي يعتقدون أن محو الملفات وإلغاء محتويات سلة المهملات تعني نهاية تلك البيانات. ولكن ليس ذلك صحيحاً. إن محو الملفات لا يعني إزالة محتوياتها نهائياً من الحاسب الآلي، بل يعني مجرد سحب مؤشرات تلك الملفات File allocation table أو جدول الملفات الرئيسي Master file table .والحقيقة أن البيانات مخزنة على القرص الصلب في شكل clusters وهي وحدات تتكون من مجموعة أرقام من البتس Bits . توجد بيانات الملفات التي يتم محوها مبعثرة في القرص الصلب في عدة مواقع ، ولا شك أن سحب المؤشر عنها يجعل من الصعب إعادة جمع بياناتها، ولكن ليس من المستحيل استرجاع كل ذلك إلى حالتها الطبيعية. هنالك برامج عديدة تساعد على استرجاع الملفات المفقودة مثل برنامج NTIS Filter Get Free .في كثر من الحالات تكون هنالك بيانات قيمة مخفية في الحاسب الآلي، كما أن هنالك العديد من المواقع التي يمكن إخفاء الملفات فيها. ورغم أنه من الصعب إيجاد مثل هذه البيانات، إلا أنها تكون مفيدة أحياناً، وتستحق أن يبذل الجهد في استرجاعها.

توثيق الأدلة الرقمية

وفقاً لمعايير الأدلة الرقمية التي تم تطويرها بواسطة SWGDE و 1OCE في عام ١٩٩٩ يجب أن يكون توثيق الملاحظات والبيانات المتصلة بالجريمة مدونة بأقلام الحبر وليس بقلم الرصاص. كما يجب التوقيع على أي تعديل فيما تم تدوينه. فيما يلي نشير إلى قواعد وإجراءات توثيق الأدلة الرقمية:

١. يجب وضع الأرقام وبطاقات تعريف الأدلة بواسطة الشخص الذي قام بنقله إلى مكان الحفظ. وعلى هذا الشخص أن يوقع على البطاقات والأرقام أو الرموز التي وضع على الأدلة.[١]

٢. يجب أن يصاحب الأدلة قائمة الأدلة Evidence Logs ، التي توضح كل قطعة من الأدلة وفق أرقام متسلسلة مع بيان وصف كل قطعة مع ذكر أسماء الأشخاص الذين اكتشفوا تلك الأدلة وقاموا برفعها وتاريخ العثور عليها وحركتها من شخص إلى آخر.

٢. ٢ . ٣- طرق جمع وتوثيق الأدلة الجنائية الرقمية:

إن أول سؤال قانوني ينبغي طرحه عند الحديث حول التحقيق في جرائم المعلوماتية هو ؛ من هو الشخص الذي يحق له جمع وتحليل الأدلة الجنائية الرقمية؟ وللإجابة على ذلك نقول: الشخص الذي يُكلف بجمع الأدلة الرقمية هو الخبير المتخصص والمدرب على معالجة جميع أنواع الأدلة الرقمية وفحصها وتحليلها. إن عمليات الضبط والحجز والتأمين وتحليل الأدلة الرقمية المخزنة في شبكات المعلوماتية هي التحدي الذي يواجه أجهزة العدالة الجنائية في هذه المرحلة التي تعاني فيها تلك الأجهزة من الأمية المعلوماتية[(١)] .

وفي الوقت الذي تم فيه إعداد الخبراء والمختبرات الجنائية اللازمة للتعامل مع الأدلة المادية ، برزت مشكلة الأدلة الرقمية كنتيجة لانتشار تقنية المعلومات في مجال الجريمة. الشيء الذي يتطلب معامل ومختبرات خاصة وإعداد خبراء يجمعون بين

---

[1] Briad Matthew, "Collecting Electronic Evidence After a System Compromise" Australian Computer Emergency Team. University of Queens land. 2001

(1) **Rosenblatt. K. S. High-Technology Crime: Investigating Cases Involving Computer. San Jose: K S K Publications. 1999, P. 21.**

المعرفة القانونية ومهارة التحقيق وعلوم تقنية المعلومات. وعلاوة على ذلك ، يتطلب مواجهة التحدي الجديد بناء قدر من التعاون والثقة بين أجهزة تنفيذ القوانين والمؤسسات التي تقوم بتقديم خدمات المعلومات والاتصالات[1].

الأدلة الجنائية الرقمية مثل غيرها من الأدلة المادية تحتاج إلى التوثيق والتأمين بالقدر الذي يكفل لها المصداقية ويُبعد عنها العيوب وذلك لأسباب عدة منها:

(١) التوثيق الذي يحفظ الأدلة الرقمية في شكلها الأصلي يستعمل لعرض وتأكيد مصداقية الدليل وعدم تعرضه لتحريف أو تعديل. الصورة المسجلة بالفيديو – مثلاً – يمكن الاستعانة بها في تأكيد مدى صحة المناقشة الحية بين طرفين عن طريق مطابقة النص الرقمي مع النص المصور على الشاشة.

(٢) الأشخاص الذين يقومون بجمع الأدلة عليهم الإدلاء بشهاداتهم حول مطابقة الأدلة التي قاموا بجمعها مع تلك المقدمة أمام المحكمة والتوثيق هو الأسلوب الوحيد الذي يمكن المحققين من القيام بهذا الدور أمام القضاء. ويعتبر فشل المحقق في التمييز بين أصل الدليل وصورته أمام القضاء سببًا في بطلان الدليل.

(٣) من المهم توثيق مكان ضبط الدليل الرقمي في حالة إعادة تكوين الجريمة ، إذ أن تشابه أجهزة الحاسوب وملحقاتها يجعل من الصعب إعادة ترتيبها دون وجود توثيق سليم ومفصل يحدد الأجزاء والملحقات وأوضاعها الأصلية بدقة.

(٤) يشكل التوثيق جزءًا من عمليات حفظ الأدلة الرقمية حتى انتهاء إجراءات التحقيق والمحاكمة ، إذ أن التوثيق يشمل تحديدًا دقيقًا للجهات التي تحتفظ بالأدلة وقنوات تداولها والتي ينبغي حصرها في نطاق محدود – قدر الإمكان[1].

---

(1) **Saferstein, R. Criminalistics: An Introduction to Forensic Science, Upper Saddle River, NJ: Prentice-Hall, 1998, P. 34.**

عند توثيق الدليل الرقمي يجب التأكد من ، أين ، كيف ، متى وبواسطة من تم ضبط الدليل وتأمينه. كما أنه من الضروري توثيق الأدلة الرقمية بعدة طرق كالتصوير الفوتوغرافي ، التصوير بالفيديو ، الخرائط الكروكية وطباعة نسخ من الملفات المخزنة في جهاز الحاسوب أو المحفوظة في الأقراص. وعند حفظ الأدلة الرقمية على الأقراص والشرائط يجب تدوين البيانات التالية على كل منها:

- التاريخ والوقت.
- توقيع الشخص الذي قام بإعداد النسخة.
- اسم أو نوع نظام التشغيل.
- اسم البرنامج أو الأوامر المستعملة لإعداد النسخ.
- المعلومات المضمنة في الملف المحفوظ.

- رسالة التصنيف والتوقيعات الرقمية

رسالة التصنيف الحسابي Message Digest Algorithm هي مجموعة من الأحرف والأرقام المركبة بطريقة حسابية خاصة تمثل أي نوع من البيانات الرقمية. ويمكن ترجمة جميع محتويات أي ملف إلى كود محدد من الأحرف والأرقام أشبه بقراءة بصمات الأصابع. إن إعداد التصنيف السليم ينتج دائمًا قراءة خاصة ومميزة لكل ملف، تختلف تمامًا عن قراءة الملفات الأخرى ، إلا أنها مطابقة لقراءة النسخ الصحيحة لنفس الملف.

تستخدم رسالة التصنيف الحسابي لمضاهاة الأدلة الرقمية الأصلية مع النسخ للتأكد من صحتها وعدم تعرضها لأي تلاعب أو تحريف

٢. ٢ .٤- برامج جمع وتحليل الأدلة الرقمية

توجد الآن في الأسواق العديد من البرامج الخاصة بجمع وتحليل الأدلة الرقمية، إلا أنه من مقتضيات العدالة الجنائية أن تتعهد أجهزتها ومراكز أبحاثها بتطوير برامج خاصة ومعتمدة قانوناً للاستعمال في جمع وتحليل الأدلة الجنائية وفق معايير موحدة. وحتى تتوفر تلك البرامج نشير هنا بإيجاز إلى بعض البرامج المتوفرة في الأسواق وخصائصها، تاركين لخبراء البرمجة مهمة بيان طرق الاستفادة منها. والبرامج هي:[1]

١. **Safe Back**

ويقوم هذا البرنامج بالبحث عن الأدلة داخل أجهزة الحاسب الآلي التي تم الاعتداء عليها ومن ثم نقل تلك الأدلة وتخزينها في جهاز التحليل الخاص بالخبير، Analysis Computer

٢. Get Time

ويستخدم لتوثيق الوقت والتاريخ للحاسب الآلي الضحية من خلال قراءة وقت وتاريخ النظام من ال COMS .

٣. File List, File Convt, and Excel

يستخدم برنامج File List لجدولة المحتويات التي تم العثور عليها في الحاسب الآلي الضحية، بينما تستخدم برامج File Convt, Excel لقراءة معطيات برنامج File List .

٤. **Get Free**

ويستخدم لتقدير مساحة الملفات المطلوبة التي تم محوها Deleted وذلك كخطوة ضرورية لاسترجاع تلك المحتويات.

٥. Swap Files and Get Swap

[1] New Technologies, Inc.http:/www..Forensic-Intl/com.

يشكل برنامج Swap File جزءاً من عمليات التخزين التي تمت في جهاز الحاسب الآلي الخاص بالتحليل، لذا يكون برنامج Get Swap ضرورياً للحصول على البيانات التي تم العثور عليها في Swap File حتى يتم تحليلها فيما بعد. ويعمل هذا البرنامج في بيئةDos .

٦. Get Slack

ويوظف هذا البرنامج لالتقاط البيانات الموجودة في Hard drive الخاص بجهاز التحليلAC.

٧. Filter-1

برنامج له القدرة على جعل البيانات الرقمية binary data قابلة للطباعة واستخلاص المعلومات المفيدة من بين كميات كبيرة من البيانات. ولهذا البرنامج خيارات أربعة، وهي تحليل واستبدال ملفات، تحليل واستبدال لغات، تحليل أرقام وتحليل الأسماء.

٨. Text Search Plus

ويستعمل لقراءة جميع الملفات التي تم فتحها.

