International Review of Law, Computers & Technology

ISSN: 1360-0869 (Print) 1364-6885 (Online) Journal homepage: https://www.tandfonline.com/loi/cirl20

Catches to the right to be forgotten, looking from an administrative law perspective to data processing by public authorities

A.M. Klingenberg

To cite this article: A.M. Klingenberg (2016) Catches to the right to be forgotten, looking from an administrative law perspective to data processing by public authorities, International Review of Law, Computers & Technology, 30:1-2, 67-75, DOI: 10.1080/13600869.2015.1125161

To link to this article: https://doi.org/10.1080/13600869.2015.1125161

© 2016 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 29 Feb 2016.

Submit your article to this journal

Article views: 803

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at https://www.tandfonline.com/action/journalInformation?journalCode=cirl20

www.manaraa.com

International Review of Law, Computers & Technology, 2016
Vol. 30, Nos. 1–2, 67–75, http://dx.doi.org/10.1080/13600869.2015.1125161

Routledge
Taylor & Francis Group

Catches to the right to be forgotten, looking from an administrative law perspective to data processing by public authorities

A.M. Klingenberg*

Department of Public Law and Public Administration, Faculty of Law, University of Groningen, 9700 AS Groningen, the Netherlands

Public authorities process personal data. In most cases these data are processed because there is a legal obligation to do so, or because processing is necessary for the performance of a task carried out in the public interest. The right to be forgotten or to erasure will, in this situation, play a limited role in the protection of the rights of the individual. There is even a public interest in maintaining archives, thus in not forgetting. At the same time, the possibility exists that not forgetting might be more valuable for the protection of rights of data subjects then forgetting. In the case of data processing by public authorities, it is important that the processing is based on a law. A close watch should be held on the grounds that public authorities use to justify the processing. As the right to be forgotten will play a limited role in the protection of the rights of data subjects in the case of data processed by public authorities, it is important to emphasize the right of access and rectification of data. It is therefore essential that the controller is transparent to the public with regard to the processing of data.

Keywords: right to be forgotten; public authorities; archives

Introduction

For public authorities, several obligations exist in order to process personal data. When they are not able to process information, public authorities will not be able to exercise their public tasks well. A request for a building permit or for social welfare, for example, cannot be processed without processing personal data. There are also legal obligations for public authorities to store (personal) information. The Dutch Act on Archives, for example, obliges public authorities to keep information stored for different periods, ranging from several years until for ever. In addition. the Dutch Land Registry Office (the Kadaster) – whose public task is to collect 'information about registered properties in the Netherlands, record them in public registers and in cadastral maps and make this information available to members of the public, companies and other interested parties in society' – processes personal information in order to exercise its public duty.[1]

In the proposal for a General Data Protection Regulation (DPR), Article 17 provides the data subject's right to be forgotten and to erasure (European Commission 2012). In this article, I will explore the question of whether this right to be forgotten will, in the case of data processing by public authorities, improve the rights of the data subjects. The right not to forget is probably just as important. If the right to be forgotten might not be

*Email: a.m.klingenberg@rug.nl

© 2016 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

المنارة للاستشارات
www.

of use in the relationship between public authority and citizen, in which other ways can the rights of the data subject be strengthened?

To answer the above question, I will first set out why a public authority processes personal data. What are the legal grounds on which public authorities ground the processing of personal data? The right to be forgotten, as proposed by the European Commission, will then be discussed in the light of administrative law. It looks like the right to be forgotten will be of (very) limited use when public authorities are processing personal data. So how can we strengthen data subject's rights? Solutions are to be found in a strict application of the reasons for public authorities to start processing data and in explicit rights of access and rectification for the data subject.

Material scope of the DPR

A first question is whether the DPR will be applicable on the processing of data by public authorities. The DPR will be applicable on the processing of data by controllers, in the context of activities of an establishment in the Union. Article 2, DPR, determines the material scope of the Regulation. Section 2, sub a, of this article provides that the regulation does not apply to the processing of personal data in the course of an activity that falls outside the scope of Union law, in particular concerning national security. Article 2, section 2, sub c, excludes processing by Member States, when carrying out activities concerning common foreign and security policy. And finally, article 2, section 2, sub e, DPR, excludes data processing for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties by competent authorities from the scope of the DPR.

Almost the same restriction on the material scope as in art. 2, DPR, is provided for in Article 3(2), Directive 95/46. This directive is at present the basis for the regulation of data protection within the EU member states. In case law based on this directive, the ECJ decided that 'the applicability of Directive 95/46 cannot depend on whether the specific situations [. . .] have a sufficient link with the exercise of the fundamental freedoms guaranteed by the Treaty' (*Österreichischer Rundfunk*). More important, however, is Article 16 of the Treaty of the Functioning of the European Union, which establishes the principle that everyone has the right to the protection of personal data. Section 2 of Article 16 introduces a specific legal basis for the adoption of rules on the protection on personal data:

> The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

Also important is that data protection, which is part of the fundamental right to privacy, is a general principle of Community law and is laid down in Article 8 of the Charter of fundamental rights of the European Union. Obviously, data processing, whether or not it has a relation with the exercise of the fundamental freedoms guaranteed by the Treaty of the Functioning of the European Union, falls within the scope of Union law.