٩. CRCMD 5

يقوم بالعمليات الحسابية لملف أو ملفات Dos ويؤكد التنسيق أو التداخل بين الملف الواحد أو عدد من الملفات.

١٠. Disk Sig

يستخدم لحوسبة CRC و MD5 على نطاق جهاز كامل ومحتوياته الراهنة والسابقة.

١١. Doc

يقوم بتوثيق المحتويات الموجودة في الدليل وصولاً إلى قائمة بأسماء الملفات، أحجامها، التاريخ، الوقت بما في ذلك الملفات للقراءة فقط أو الملفات المخفية.

١٢. Mcrypt

يقوم بتشفير الملفات أو فك تشفيراتها على عدة مستويات كما يقوم بمعالجة المضغوطة والمشفرة المضغوطة.

١٣. Micro-Zap

الملفات التي يتم محوها أو إلغاءها تظل موجودة ويمكن استرجاعها، كما سبق أن أشرنا، ولكن ببرنامج Micro-Zap يمكن إزالة أسماء الملفات ومحتوياتها نهائياً بإعادة الكتابة عليها حتى سبعة مرات.

١٤. Map

يستعمل للبحث والتعرف على برامج معلقة أو مخفية في ذاكرة الحاسب الآلي وغير معروفة.

١٥. Net Threat Analyzer

له القدرة على التعرف على الأنشطة الإجرامية عبر الإنترنت قبل حدوثها.

١٦. Seized

يقوم هذا البرنامج بإغلاق الحاسب الآلي والإشعار بأن الجهاز قد تم الحجز عليه كدليل ويحظر استعماله.

١٧. NTI copy

يسمح بنسخ الملفات من جهاز الحاسب الآلي دون تغيير في البيانات أو التاريخ.

١٨. PRTK

يقوم باسترجاع كلمة السر ويستخدم عادة بواسطة الأجهزة الأمنية ويتم تطويره بصفة دورية.

١٩. Net stat

يستخدم هذا البرنامج لاكتشاف الدخول غير المصرح به على جهاز الحاسب الآلي أو شبكة من الأجهزة.

٣,٢- تصور شخصيات أطراف الجريمة السايبرانية

لا ترتبط الجرائم السايبرانية بالحاسب الآلي فقط ، بل إنها ترتبط أيضاً بالانسان ، وتعتبر معرفة الجرائم السايبرانية هي الخطوة الأولى نحو مكافحتها ، ثم تأتي معرفة الأشخاص الذين يتواجدون في مسرح الجريمة ومنهم الجناة ، الضحايا والمعنيون بمكافحتها . إن معرفة هذه الأطراف ورسم صورة نموذجية لكل منها Profiling people هو الخطوة الثانية لمكافحة الجرائم السايبرانية . و يصعب رسم صورة يصعب تعريف المجرم الالكتروني ، مثلما نموذجية للمجرم الإلكتروني ، لتعدد وتنوع أسبابها ودوافعها . ولكن يمكننا تصنيف مرتكبي الجرائم السايبرانية ووضع صورة نموذجية لكل فئة وفقاً للدوافع والخصائص والسلوكيات التي تتميز بها كل فئة . أما تصوير ضحايا الجرائم السايبرانية وتحديد سماتهم فيساعد كثيراً على نشر الوعي الأمني وتسهيل مهمة المحققين في اكتشاف الجرائم السايبرانية قبل وقوعها وارشاد الضحايا على إجراءات الوقاية منها . يتطلب التعامل مع الجرائم السايبرانية في مختلف مراحلها التعرف على الأشخاص المعنيين بها وكتابة لمحة تاريخية وإجتماعية لشخصياتهم وخصائصها ووضع تصور دقيق لكل منهم وهم مرتكبو الجرائم السايبرانية ، ضحايا الجرائم السايبرانية والمحققون فيها . فمن هم هؤلاء الأشخاص وما هي خصائصهم التي تساعدهم على القيام بأدوارهم ، وكيف يمكننا أن تميزهم عن غيرهم ؟

أولاً : مرتكبو الجرائم السايبرانية Cybercriminals

التعرف على المجرم الالكتروني ورسم صورة له يعتمد على توفر معلومات عن تكوينة البدني ، العقلي والعاطفي . ولا تعتبر الصورة التي نرسمها للمجرم دليلاً ضده ، ولكن قد تكون البداية للبحث عن الأدلة . وتبني صورة المجرم عادة من خصائص يتم استنباطها من المؤشرات التالية :

- ملاحظة الجريمة ومسرح الجريمة .
- أقوال الشهود وضحايا الجريمة .
- دراسة سيكولوجيا الجريمة .
- الدراسة الإجتماعية
- فحص أنماط عديدة من الجرائم للمقارنة .

وهنالك طريقتان لرسم صورة المجرم هما الرسم الاستقرائي Inductive profiling والرسم الإستنتاجي Deductive profiling .

تعتمد طريقة الرسم الإستقرائي Inductive profiling على الإحصاءات والتحليل المقارن للمعلومات التي يتم جمعها عن المجرم .

أما طريقة الرسم الإستنتاجي Deductive profiling فتعتمد على الأدلة الملحوظة التي يجمعها المحققون ومن ثم يقوم رسام الصورة Profiler باستنباط الخصائص المميزة بناءً على خبرته عبر خطوات محددة هي :

١. تحديد المشكلة .
٢. جمع المعلومات .
٣. وضع الفرضيات .
٤. إختبار الفرضيات .

٥. فحص نتائج الاختبار .

٦. الوصول إلى النتائج .

وكما سبق أن أشرنا فإن رسم صورة المجرم لا يُعد حلاً للجريمة ولكن يمكن استخدام تلك الصورة في الآتي :

- تضييق نطاق بحث المشتبه فيهم .
- الربط بين الجرائم ذات العلاقة .
- تزويد المحققين بخيوط قيمة للبحث .

وعلاوة على ذلك ، وفي ضوء قراءة عامة لتاريخ الجرائم السايبرانية نجد عدداً من الخصائص المساعدة على رسم صورة للمجرم الالكتروني وهي :

- الذكاء .
- المعرفة بالتقنيات العالية .
- في العشرينات من العمر .
- الذكور .
- عدم الميل للعنف .
- عدم إحترام القانون .
- انتحال الشخصية .
- المقامرة .
- قوة الدافعية ، وقد تكون هذه الدافعية التسلية ، حب المال ، الانتقام ، أهداف سياسية ، دوافع جنسية أو أمراض نفسية .

ثانياً : ضحايا الجرائم السايبرانية

التعرف على أنماط ضحايا الجرائم السايبرانية ورسم صورة نموذجية لهم له فوائد كثيرة منها :

- تمكين ضباط تنفيذ القانون من الشرطة والنيابة والقضاء على التنبؤ بالأشخاص والمؤسسات التي قد تكون عرضه للجرائم الالكترونية ومن ثم إنذارهم وإرشادهم .
- تنبيه الضحايا المحتملين لاتخاذ خطوات عملية لتفادي الجريمة .
- مساعدة المحققين على رسم صورة لمرتكب الجريمة ، لأن اختيار الضحية عنصر من عناصر شخصية المجرم .
- تمكين جهاز مكافحة الجرائم السايبرانية من استخدام الصورة النموذجية للضحايا في نصب الشراك وإلقاء القبض على مرتكبي الجرائم السايبرانية .

ويصعب رسم صورة نموذجية لضحايا الجرائم السايبرانية لتعدد أنماط الضحايا من أشخاص إلى مؤسسات عامة أو خاصة أو منظمات سياسية أو اجتماعية . فإذا أخذنا ضحايا الجرائم السايبرانية الأفراد ، فتشير الدراسات السابقة [1] إلى تميزهم بالخصائص التالية :

- معاقون بأي شكل من أشكال الاعاقة الطبيعية أو المكتسبة .
- المعانون من التوحد .
- قصور في الحياة العاطفية .
- الاحساس بالظلم والتضحية دون أن يتعرضوا لذلك .
- حديثو عهد بالانترنت .
- غير محظوظون في تنظيم تحركاتهم .

أما بالنسبة للمؤسسات العامة والخاصة والمنظمات السياسية والاجتماعية فإن الصورة النموذجية للضحايا منها قد تتمثل في النظم الادارية والمالية التي تطبعها تلك المنظمات

[1] Lan Walden , computer crimes and Digital investigations , New york , oxford university press , 2007

بجانب طبيعة الأنشطة التي تقوم بها ومدى الرضا والقبول التي تحظى بها تلك الأنشطة وسط عامة الناس .

ثالثاً : موظف العدالة الجنائية و الجرائم السايبرانية :

موظف العدالة الجنائية المعني بالجرائم السايبرانية هو في الأصل من **موظفي العدالة الجنائية المعنيين** بالجرائم العادية أو من الأشخاص الذين اكتسبوا الخبرة في التحقيقات الجنائية . وهم في الغالب من رجال الشرطة والنيابة والقضاء أو الجهات الأخرى المتخصصة في التحقيق . ولكن للعمل في مجال الجرائم السايبرانية فينبغي المامه بتقنيات الحاسب الآلي [1] والإتصالات بالإضافة الى المهارات المعروفة للتعامل مع الجرائم التقليدية والجرائم المستحدثة ومن المهارات اللازمة للتعامل مع الجرائم السايبرانية ما يلي :

- المهارة الفائقة في الملاحظة وملاحظة الأشياء الدقيقة .
- قوة الذاكرة التي تمكنه من تخزين الملاحظات الدقيقة وربطها ببعضها البعض .
- مهارة التنظيم والترتيب المنطقي للمعلومات والملاحظات .
- مهارة التوثيق والحفظ للمعلومات الواقعية .
- عدم التأثر بالمؤثرات الخارجية .
- معرفة القوانين وقواعد البينة وتقنيات التحقيق .
- مهارة التفكير بعقلية المجرم والتنبؤ بتحركاته .
- القدرة على التخيل الذكي البناء .
- القدرة على العمل لساعات طويلة .
- حب التعلم .

[1] Debra littlejohn Shinder Scene of the Cybercrime – computer forensic Handbook . Rockland : Singress Publishing , 2002

- المعرفة بأساسيات الحاسب الآلي .
- معرفة بروتوكولات شبكات الحاسب الآلي .
- معرفة مختصرات لغة الحاسب الآلي .
- الالمام بأمن الحاسب الآلي والشبكات ويشمل :
  - معرفة مكونات الحاسب الآلي Hardware .
  - معرفة لغات الحاسب الآلي .
  - معرفة نظم تشغيل الحاسب الآلي .
  - معرفة نظم الملفات .
  - معرفة دور برامج التشغيل .
  - معرفة نظام الترقيم Binary Numbering
  - معرفة كيفية عمل الحاسب الآلي في شبكات الاتصالات .
  - معرفة بروتوكولات TCP/IP المستعملة في الانترنت .
  - معرفة الاختراقات والهجمات .
  - معرفة الأنشطة السابقة للهجمات .
  - معرفة أساليب سرقة كلمات السر .
  - معرفة طرق منع الجرائم السايبرانية .
  - معرفة مفاهيم أمن النظم .
  - معرفة تطبيق تدابير أمن النظم .
  - معرفة تطبيق تقنيات إكتشاف الجرائم السايبرانية مثل :
    (١) المراجعة الأمنية للملفات .
    (٢) الجدران النارية والانذارات .
    (٣) تتبع الحقول والعناوين .

(٤) التلاعب بالبريد الالكتروني .[١]

٢. ١,٣- البحث التقني القانوني للحاسب الآلي والتحقيق في الجرائم السايبرانية

لبيان ماهية البحث التقني القانوني للحاسب الآلي والتعريف بدوره في الحقيق الجنائي ينبغي في البدء ، التعريف بعبارة البحث العلمي القضائي المعروفة بالطب الشرعي Forensic Sciences. عبارة البحث العلمي القضائي أصلها من العبارة اللاتينية Forensisالتي تعني ، (في أو أمام المحكمة) of or before the forum . وكانت هذه العبارة معروفة في العهد الروماني في مجال محاكمة القضايا الجنائية، حيث كان الجاني والمجني عليه يمثلان أمام لجنة من عامة الناس ليقوم كل منهما بتقديم الحجج والأدلة التي تثبت أو تنفي التهمة. وكان، عادة، الطرف الذي يملك القدرة على مخاطبة اللجنة ويتميز بمهارة العرض والإقناع هو الذي يكسب القضية. ويُعد مفهوم الأدلة القانونية والعرض العام الكامن في العبارة اللاتينية هو السبب في ربط عبارة Forensic sciences أو الطب الشرعي بمجال الأدلة الجنائية واستخدامات العلوم التطبيقية في تحقيق العدالة الجنائية.[٢]

في كثير من القواميس الحديثة نجد تعريفات لعبارة البحث العلمي القضائئ لاتخرج عن المعاني المتضمنة في الأصل اللاتيني لعبارة Forensis ومدلولها القضائي. القاموس الأمريكي للتراث يشير إلى عبارة Forensis بأنها:

(١)تتعلق أو تستعمل أو تتناسب للمحاكم المشكلة القانون أو المناقشة والجدال في مكان عام.

[1] Clifford , R , Cybercrime : The Investigation , prosecution and Defense of a Computer related crime , (2nd . ed) Carolina Academic Press , 2006
[2] Kind. S., Over man, Science Against Crime. New York: Doubleday,1972, pp21-27

(٢) يتعلق باستعمال العلوم أو التقانة في التحقيق أو إثبات حقائق أو أدلة أمام محكمة قانون.

(1)Relating to, used in or appropriate for courts of law or for public discussion or argument.

(2)Relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law.

أما قاموس مريام وبستر Merriam Webster's online Dictionary فيشير إلى عبارة Forensis بأنها ترتبط أو تستعمل أو ملائمة لمحاكم قضائية أو مناقشة عامة.

Belonging to, used in, or suitable to courts of judicature or to public discussion and debate.

١. الملفات التي تم محوها .

٢. كشف محتويات الملفات المخفية.

٣. الدخول على محتويات الملفات المحمية أو المشفرة.

٤. تحليل جميع البيانات ذات العلاقة التي يتم العثور عليها.

٥. طباعة جميع تحليلات نظام الحاسب الآلي موضع الفحص.

٦. تقديم استشارة خبير كشاهد عند الطلب.

ولا تقتصر أدلة الفحص المخبري للحاسب الآلي على قضايا الجرائم السايبرانية فحسب، بل يمكن الاستفادة منها .

. إلا أننا نجد اليوم أن هذه العبارة قد اتسع مفهومها ليغطي كافة أبواب المعرفة التي يتطلب البحث فيها طرقاً علمية تطبيقية . فالعبارة تستخدم في مجالات عديدة منها[١] :

- السياسة Diplomatics (forensic paleography
- المحاسبة Forensic accounting
- الرسوم المتحركة Forensic animation

[١] Owen D. Hidden Evidence: The Story of Forensic Science and how it helped to Worlds Toughest Crimes. London: Quintet publishing, 2006.pp.48-50، Solve 4

- الأنثروبولوجي Forensic anthropology
- الكيميـــاء Forensic chemistry
- الهندســـة Forensic engineering
- إعادة تركيب الوجه Forensic facial reconstruction
- التعـــرف forensic identification
- هندسة المـــواد Forensic materials engineering
- هندســـــة Forensic polymer engineering
- هندسة رسم التصوير Forensic profiling
- السيكولوجي Forensic psychology
- الحاسب الآلي Computer forensics

١. الإثبـــات أو النفـــي في الجـــرائم التقليديـــة مثـــل جـــرائم القتـــل، الســـرقات والاختلاسات.

٢. الدعاوى المدنية التي تقتضي معرفة سجلات الأشخاص والمؤسسات.

٣. القضايا الإدارية والقضايا المتعلقة بسلوك الموظفين.

٤. الدعاوى الشرعية التي تتطلب بيان العلاقات الأسرية والنسب.

٥. المسائل العسكرية.

٦. قضايا الاستخبارات وأمن الدولة.

٧. قضايا شركات التأمين.

الفصل الثالث

أساليب التعامل مع الجرائم السايبرانية في مرحلة الإدعاء والمحاكمة

٣. ١ أساليب التعامل في مرحلة الإدعاء

تتميز الجرائم السايبرانية بخصائص فنية عن غيرها من الجرائم ، مما يعقد إجراءات الادعاء فيها أمام المحاكم فالجريمة الالكترونية بطبيعتها جريمة معقدة لأن أداتها جهاز الحاسب الآلي وملحقاته العديدة ولغاته وبرامجه التي لا يفهمها إلا القلة من الخبراء والمختصين . وقد أدت تعقيدات أداة الجريمة الالكترونية إلى تعقيدات أخرى في تعريف الجريمة الالكترونية وتحديد عناصرها والنوعية الخاصة من الأدلة الرقمية اللازمة لاثباتها . لكل ذلك نجد الادعاء في الجرائم السايبرانية يواجه صعوبات جمة نبحثها في هذا الجزء على النحو التالي :

أولا : الشكوى أو البلاغ الذي يتقدم به المتضرر من الجريمة للسلطات الرسمية هو أولى خطوات نجاح التحقيق والادعاء في الجرائم . إن غموض طبيعة الجريمة الالكترونية وتعقيداتها الفنية يجعل من الصعب على أي شخص غير متخصص في مجال الحاسب الآلي والانترنت أن يدرك ما حدث له من ضرر أو الكيفية التي إعتدى بها الجاني على

أنظمته . هذا من جهة الضحايا العاديين سواءً كانوا أفراد أو مؤسسات . أما من جهة أجهزة انفاذ القوانين كالنيابة العامة أو الشرطة التي تقوم عادة بملاحظة مخالفة القانون واكتشاف مرتكبي الجريمة تضييق أمامهم فرص رصد أو ملاحظة الجرائم السايبرانية التي لا تقع عادة في الطرقات والأماكن العامة المسموح للأجهزة الأمنية مراقبتها .

أما إذا كان اعتمادنا على الخبراء ومدراء النظم القائمين على أجهزة الحاسب الألي وشبكاته ، فإنهم أولاً قلة ولا يتواجدون سوى في المؤسسات والشركات الكبيرة ، وثانياً، إنهم غير ملمين بالقوانين الجنائية بالقدر الذي يمكنهم من القول بأن ما يحدث في أماكن عملهم من اختراقات ، ما اذا كانت تشكل جريمة ينبغي التبليغ عنها ، أم خللاً فنياً عليهم معالجتها . ويترتب على ما تقدم ما يلي :

١. قلة البلاغات التي تصل إلى علم النيابة العامة .
٢. وصول البلاغات متأخرة مما يفقد التحقيق فرص ضبط الجناه وإيقاف الجريمة والحد من أضرارها .
٣. وصول البلاغات ببيانات غير واضحة أو مفيدة للعدالة بسبب جهل المبلغين بأبعاد الجريمة وكيفية حدوثها .
٤. صعوبة التفاهم مع الضحايا والشهود إن وجدوا بسبب عدم إلمامهم بلغات الحاسب الآلي ومختصراتها .
٥. ندرة فرص العثور على أدلة مادية أو مسرح للجريمة في بعض الحالات .

ثانياً : الجانب القانوني

١. من حيث التجريم : يشكل القانون الجنائي الذي يحكم التعامل مع الجرائم السايبرانية معضلة بالنسبة للادعاء العام . وتنقسم الجرائم من حيث تقييم عامة الناس لها إلى قسمين هما :

- جرائم حقيقية تحت القانون الطبيعي أو القانون الوضعي تُعرف ب Mala in se كالقتل والسرقة والنهب والتي لا يختلف الناس حول تجريمها .
- جرائم صنعها المشرع وتُعرف mala prohibita والتي تختلف المجتمعات حول تجريمها مثل حيازة الأسلحة وشرب الخمر، وتعتبر الجرائم السايبرانية من هذا النوع الأخير .

لذا يعتقد البعض أن بعض أنماط الأنشطة الالكترونية لا تشكل جريمة . وهذه الحالة من عدم قناعة بعض أفراد المجتمع بتجريم أخذ نسخة من بيانات شخص آخر – على سبيل المثال – يجعل الكثيرين لا يعيرون اهتماماً بالتبليغ عن الجرائم السايبرانية أو الإدلاء بشهادات فيها ، تاركين كامل المسؤولية لأجهزة تنفيذ القانون .

٢. من حيث وجود جسم الجريمة : تأتي في المرتبة الثانية من المعضلة القانونية التي يواجهها الادعاء العام في الجرائم السايبرانية مسألة جسم الجريمة ، وجوده الفعلي .

إن مفهوم Corpus delicti أم جسم الجريمة يصنف لنا دائماً الدليل المادي الذي يؤكد وقوع الجريمة فالقاعدة التاريخية تقول أن وجود الجثة هو أهم الأدلة التي تثبت أن هنالك جريمة قتل تستدعي التحقيق وجمع الأدلة . ففي حالة الجريمة الالكترونية يقف الادعاء حائراً في غياب جسم الجريمة الالكترونية ، خاصة وليست هنالك أدلة مادية تثبت وقوع الجريمة .

قبل أن يوجه الادعاء التهمة في أية جريمة ، عليه أن اثبات عنصرين رئيسين وهما

٣. من حيث القصد الجنائي :

- الفعل أو الامتناع الجنائي Actus والتي تعني guilty act .
- والقصد الجنائي Mens rea والتي تعني guilty mind . وتصف معظم القوانين الجنائية القصد الجنائي بالنية والعلم حتى ولو كان هنالك حالة من الطيش والاهمال .

فإلى أي مدى يمكننا إعتماد هذه المفاهيم الراسخة في الجرائم السايبرانية ، الأمر الذي يلقي على المحقق وممثل الادعاء في الجرائم السايبرانية مهمة البحث عن أدلة مقبولة لاثبات Actus reus و Mens rea .

٤. من حيث الاثبات : يتطلب توجيه الاتهام وايقاف أي شخص للتحقيق معه في أية جريمة توفر أدلة تثبت أن هنالك سبباً معقولاً reasonable cause يجعل الرجل العادي يعتقد بأن الشخص المراد إيقافه ارتكب الجريمة المعنية . وبعد الاتهام على المحقق وممثل الادعاء توفير أدلة تثبت بما لا يدع مجالاً للشك byond reasonable doubt بأن المتهم هو مرتكب تلك الجريمة .

ثالثا : في الجرائم السايبرانية يواجه الادعاء صعوبة في توجيه الاتهام بسبب ندرة الأدلة المادية التي يمكن أن يلمسها ويستوعبها الرجل العادي حتى يعتقد أن هنالك سبباً معقولاً . وتتضاعف بالطبع الصعوبة عند سعي الادعاء لاثبات التهمة بما لا يدع مجالاً للشك ، خاصة وطبيعة الجريمة الالكترونية المعقدة والعمليات الافتراضية التي تشكل عناصر الجريمة يصعب اخضاعها لمعايير وقواعد البينة التقليدية .

رابعا : مسألة الاختصاص : يعتبر الاختصاص من المسائل المثيرة للجدل في الجرائم السايبرانية التي ترتكب أحياناً في الفضاء دون تحديد لمكان معروف . قد يكون الجناه والضحايا في أماكن أو دول مختلفة وهنالك من يرون أن الانترنت منطقة حرة لا ينبغي للدول التحكم عليها بالقوانين ، بينما يرى البعض الآخر أنه من الضروري انشاء شرطة خاصة للانترنت . ويتفرع عن هذا الأخير أسئلة أخرى عن الجهة التي تتبع لها الشرطة الخاصة بالانترنت ، هل تكون تابعة لمنظمات إقليمية أو دولية كالأمم المتحدة . كل ذلك مؤشرات عن المشكلة المعقدة التي يواجهها الادعاء في التعامل مع دائرة الاختصاص . ورغم اتجاه المجتمع الدولي إلى اعتماد الجريمة الالكترونية جريمة دولية تعالجها الاتفاقية الدولية لمكافحة الجرائم السايبرانية ، إلا أن هذه الاتفاقية لم تعالج بوضوح المسائل المتعلقة بالاختصاص والإجراءات الشكلية التي يضطلع بها المحققون ووكلاء النيابة [١] .

ومن جهة أخرى فإن الطبيعة الدولية للجريمة الالكترونية وامتدادها عبر مساحات جغرافية واسعة تعيق التحقيق والادعاء فيها لأسباب منها [٢] :

١. تكلفة السفر للتحقيق في أماكن نائية .
٢. صعوبة نقل الشهود من وإلى مكان التحقيق أو المحاكمة .
٣. تعقيدات التعامل مع متهمين في دول أخرى أو خارج دائرة الاختصاص .
٤. المسؤولية السياسية التي تقتضي بتولي أجهزة الدولة شؤون رعاياها .
٥. عدم توفر الخبرات التقنية الكافية في مجال الجرائم السايبرانية .
٦. الإجراءات الورقية المعقدة التي تتطلبها التعامل مع الدول الأخرى في الأمور الجنائية .

[1] Vacca John, ldentity theft . New york , Prentice Hall , 2002
[2] Mcquade , s. Understanding and Managing Cybercrime Boston . Auyn and Bacon , 2006

٧. حاجز اللغة الذي يحول دون التفاهم المباشر بين المحققين والشهود من الدول الأخرى .

رغم وجود صعوبات عديدة أمام التحقيق والإدعاء ، في الجرائم السايبرانية هنالك حلول تساعد على تجاوز تلك الصعوبات والقيام بالادعاء الفعال وذلك باتباع ما يلي :

١. التعاون والتنسيق بين المحقق وممثل الادعاء وخبير تقنية المعلومات ، والعمل منذ البداية على أسس واضحة تحدد الأدوار .
٢. عدم سعي أي من المحقق أو ممثل النيابة أو خبير تقنية المعلومات الانفراد بالقضية أو نصب نفسه مسئولاً أولاً عنها .
٣. قناعة كل طرف من الأطراف الثلاثة المذكورة أعلاه بحدود معرفته ومهارته واحترام معرفة غيره من الأطراف .
٤. على خبراء تقنية المعلومات الذين يعملون مع رجال تنفيذ القانون أن يكونوا ملمين بالاجراءات الشكلية الخاصة بنظام العدالة الجنائية ، حتى لا تكون الأدلة التي يحصلون عليها باطلة .
٥. يجب الادراك بالتعقيدات الخاصة بالجوانب القانونية ومسائل الاختصاص ، وتوقع جميع المعوقات التي أشرنا إليها إعلاه والتحضير المسبق للتعامل معها حتى لا تكون تلك المعوقات مفاجئة ومحبطة لهم .
٦. يجب أن يسعى المحقق وممثل الادعاء إلى فهم لغة الحاسب الآلي والمختصرات التي يذكرها خبير تقنية المعلومات في كل قضية والتحدث بذات المختصرات ومعانيها المتفق عليها ، لأن اختلافهم حول تلك المفردات قد تكون مدعاة للشك الذي يُبطل التهمة .
٧. على الأطراف الثلاثة المذكورة أعلاه العمل معاً والتشاور في جميع الخطوات قبل تنفيذها ، خاصة فيما يتعلق بترتيب الأولويات الاجرائية .

٨. التأكيد بأن التحقيق السليم هو المدخل لبناء الادعاء القوى . والتحقيق السليم يقوم أساساً على معرفة القانون الجنائي وقواعد البينة واستخدام أدوات التحقيق المعيارية Stanard investigative tool kits ، التي تتكون من المعلومات ، المقابلة ، والاستجواب instrumentation [1] على أن يكون استخدام تلك الأدوات وفقاً للترتيب التالي :

- تحليل الشكوى أو البلاغ .
- جمع الأدلة المادية .
- الحصول على استشارة الخبراء .
- مقابلة الشهود واستجواب المشتبه فيهم .
- بناء ملف القضية .
- تحليل القضية .
- إجراء تحقيقات المتابعة .
- اتخاذ قرار الادعاء .

٣. ٢ – أساليب التعامل في مرحلة المحاكمة

لا تختلف إجراءات محاكمة الجرائم السايبرانية عن غيرها من الجرائم الأخرى وينظم قانون الإجراءات الجنائية مراحل التقاضي ، إحضار الشهود ، الاستماع ، المناقشة وعرض الأدلة ومناقشتها من قبل طرفي الادعاء والدفاع ومن ثم المحكمة . الذي يهمنا في هذا السياق ، ونحن بصدد تقديم جريمة الكترونية أمام محاكم تقليدية ، أن نحرص على إعداد الأدلة والشهود وكافة الوثائق بالكيفية التي يسهل فهمها واستيعابها من قبل المحكمة التي قد لا تكون متخصصة في مجال تقنية المعلومات والاتصالات . ومن

[1] John R. Vacca , computer forensics – computer crime scene lnvestigation (snd.ed) massachus – etts, charles River media , 2005

الواجب هنا التنسيق المسبق بين ممثل الادعاء والمحققين والخبراء حول كيفية تقديم الأدلة وإفادات الشهود وطبيعة الأسئلة التي توجه لهم ، بالإضافة إلى وضع سناريوهات لمواجهة الأسئلة التي قد يطرحها الدفاع .

يعتمد الادعاء في الجرائم السايبرانية في الغالب على الخبراء ، والشرطة والشهود وعلى رأسهم الشاكي . فالخبير هو أهم عناصر القوة في إثبات التهمة وبيان الحقائق أمام المحكمة . عليه على الادعاء اعداد الخبير إعداداً جيداً ، وذلك من حيث الأسئلة التي قد تطرح عليه يهدف التشكيك في خبرته ، وتوفير إجابات نموذجية وموثقة . ومن الأسئلة التقليدية التي قد تطرحها المحكمة أو الدفاع ما يلي :

١. ما هي الشهادات العلمية التي حصلت عليها ؟

- الإجابة : هي ذكر الدرجة العلمية والجهة التعليمية المانحة لها ومعادلاتها من الشهادات الوطنية حالة حصولها من جهات تعليمية أجنبية .

٢. ما هي مدة خبرتك في هذا المجال ؟

- الاجابة : ذكر عدد السنوات والأشهر التي مضت عليه وهو يعمل في المجال بتخصصاته المفصلة بما في ذلك الأعمال الميدانية ، المكتبية ، البحتية والتدريسية .

٣. ما هي الوظائف أو الدرجات الوظيفية التي شغلتها في هذا المجال ؟

- الاجابة : ذكر أسماء الوظائف ، سواءً كانت إدارية أو فنية مع بيان المدة الزمنية التي أمضاها في كل وظيفة ، وما إذا كانت في نفس المنظمة أو في أكثر من منظمة .

٤. ماهي الكورسات التي قمت بتدريسها في هذا المجال ؟

- الاجابة : ذكر أسماء الكورسات ذات العلاقة بموضوع شهادته أمام المحكمة مع بيان عددها والجهات التي قدم فيها تلك الكورسات .

٥. ما هي الكتب أو البحوث التي قمت بنشرها في هذا المجال :

- الاجابة : ذكر أسماء الكتب وعناوين البحوث وأماكن نشرها وتاريخ نشرها مع التركيز على البحوث والمؤلفات التي تتصل بموضوع الشهادة .

٦. ما هي خبرتك كشاهد في هذا المجال ؟

- الاجابة : ذكر القضايا والمحاكم التي مثل أمامها وبيان الموضوعات التي قدم خبرته حولها بالاعداد والتواريخ بالتسلسل ، سواءً كانت تلك الخبرة في محاكم داخل دائرة الاختصاص أو خارج الدولة [١] .

ومن المؤكد أن يسعى الدفاع بكل قوة إلى ايجاد ثغرات في كل ما يتعلق بخبرة الشاهد حتى يثير حوله الشكوك ، لذا ينبغي تذكير الخبير بأهمية الدقة والايجاز وانتقاء العبارات والمسميات ، حسبما يتم الاتفاق عليه مسبقاً مع ممثل الادعاء .

أما المحققون فإن شهادتهم تقتصر على تأكيد وشرح الاجراءات التي قاموا بها ونقل الصورة الحقيقية لمسرح الجريمة إلى المحكمة . ومع ذلك ينبغي حرصهم على الدقة والاستعانة بمحضر التحقيقات قبل بداية الجلسة ، للتأكد من الأرقام والتواريخ والمسميات الفنية حتى لا يقعوا في أخطاء تكون زريعة للدفاع . ويجب على المحقق كشاهد على اليمين أن لا يقول سوى الحق . وليس من العيب أن يجيب على أسئلة المحكمة أو الدفاع بعبارة " لا أعرف " أو " لا أذكر " وفيما يلي بعض المؤشرات التي من شأنها أن تعزز مصداقية المحقق أو غيره من الشهود .

[1] kenneth s. Rosenblatt , high – technology crime – investigating cases involving computers . san Jose :ksk publications , 2000

١. الحضور إلى المحكمة قبل وقت الجلسة للتعرف على قاعة المحكمة ومعرفة الطريق إلى مكانه أمام المحكمة .

٢. الوقوف أمام المحكمة بثقة وهدوء وعدم اظهار الخوف أو القلق أو الانزعاج من الأسئلة التي تطرح عليه ، وأن يتذكر دائماً أنه ليس صاحب مصلحة خاصة في القضية كما أن وظيفته هي اظهار الحقيقة وليس مجرد إدانة المتهم .

٣. عدم الانقياد للاثارة والاستفزاز والبعد عن معاداة الدفاع واظهار عدم احترامه .

٤. لا تتقدم تطوعاً بمعلومات اضافية أكثر مما تتطلبه الأسئلة .

٥. إرتداء الزي المهني الرسمي والظهور بالمظهر اللائق .

٦. الاستماع إلى الأسئلة جيداً واستيعاب المقصود منها قبل الشروع في الاجابة عليها ، وعلى الشاهد طلب المزيد من التوضيح متى كانت الأسئلة غير مفهومه لديه .

٧. التحدث بوضوح وطلاقة وبعبارات دقيقة وصوت مسموع للجميع .

٨. الاستعداد النفسي الجيد لمرحلة مناقشة الدفاع الذي قد يميل إلى اتباع تقنيات سيكولوجية للتأثير على الشاهد عن طريق :-

- توجيه أسئلة عديدة دون ترك وقت لإجابة الشاهد Rapid – fire questions .
- الأسئلة التي توحي بالإجابة Leading questions .
- استبدال كلماتك بشكل مغاير من العبارات وكأنك قصدتها .
- الظهور بمظهر الصديق ثم الانتقال إلى مظهر عدائي .
- اطلاق بعض العبارات الحرجة أو الجارحة .
- السكوت والنظر إليك لفترة طويلة لمضايقتك أو استفزازك .[1]

[1] Arkin stanley s. Et al. Prevention and prosecution of computer and high technology crime . new yourk mathew bender 1999.

١,٢,٣- حجية أدلة الحاسب الآلي و الأدلة الجنائية الرقمية

استقر الفقه والقانون الوضعي على أن للقاضي سلطة واسعة في تقدير الأدلة واستنباط القرائن وما تحمله الوقائع من دلالات ، شريطة أن يكون الدليل ثابتًا بيقين ، مرتبطًا بالواقعية الرئيسة ومنسجمًا مع التسلسل المنطقي للأحداث. من الطبيعي أن ينسحب هذا الرأي على الأدلة الجنائية الرقمية باعتبارها أحد أقسام الأدلة المادية العلمية ، بل أكثر منها حجية في الإثبات ، لأنها محكمة بقواعد علمية وحسابية قاطعة لا تقبل التأويل[1] كما أنها في ذات الوقت معالجة بوسائل التقنية المعلوماتية التي أصبحت تستغل في الجرائم المستحدثة. ورغم عدم توفر التشريعات الموضوعية والشكلية التي تنظم التعامل مع الحاسوب وتقنية المعلوماتية لم تواجه المحاكم مشكلة في تعاملها مع الأدلة الجنائية الرقمية وذلك للأسباب التالية :

١. الثقة التي اكتسبها الحاسوب والكفاءة التي حققتها النظم الحديثة للمعلوماتية في مختلف المجالات.
٢. ارتباط الأدلة الجنائية الرقمية وآثارها بالجريمة موضوع المحاكمة.
٣. وضوح الأدلة الرقمية ودقتها في إثبات العلاقة بين الجاني والمجني عليه أو بين الجاني والسلوك الإجرامي.
٤. إمكانية تعقب آثار الأدلة الرقمية والوصول إلى مصادرها بدقة.

---

(1) Amadt, B.L. and Plaza, E., "Case-based Reasoning: Foundational Issues, Methodological Variations, and System Approaches", Alcom-Artficial Intelligence Communications, 7 (1), 1994, P. 18.

٥. قيام الأدلة الرقمية على نظريات حسابية مؤكدة لا يتطرق إليها الشك مما قوى يقينية الأدلة الرقمية.

٦. انتهاء العلم برأي قاطع إلى صحة النتائج التي توصل إليها علوم الحاسوب.

٧. الأدلة الجنائية الرقمية يدعمها – عادة – رأي خبير ، وللخبرة في المواد الجنائية دورها في الكشف عن الأدلة وفحصها وتقييمها وعرضها أمام المحاكم وفق شروط وقواعد نظمها القانون وأقرها القضاء[1] .

٨. انتشار الجريمة التخيلية Cyber Crime وجرائم التقنية العالية High-tech. Crimes كظاهرة مستحدثة لم يترك مجالاً للبحث عن وسائل لتحقيق العدالة في سياق تلك الأنماط من السلوكيات إلا من خلال ذات التقانة التخيلية.

من القواعد العامة للبينة المستقرة في القانون الوضعي عدم قبول البينة السمعية Hearsay Evidence أمام المحاكم الجنائية ، إلا في حالات استثنائية حصرها القانون بشروط مشددة. ويعزي عدم قبول البينة السماعية إلى استحالة استجواب ومناقشة الشاهد الأصلي بواسطة المحكمة والدفاع[٢]. ولاستثناءات البينة السماعية علاقة بمناقشة حجية الأدلة الجنائية الرقمية. على سبيل المثال ، لقد تضمنت القواعد الاتحادية للبينة في الولايات المتحدة الأمريكية نصًا يعتبر السجلات والبيانات المنظمة بدقة بينة مقبولة أمام الجنائية استثناء للبينة السماعية. وبناءً على تلك القواعد تعتبر التقارير والمعلومات والبيانات المحفوظة في أي

---

[1] أكدت أحكام النقض في جمهورية مصر العربية عدة مبادئ منها: "أنه إذا كانت المسألة المعروضة عليها من المسائل الفنية البحتة التي لا تستطيع المحكمة أن تشق طريقها إليها لإبداء الرأي فيها ، فالمحكمة ملزمة بندب خبير ، بل إنها ملزمة بالأخذ برأي هذا الخبير ، إذا كان العلم قد انتهى برأي قاطع إلى صحة النتائج التي تم التوصل إليها" نقض ١٣ مايو ١٩٦٨ ، مجموعة الأحكام رقم (١٠٧) حكم رقم ٣٠٣ لسنة ١٩٦٨ ، ص ٣٨.

(2) Hoey, A. "Analysis of the Police and Criminal Evidence Act-Computer Generated Evidence", Web Journal of crrent legal issues. Black stone press Ltd. 1996, P. 73.

شكل ، وكذا الوقائع والأحداث والآراء ونتائج التحاليل المنقولة بواسطة أشخاص ذوي معرفة وخبرة في نطاق الأنشطة والممارسات المنظمة بينة مقبولة أمام المحاكم الجنائية لكونها بيانات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من الأدلة السماعية. والأدلة الجنائية الرقمية من هذا القبيل ، لكونها معدة بعمليات حسابية دقيقة لا يتطرق إليه

قبول الأدلة الجنائية الرقمية

إذا كنا بصدد مناقشة مدى إمكانية قبول الأدلة الرقمية admissibility of digital evidence للإثبات أمام المحاكم، فينبغي النظر إليها بمعيار القواعد العامة المعتمدة لقبول الأدلة الجنائية. وهنالك ثلاثة قواعد تجعل الأدلة الجنائية مقبولة وهي:

١. المصادقة Authentication
٢. الدليل الأفضل (الأصل) Best evidence rule
٣. إستثناءات البينة السماعية Exceptions of the hearsay evidence

ولا شك أن النظر إلى الأدلة الرقمية من خلال هذه القواعد العامة للأدلة الجنائية تطرح تساؤلات حرجة حول مدى قدرة المحققين التقليديين في الحكم على الأدلة الرقمية وتصنيفها إلى أدلة أصلية أم صورة موثقة رسمياً، وما إذا كانت الأقوال والإفادات المنقولة عبر الحاسب الآلي والإنترنت هي بينة سماعية أم أصواتاً تم إعدادها وتغذيتها أو دبلجتها بصورة رقمية. كل ذلك يتطلب من المحققين أن يكونوا على درجة عالية من المعرفة والإلمام بتفاصيل عمليات تقنية المعلومات والاتصالات. كما يطرح في هذا السياق سؤال أكثر أهمية فيما يتصل باعتماد المحققين على خبراء تقنية المعلومات. فهل في وسعهم مناقشة التقارير التي يقدمها الخبراء .

تمر الأدلة الجنائية منذ نشأتها بمراحل عديدة تتطلب مهارات خاصة للتعامل وهي[1]:

- مرحلة تلقي البلاغ الأول لوقوع الجريمة، ويقتصر دور الضابط المسؤول في هذه المرحلة على التعرف على مسرح الجريمة والمحافظة عليه والتحفظ المؤقت على الأدلة.

- مرحلة التحقيق، ويكون دور المحقق فيها تأسيس حلقات الحدث وتفتيش مسرح الجريمة وإيجاد العلاقة بين الأدلة المتوفرة من جهة والجريمة والمجرم والصحية من جهة أخرى.

- مرحلة التأمين على الأدلة، ويقوم فيها فني مسرح الجريمة بإجراءات حفظ وتحريز الأدلة ونقلها إلى مختبرات الأدلة الجنائية وتحليلها.

- مرحلة الاتهام والإدعاء، ويقوم فيها وكلاء النيابة بتقييم الأدلة واتخاذ قرارات هامة قد يكون من بينها إنهاء التحقيق، بشطب الاتهام، الإحالة إلى إجراءات تتخذ خارج نظام العادلة الجنائية أو الإحالة إلى المحاكمة.

- مرحلة المحاكمة التي يقوم فيها القضاة بالوقوف على الأدلة ومدى كفايتها لإثبات التهمة بما لا يدع مجالاً للشك.

٢,٢,٣ – معايير وقواعد الأدلة الرقمية

لأهمية الطبيعة الدولية لالجرائم السايبرانية وشبكات الإنترنت حرصت المنظمات الدولية ذات العلاقة على بلورة معايير وقواعد وموجهات متفق عليها حتى تكون الأدلة

[1] محمد الأمين البشرى، " الأدلة الجنائية الرقمية ودورها في الإثبات" المجلة العربية للدراسات الأمنية والتدريب، الرياض: جامعة نايف العربية للعلوم الأمنية،٢٠٠٢

الرقمية قابلة للتداول والتبادل وفق أسس قانونية. ويجري تطوير تلك المعايير والقواعد بصفة مستمرة لتعميمها واعتمادها كمبادىء جديدة لهذا النوع من الأدلة بجانب مبادئ وقواعد البينة التقليدية، ومن تلك المعايير والقواعد:

أولاً: المبادئ الدولية لأدلة الحاسب الآلي

International Principles for Computer Evidence

التي تم تطويرها بواسطة المنظمة الدولية لأدلة الحاسب الآلي (IOCE). وتهدف هذه المبادئ إلى تزويد الأجهزة المعنية بالتحقيق في الجرائم السايبرانية بآليات وأساليب واضحة تمكنهم على العمل والتعاون والتنسيق على المستوى الدولي. وقد اعتمدت (٥) من تلك المبادئ بواسطة الأجهزة القانونية المعنية في عدد من الدول المتقدمة، بينما يجري التشاور حول (٣) مبادئ أخرى. والمبادئ المعتمدة حتى الآن هي:

(١) الأدلة الرقمية عند ضبطها أو حجزها يجب أن لا تؤدي العمليات إلى تغيير.

(٢) عند الحاجة لدخول أي شخص على الأدلة الرقمية الأصلية ، يجب أن يكون الشخص مؤهلاً.

(٣) يجب توثيق جميع إجراءات ضبط الأدلة الرقمية وتأمينها وحفظها أو نقلها.

(٤) الأفراد الذين يقومون بالإجراءات المتعلقة بالأدلة الرقمية مسؤولون عن ما في حيازتهم من تلك الأدلة.

(٥) على الأجهزة التي تتعامل مع الأدلة الرقمية إثبات مدى التزامها بهذه القواعد.

ثانياً: معايير تبادل الأدلة الرقمية

Standards for the exchange of digital evidence

التي أعدتها مجموعة العمل العلمية للأدلة الرقمية (SWGDE) بالتعاون مع المنظمة الدولية للأدلة الرقمية. عرضت هذه المعايير لأول مرة في المؤتمر الدولي لجرائم التقنية العالية والعلوم القضائية الذي عقد في لندن عام ١٩٩٩ . وقد اعتمدت مسودة هذه المعايير بواسطة أجهزة إنفاذ القوانين في الولايات المتحدة الأمريكية وبريطانيا واليابان. وتعرف هذه المعايير العبارات الرئيسية في سياق الأدلة الرقمية وأدلة الحاسب الآلي وتنظم إجراءات التفتيش والحجز على هذا النوع من الأدلة وطرق نقلها وتوثيقها بالقدر الذي يؤمن جودتها. كما تتضمن هذه المعايير توصيفاً للأشخاص المؤهلين للتعامل مع الأدلة الرقمية وشروط قبولها أمام القضاء.

ثالثاً:

مبادئ الدول الثمانية G8 للإجراءات الخاصة بالأدلة الرقمية، والتي اعتمدت وأوصت الدول الأخرى باعتماد مجموعة المبادئ والمعايير التي أعدتها المنظمة الدولية لأدلة الحاسب الآلي.

٣. ٣- أساليب التعامل في مرحلة المؤسسات الإصلاحية والعقابية

مرتكب الجريمة الالكترونية ، كما سبق أن أشرنا ، ليس مجرماً تقليدياً ، ولكن ربما تتوفر فيه بعض خصائص المجرم التقليدي التي أفصحت عنها نظريات علم الاجرام ، خاصة ما يتصل منها بالظروف الاجتماعية والصحة النفسية . غير أن المؤكد أن مرتكب الجريمة الالكترونية يمتلك مهارات مهنية وذكاءً متقدماً ومعرفة واسعة ، ليس في علوم الحاسب الألي وهندسة الاتصالات فحسب ، بل تمتد معرفته الخاصة وثقافته العامة لمجالات هامة كالتجارة والاقتصاد والعمليات المصرفية والنظم الادارية للأعمال المدنية

والعسكرية وغيرها من الأنشطة الانسانية التي تعتبر ميداناً يمارس فيها جرائمة أو هواياته .

الذي يهمنا في المؤسسات العقابية والاصلاحية هو تحقيق أهداف السياسة العقابية بتأهيل المذنبين واعادتهم إلى المجتمع مرة أخرى أعضاء صالحين يسهمون في البناء والتنمية فإذا أخذنا المجرم التقليدي والبرامج المتوفرة في المؤسسات العقابية لاصلاحه وتأهيله ، نجدها برامج عالية التكلفة ومتدنية المردود في معظم دول العالم لأسباب أهمها تدني المستوى التعليمي والثقافي لدى المجرمين التقليديين وضعف الامكانيات مقابل الأعداد الكبيرة من نزلاء السجون . كل ذلك جعل المؤسسات العقابية في كثير من أنحاء العالم مدارس يتخرج منها المجرمون التقليديون أكثر اجراماً وأكثر استعداداً للمواصلة على طريق الجريمة . ويعزز موقفهم هذا نظرة المجتمع السلبية لنزلاء السجون ، وعدم توفر فرص عمل تمنهم من العيش الكريم والانخراط في المجتمع من جديد [١] .

والسؤال الذي يُطرح هنا ، هل تصلح المؤسسات العقابية الراهنة وبرامج الإصلاح والتأهيل والسياسات العقابية لمرتكبي الجرائم السايبرانية ؟ وما هي الاحتياجات الإصلاحية اللازمة للمجرم الالكتروني ؟ وكيف يمكن الاستفادة منه في المجتمع بعد إصلاحه وإعادته إلى المجتمع [٢] .

المجرم الالكتروني ، سواء كان مجرماً مبتدئاً أو مجرماً عائداً ، هو شخص يملك علماً ومعرفة متقدمة في ميدان مازال وسيظل مطلوباً في السوق .

[1] Manilyn D. Mc shane and franklin Williams . the management of conectional institutions : valum (5) , current lssves in criminal justice New York : Garland Publishing , 1993

[2] Richard Wortly , situational Prison Control : Crime reven tion in correctional institutions . london : Cambndge University Press , 2002

المجرم الالكتروني المحترف ثروة قومية ضلت الطريق وجرى استثمارها في المكان الخطأ ولا شك أن إيداعه السجون التقليدية إهدار لهذه الثروة القومية ، بل ربما يكون ذلك أبعد من مجرد إهدار للثروة القومية ، متى تمكن المجرم الالكتروني من الاختلاط بالمجرمين التقليديين وتبادل الثقافات معهم ، ليخرج كل من المجرم الالكتروني والمجرم التقليدي بمعارف إجرامية أكثر خطورة .

١,٣,٣ – كيفية معاملة المجرم الالكتروني :

يتطلب معاملة المجرم الالكتروني فلسفة جديدة تواكب التحديث الذي طرأ على المجرم ومعارفه . معاملة المجرم الالكتروني تحتاج إلى مؤسسه عقابية الكترونية ، تلبي احتياجات المجرم المراد إصلاحه وتهذيبه فالمؤسسة العقابية هنا لا تهدف إلى محو المهارات وأدوات الجريمة من ذاكرة المجرم ، بل ترشيد تلك المهارات وتعزيزها ، وإعادة استثمارها في المكان الصحيح ، وذلك وفق ما يلي :-

١. إنشاء مؤسسات عقابية وإصلاحه متخصصة لمعاملة المذنبين في الجرائم السايبرانية . وتتكون هذه المؤسسات من معاهد ومختبرات للحاسب الآلي ونظم الاتصالات ومصانع للبرمجيات وهندسة الحاسب الآلي ومجسمات من المرافق الحيوية وقواعد البيانات وأجهزة الاتصالات .

٢. تكون المؤسسات العقابية والاصلاحية الخاصة بمرتكبي الجرائم السايبرانية مؤسسة بحتية وتعليمية ، يعمل فيها والنزلاء على تطوير أبحاثهم وإجراء تجاربهم بجانب قيامهم بالتدريس والتعليم ونقل خبراتهم للطلاب والمتدربين من العاملين في مجال نظم المعلومات .

٣. إعداد المؤسسات العقابية والاصلاحية بعيداً عن النمط التقليدي للسجون من حيث الشكل والمضمون والمظهر الأمني ، وتسخير التقنيات الالكترونية لإدارتها وتأمينها على أن يكون للنزلاء دوراً بارزاً في تنظيم وإدارة تلك المؤسسات .

٤. توفير كادر تعليمي متخصص في مجال هندسة الحاسب الآلي وتقنياته المختلفة للعمل في المؤسسات العقابية والاصلاحية ، وظيفته التدريس والارشاد والاشراف العلمي والفني واكتشاف المواهب ، بجانب كوادر أخرى متخصصه في الاصلاح والتوجيه والارشاد الاجتماعي والصحة النفسية ، وظيفتها معالجة الجوانب الاجتماعية والنفسية التي قادت النزيل إلى طريق الجريمة الالكترونية .

٥. تهيئة فرص العمل للمدانين في الجرائم السايبرانية بعد الافراج عنهم للاستفادة من مهاراتهم في صناعة البرامج وتأمين نظم المعلومات وأمن وسلامة الاتصالات وتطوير صناعات تقنية المعلومات .

٦. يتم تقييم وتصنيف المادنين في الجرائم السايبرانية ودراسة حالاتهم الاجتماعية والنفسية وقياس مقدراتهم في مجال نظم الحاسب الآلي وتقنيات الأنترنت والاتصالات واختيار من تتوفر فيهم صفة المجرم الالكتروني المحترف أو الهاوي الواجب الحاقه بالمؤسسة العقابية والاصلاحية [١] .

٧. تطوير المؤسسات العقابية والاصلاحية الخاصة و بالمدانين في الجرائم السايبرانية لتصحيح مؤسسات لنشر ثقافة المعلوماتية وإعداد الموارد البشرية وتعزيز صناعات البرمجيات اللينة Software والصعبة Hard ware .

[1] Lyle Wildes and Joekelly . Positive Attitude Development workbook . Amagon books , 2009

لا شك إن استحداث منشآت عقابية وإصلاحية متخصصة في معاملة مرتكبي الجرائم السايبرانية ، يحتاج إلى تشريعات وطنية ونظم وقواعد خاصة ، علاوة إلى بلورة فلسفة لهذا النوع من المعاملة المتميزة التي لا تتوفر لجميع نزلاء المؤسسات العقابية . كما أنه من الضروري وضع قواعد لنظام العمل والانتاج وحقوق ملكية انجازات النزلاء وتصنيف خدماتهم إلى خدمات عقابية تعوض الأضرار التي نجمت عن الجرائم السايبرانية وأخرى استثمارية يجوز للنزلاء التمتع بكامل حقوقهم فيها . ويتوقف تطوير هذا النوع من المنشآت العقابية والاصلاحية على تطوير نظام العدالة الجنائية الالكترونية على النحو الوارد في الفصل التالي من هذا المؤلف . إن اتجاه الجريمة المتسارع نحو استخدام تقنيات الحاسب الألي والانترنت . يتطلب حوسبة نظام العدالة الجنائية وعملياتها ، الا أن ذلك لا يعني إيداع جميع المدينين في المؤسسات العقابية الخاصة لمرتكبي الجرائم السايبرانية .

٣. ٤ – نظام العدالة الجنائية السايبراني

حُظيت نظم العدالة الجنائية بأجهزتها وتشريعاتها باهتمام خاص خلال القرن العشرين، في كافة المستويات الدولية والاقليمية والوطنية . وقد لعبت الأمم المتحدة وأجهزتها المتخصصة دوراً واضحاً في تطوير قواعد وموجهات العدالة الجنائية ، واعتماد اتفاقيات دولية وقوانين نموذجية أسهمت في تعزيز نظم العدالة الجنائية وترسيخ المفاهيم والمتطلبات التي نادى بها الاعلان العالمي لحقوق الانسان في كثير من دول العالم .

تأسست نظم العدالة الجنائية في تلك المرحلة على القوانين الجنائية وقواعد البينة ونظم العقاب والاصلاح التقليدية لمواجهة الجرائم التقليدية التي عرفتها المجتمعات منذ أقدم العصور ونحن نشهد اليوم انتقال الجريمة إلى مرحلة جديدة ، هي مرحلة الجريمة الرقمية القائمة على تقنيات المعلومات والاتصالات الحديثة ، قد لا يكون من الممكن

التعامل معها بنظم تقليدية . فإذا كانت معاملاتنا اليومية وأنشطتنا الاجتماعية والاقتصادية تتجه بخطى متسارعة نحو النهج الرقمي الالكتروني ، فكيف لنا أن نكفل أمن وسلامة تلك الأنشطة بخلاف المناهج الرقمية الالكترونية . وإذا كانت أنشطتنا الاجتماعية والاقتصادية السالبة وسلوكيات أفراد المجتمع المارقين على القانون تتخذ من تلك النهج الرقمية الالكترونية وسيلة لتحقيق أهدافها الاجرامية ، فكيف لنا أن نحقق العدالة الجنائية ونعزز تدابير الوقاية من الجريمة دون اللجوء إلى وسائل وأليات رقمية الكترونية لإدارة عمليات العدالة الجنائية في جميع مراحلها المتداخله .

في هذا السياق يقول Tofflers [1]

" نظام العدالة الجنائية نظام اجتماعي وظيفته توفير العدل والمحافظة على الاستقرار الاجتماعي فإذا كان المجتمع مستقراً ، يظل نظام العدالة الجنائية مستقراً يعمل دون تحديات ، بإعتباره مرآة المجتمع Mirror of the society .تكون نظام العدالة الجنائية الراهن خلال الموجه الأولى والموجه الثانية First ware second ware من النهضية التكنولوجية الحديثة ، وقد قفزت المجتمعات الآن إلى الموجه الثالثة Third ware من النهضة التكنولوجية ، وعجزت عمليات العدالة الجنائية التي تكونت في الموجه الأولى والموجه الثانية من النهضة التكنولوجية عن اللحاق بعمليات وحركة

الموجه الثالثة ، التي تضاعفت فيها تعقيدات الجريمة وسرعتها عن سرعة حركة نظام العدالة الجنائية العتيق "

[1] Toffler, Alvin, and Heidi Toffler . Creating a New world Civilization، Atlanta : Turner Publishing , 1994

رغم ظهور هذه المفاهيم في وقت مبكر ، ورغم النداءات المبكرة التي أطلقتها الأمم المتحدة والداعية إلى حوسبة نظم العدالة الجنائية Computerization of the criminal justice system قبل ثلاثة عقود[1] ، لم تتقدم تلك المحاولات إلا في جوانب ادارية محدودة من عمليات الشرطة والمؤسسات الاصلاحية .

عناصر نظام العدالة الجنائية الالكتروني :

تتكون منظومة العدالة الجنائية الالكترونية من عناصر رئيسية تؤثر عليها وتتأثر بمعطياتها وهي :

١. الجريمة الالكترونية .
٢. المجرم الالكتروني .
٣. ضحايا الجريمة الالكترونية .
٤. تشريعات الجريمة الالكترونية .
٥. أجهزة نظام العدالة الجنائية الالكتروني .

ثانياً : المجرم الالكتروني

المجرم الالكتروني أو مرتكب الجرائم السايبرانية هو شخص يختلف كثيراً عن المجرم التقليدي الذي تناولته نظريات علم الإجرام بالتحليل والتعريف والتصنيف . مرتكب الجريمة الالكترونية شخص يتميز بالذكاء والإلمام بعلوم ومعارف التقنيات العالية للمعلومات والاتصالات . قد يكون المجرم هنا مهنياً أو خبيراً أو موظفاً كبيراً في المؤسسة أو الموقع الذي يرتكب فيه جريمته الالكترونية . وقد يكون باحثاً أو هاوياً يختبر قدراته وبرامجه الخاصة لاختراق المواقع أو اكتشاف الأسرار الخاصة بالغير المخزنة في قواعد

[1] Archambeault , w. G. And Archambeault , G.J. Computers in Criminal Justice Administration , Cincinnati : Anderson , 1988, p. 40

البيانات . مرتكب الجرائم السايبرانية ليس مجرماً بالميلاد أو مجرماً بالصدفة أو شخصاً دفعته الظروف الاجتماعية والاقتصادية كما تقول نظريات علم الاجرام .

مرتكب الجريمة الالكترونية – في الغالب – من الطبقة الاجتماعية الوسطى ، نال قدراً من التعليم والتأهيل واكتسب مهارات معلوماتية يعيش في وضع اجتماعي يسمح له بالتعامل مع أجهزة الحاسب الألي وبرامجه ، فهو رغم سلوكياته السالبة يُعد ثروة قومية ينبغي حسن استغلاله . ومن هنا يكون من الضروري التعامل معه كمجرم متميز . فالتحقيق معه ليس بالسهل لذكائه ولغته التي قد لا يفهمها المحقق العادي ، سواءً كان شرطياً أو وكيلاً للنيابة أو قاضياً . كما أن العقوبات التقليدية كالحبس والسجن والغرامة وغيرها من السياسات العقابية السائدة لا تصلح لردعه أو اصلاحه والاستفادة من طاقاته الكامنة .

ثالثاً : ضحايا الجرائم السايبرانية

ضحايا الجرائم السايبرانية قطاع واسع من المجتمعات الحضرية بأطفالها ، نسائها ، مؤسساتها الاجتماعية والاقتصادية ، بنياتها التحتية وقيمها وتقاليدها . ضحايا الجرائم السايبرانية قطاع بلا حدود شخصية أو اقليمية . قد لا يكون الضحايا على علم بما أصابهم من ضرر مادي أو معنوي . وقد لا يدرك الضحايا طبيعية النشاط الاجرامي الالكتروني في الغالب ، بحكم التعقيدات الفنية أو جهل الضحية بالعلوم الحديثة وتقانة المعلومات . سحب درهم واحد أو فلس من حساب الضحية شهرياً ، قد لا يعني شيئاً بالنسبة للفرد ، بينما تكرار السحب من عملاء أي بنك ولمدة أعوام يُعد ضرراً اقتصادياً كبيراً . بهذه الخصائص يشكل ضحايا الجرائم السايبرانية عبئاً على نظام العدالة الجنائية وتدابير الوقاية منها . الضحايا هنا لا يسهمون في اكتشاف الجرائم أو التحقيق فيها وقد لا يصلحون للمثول أمام المحاكم لتقديم أدلة تساعد على تحقيق

العدالة الاجنائية . وهم فوق ذلك قد يسهمون عن جهل في مساعدة مرتكبي الجرائم واخفاء آثار الجريمة وتخريب الأدلة الرقمية .

خامساً : أجهزة نظام العدالة الجنائية الالكترونية

يقتضي تفعيل نظام العدالة الجنائية الالكتروني تهيئة أجهزة متخصصة في مجال عمل هذا النظام . يتكون نظام العدالة الجنائية الالكتروني من ذات الأجهزة التي يتكون منها نظام العدالة الجنائية الالكتروني ، الا أنها مؤهلة للتعامل مع الجرائم والمجرمين في بيئة التقنيات العالية للمعلومات والاتصالات . ينبغي أن تكون لهذه الغاية أجهزة شرطة الكترونية Cyber Cops ، نيابة الكترونيه ، قضاء الكتروني ومنشآت عقابية تعمل بنهج الكتروني . تتجه أجهزة العدالة الجنائية التقليدية الآن نحو حوسبة عملياتها وسجلاتها . وقد انتقلت بعض أجهزة العدالة الجنائية التقليدية إلى التعامل مع مراكز الشرطة الالكترونية ونظم تسجيل البلاغات والتحقيق فيها الكترونياً . ولعل كل ذلك مدعاه إلى تعزيز التخصصات وهيكلة نظم خاصة للعدالة الجنائية الالكترونية ، ومراجعة الموارد البشرية العاملة في هذا المجال واعدادها بما يتلاءم مع المستجدات التقنية .

تشكل الموارد البشرية العاملة في مجال نظام العدالة الجنائية الالكترونية العمود الفقري لنجاح النظام وتحقيق أهدافه . الموارد البشرية اللازمة لنظم المعلومات والاتصالات من أكثر المهن ندرة في سوق العمل . ومن الصعب على الأجهزة الحكومية أن تنافس مؤسسات القطاع الخاص في استقطاب الموارد البشرية المتميزة في مجال التقنيات العالية . لذا ينبغي تكوين وتأهيل عناصر خاصة بأجهزة نظم العدالة وتصميم مناهج للتعليم والتدريب مرتبطة بعمليات نظام العدالة الجنائية الالكترونية تكفل استقطاب وارتباط الموارد البشرية الخاصة بأجهزة نظام العدالة الجنائية الالكتروني .وينبغي أن تكون لتلك الموارد توصيفاً وظيفياً ومهناً معتمدة لها أصولها وفروعها ..

خاتمـة

نخلص مما تقدم إلى الآتي:-

١. هنالك قناعة عامة بوجود مخاطر أمنية متزايدة للجرائم الإلكترونية و الجرائم السايبرانية Cyber crime ،خاصة والتقنيات العالية للمعلومات والإتصالات لم تعد قاصرة على الجرائم السايبرانية و جرائم الإنترنت المستحدثة، بل تمتد لتصبح عنصرًا أو أداة في مختلف أنماط الجرائم التقليدية والممارسات الإجتماعية السالبة. أن جرائم السايبرانية – بالإضافة إلى الخسائر المالية الكبيرة التي تسببها لمؤسسات القطاع العام والخاص – أصبحت تلحق أضرارًا بالغة بالمجتمعات المحافظة. ولعل من مقتضيات مواجهة هذه الظاهرة الإعداد العلمي للمحققين وتزويدهم بالمعرفة الفنية والقانونية ذات العلاقة بهذا النوع من الجرائم.

٢. مع تزايد أنماط الجرائم الرقمية تتضاعف حالات لجوء المحققين ورجال الشرطة والقضاء إلى خبراء الحاسب الآلي والإنترنت للاستعانة بهم في كشف غموض المعلومات وأدلة الحاسب الآلي والأدلة الجنائية الرقمية الآخذة في الانتشار. ولكن مع مرور الزمن سوف تصبح الأدلة الجنائية الرقمية جزءًا أو عنصرًا من عناصر الجريمة بمختلف أنواعها ، عندئذٍ قد لا يتمكن خبراء الحاسب الآلي والإنترنت من تقديم العون للمحققين ، الشيء الذي يقتضي الشروع في إعداد رجال الشرطة والنيابة العامة والقضاء بالكيفية التي تمكنهم من التعامل مع الأدلة الجنائية الرقمية ، والتي لا غنى عنها.

٣. تعتبر أدلة الحاسب الآلي و الأدلة الجنائية الرقمية من أكثر أنواع الأدلة المادية وفرة وثباتـًا. وهي مخزنة في الأجهزة الرقمية المختلفة أو منقولة عبر شبكات الاتصال وتشكل ثروة للعدالة الجنائية متى أحسن استغلالها.

٤. للأدلة الجنائية الرقمية حجية في الإثبات أمام المحاكم المدنية والشرعية ، لما لها من أسس علمية مؤهلة نالت بها الثقة والمصداقية. فالنظرية الرقمية مصدرها علم تقنية المعلومات الذي فرض نفسه على الإنسان بإنجازاته الملموسة.

٥. يتطلب التعامل مع أدلة الحاسب الآلي و الأدلة الجنائية الرقمية معرفة تامة بأصولها ونظرياتها وتقنية المعلومات. كما يتطلب قواعد جديدة للبينة وتشريعات تنظم إجراءات جمع وتأمين هذا النوع من الأدلة ، بالقدر الذي لا يتعارض مع الحقوق الدستورية وسرية المعاملات الفردية، مما يستوجب توفر عناصر جديدة من المحققين.

٦. تسبب الجرائم السايبرانية القلق وعدم الاطمئنان في معظم دول العالم، خاصة في الدول المتقدمة التي وضعت جُلَّ معاملاتها وبياناتها الخاصة والعامة في بيئة شبكات إلكترونية معرضة لمخاطر يصعب التنبؤ بها.

٧. تشكل عملية اكتشاف الجرائم السايبرانية والتحقيق والإدعاء والمحاكمة فيها مشكلة حقيقية لنظم العدالة الجنائية التقليدية، بسبب تدني المعرفة بالتقنيات العالية وسط رجال تنفيذ القانون.

٨. يفرض دور البحث التقني القضائي للحاسب الآلي نفسه كوسيلة لا غنى عنها للتعامل مع الجرائم السايبرانية في مختلف مراحلها.

٩. هنالك حاجة غير محدودة لخبراء البحث التقني القضائي للحاسب الآلي، وصعوبة بالغة في استقطابهم للعمل في مجال العدالة الجنائية ومواجهة الجرائم السايبرانية، خاصة وهم خبراء هندسة الحاسب الآلي وتقنيات المعلومات والاتصالات الأكثر طلباً في سوق العمل.

١٠. أفضل الممارسات العالمية السائدة للتعامل مع الجرائم السايبرانية المستحدثة هي:

(١) اتجاه معظم الدول المتقدمة إلى سن تشريعات ذات طابع دولي قائمة على مبادىء الاتفاقية الدولية لمكافحة الجرائم السايبرانية.

(٢) معالجة مشكلات الاختصاص على مستوى الدوائر القضائية الوطنية والدولية.

(٣) استحداث مختبرات الأدلة الرقمية.

(٤) استحداث وتطوير مهنة خبير البحث التقني القانوني للحاسب الآلي Computer Forensies Expert .

(٥) الانتقال إلى حوسبة عمليات أجهزة العدالة الجنائية.

(٦) نشر الوعي الأمني المعلوماتي.

المراجع

أولاً: المراجع العربية

١. البشرى محمد الأمين، التحقيق في الجرائم السايبرانية والإنترنت، المجلة العربية للدراسات الأمنية والتدريب، الرياض: أكاديمة نايف العربية للعلوم الأمنية، ٢٠٠٠ .

٢. جميل صليبا، المعجم الفلسفي، بيروت: دار الكتب اللبناني، ١٩٧١ .

٣. الحويقل، معجب بن معدي، دور الأثر المادي في الإثبات الجنائي، الرياض: أكاديمة نايف العربية للعلوم الأمنية، ١٩٩٩ .

٤. سرور أحمد فتحي، الوسيط في قانون الإجراءات الجنائية، القاهرة: دار النهضة العربية، ١٩٨١ .

٥. سلامة، مأمون، الإجراءات الجنائية في التشريع المصري، القاهرة: دار الفكر العربي ١٩٧٧ .

٦. عوض، محمد محي الدين، قانون الإجراءات الجنائية السوداني، معلقاً عليه، القاهرة: المطبعة العالمية، ١٩٧١ .

ثانياً: المراجع الأجنبية

1. Amdadt, B.L. and plaza, E. "Case, Based Reasoning: Fundamental issues, Methodological variations and system Approaches" Aicom-Artificial intelligence communications, 7(1), 1994.

2. Britz, M.T. Computer Forensic and Cyber Crime: An Introduction> Prentice Hall, 2003.

3. Burgess, A. and Hazelwood, R. Practical Aspects of Rape Investigation: A Multidisciplinary approach. New York: CRC. Press. 1995.

4. Burgess, A. and Hazelwood, R.- crime classification Manual, San Francisco: Jossey Bass, 1997.

5. Carter David and Katz, A.J., Computer crime: An Emerging challenge for law enforcement. FBI Law Enforcement bulleting. 1996.

6. Charles, E. O'Hara, Fundamentals of criminal investigation (3rd) spring field: Charles Thomas. 1973.

7. Charles R. Swanson, Neil chamelin and Leonard territo. Criminal investigation (7th) London: Mc Graw Hill, 2000.

8. Elbushra Mohamed Al Amin, "Reliability of Scientific Evidence", New Trends in Criminal Investigation and Evidence, Oxford: Intersentia, 1995.

9. Eoghan Casey, Digital Evidence and Computer Crime. New York: Academic press, 2000.

10. Gaines, L., and Miller, R., Criminal Justice in Action, California: Thomson Wadsworth, 2005.

11. Harold Tuthill, Individualization Principles and Procedures in Criminalistics Oregon: lightning powder. 1994.

12. Hoey, A. "Analysis of the police and criminal Evidence Act. Computer Generated Evidence, Web Journal of current legal issues. Blackstone press, 1996.

13. Hollinger, R.C, Crime, Deviance and the Computer, Brookfield: Dartmouth publishing co. 1997.

14. Icove, D., Seger, K. and Vonstorch, W. Computer Crime, A Crime Fighter's Handbook. Sebastpol: O'Reilly and Associates, 1995.

15. John Madinger and Sydey Zalopay, Money Laundering- A Guide of Criminal Investigators. London: CRC press 1999.

16. John Nikell and Joh Fisher, Crime, Science and Methods of Forensic Detection. Lexington: University Press of Kentucky 1999.

17. Parker Donn, Fighting Computer Crime. New York: charles scribners 1983.

18. Parke Donn, Fighting Computer Crime: a New Frame work for protecting information, New York. John wiley 1998.

19. Philip, J., Law Enforcement and Digital Evidence, Handbook of Information Security, New York: John wiley & Sons, 2005.

20. Rama Subramanian "Techno-Legal Perspective of Cyber Crimes Sentencing" Stockholm criminology Symposium, Stockholm University press, 2006.

21. Richard Saferstein, Criminalistics: An Introduction to Forensic Sceince,(5^{th}) Englewood cliffs: prentice Hall, 1995.

22. Richard Saferstein, Criminalistis: An Introduction to Forensic Science. Upper Saddle River: Prentice, Hall. 1998.

23. Ronald L. Mendle, Investigating Computer Crimes: A Primer for Security Manager, New York: Charles Thomas, 1998.

24. Schneider, Brent, High – Technology Crime: Investigating Cases Involving Computers, San Jose: K S K publications, 1999.

25. Shimomura Tsutomu, and Mrkoff, J. Applied cryptography: Protocols and Source Code, New york: John Wiley, 1996.

26. Shimomura Tsutomu, The pursuit of Kevin Mitnick, America-s Morst wanted computer Outlaw by the Man who did it> New York: Hyperion 1996.

27. Brenner Susan, W., "Cyber Crime Investigation", Murdock University Electronic Journal of Law, 2001.

28. Thomas, A. Johnson, Forensic Computer Crime Investigation. London: CRC press, 2006.

29. Turvey Brent, Criminal Profiling: An Introduction to Behavioral Evidence Analysis. London: Academic press 1999.

30. Sudhir Aggarwal et.al. E-crime Investigative Technologies, Proceedings of 41st Hawaii International Conference on system Sciences, NIJ 2008