Therefore, every processing of personal data falls within the scope of Union law, unless specifically prejudiced. This article will consider all data processing by public authorities, except the data processing that takes place concerning national or common security, and

المنارة للاستشارات
www.

data processing by competent authorities. Consequently, data processing concerning the exemptions mentioned in Article 2, section 2, sub a, c and e, DPR will not be a part of this article.

Public authorities and data processing

As mentioned in the introduction, without processing personal data, public authorities will not be able to fulfil their public task well. Accordingly, processing personal data is, in these cases, inextricably bound up with the general interest. In light of the DPR, the processing of personal data is only lawful if the data are processed under one of the grounds mentioned in Article 6 DPR. At present, the same grounds apply for the lawfulness of data processing, according to Article 6 Directive. The legal grounds on which the public authority processes personal data are enumerated in Article 6 DPR.

Consent

The first ground listed in Article 6, is that the data subject gives his or her consent to the processing of the personal data. This ground seems problematic in the citizen–government relation. To me it seems that public authorities, when they are processing personal data while exercising public functions, will have to state reasons why the public interest needs the authority to process these data. And if the public interest compels the authority to process personal data, this then applies to everyone, consenting and non-consenting citizens alike. After all, if one data subject is consenting and someone else is not, the question arises of whether the public authority is still able to fulfil its public task. If the public body is able to fulfil its public task without the data of the non-consenting persons, the collected data of the consenting persons may not be relevant for the purpose for which they are collected.

Another question to be answered is whether consent will ever be a valid legal ground for data processing for public authorities exercising public powers. There is a significant imbalance between the position of the data subject and the controller. Article 7, section 4, expressly states that consent does not provide a legal basis for processing in the case of a significant imbalance in power. To me it seems unclear whether this is recognized in nr. 34 of the preamble at the DPR. In this preamble it is mentioned that:

> where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

It is unclear when an obligation is imposed. Consent, being used as a ground to process personal data, for example in an asylum procedure, or an application for social welfare, is not freely given. The consequence of refusing to consent will be that the request or application will be deemed inadmissible or disallowed. This situation is described in the preamble, under nr. 33. It says there that consent does not provide a valid legal ground where the individual is not able to refuse or withdraw consent without detriment. In the above-mentioned examples, it is clear that the consent cannot be refused without detriment and so should not be used.

Furthermore, the question arises of whether using the condition of consent in government data processing may be contrary to the basic principle that every citizen will be

المنارة للاستشارات
www.

treated equally. To decide differently upon a request from citizens, to the extent that they are willing to share their personal data, might result in a forbidden distinction between people. Therefore, the conclusion can be reached that the ground of consent should not be used as a legal ground for data processing by public authorities, when exercising public powers.

Necessary for compliance with legal obligation of public task

When exercising public powers, public authorities will have to use another legal ground for processing than consent. The public authority will have to ground the data processing on the legal basis that the processing is necessary for compliance with a legal obligation to which the controller is subject, as written in Article 6, section 1, sub c. The other applicable ground is that the processing is necessary for the performance of a task carried out in the public interest or in an exercise of official authority vested in the controller, Article 6, section 1, sub e.

These grounds seem broad. It is possible that the question of whether a task is carried out in the public interest will be answered by the public authority itself. Public authorities are also competent to establish their own rules. In that way, a public authority can establish its own legal obligation to process personal data. In this light, section 3 to Article 6, seems an important addition. This section states that

> The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or (b) the law of the Member State to which the controller is subject.
>
> The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.

This provision does not exist in the Directive 95/46. In Dutch public administration there probably are several databases concerning personal data, for which are not covered in a law. This new provision will therefore compel public authorities to rethink their databases and the reasons they collect and store personal data. This provision will guarantee that processing of data by public authorities will only then take place when provided for in a law. From the last sentence of section 3 and from nr. 36 of the preamble by the DPR, it follows that the law must meet the requirements on limitations of the rights and freedoms of the Charter of Fundamental Rights of the EU.

A public interest *not* to forget

As far as an interest exists for individuals in having their personal data removed, there is also a public interest in not removing data. First of all, this might be laid down in different national Acts on Archives, such as the Dutch Act on Archives. In this act, a public interest is recognized in keeping data stored from several years to eternity. The public interest in keeping (government) data stored comes from the interest of cultural heritage and the interest in keeping (government) data available. There is also an interest in keeping data that have played or may play a role in public debate.

Case law freedom of expression

Not forgetting not only plays a role in government files, but also in newspaper archives. In the case of *Times Newspapers vs United Kingdom*, a Russian-born businessman brought

المنارة للاستشارات
www.

proceedings for libel in respect of two articles printed in the *Times* newspaper. In these articles he is linked to money laundering and to a suspected mafia boss (*Times Newspapers ltd v The United Kingdom*). Both articles were uploaded to the *Times* newspaper's website on the day they were published. After proceedings before British Courts, the case was settled and Times Newspapers agreed to pay a sum of money.

Times Newspapers was refused to appeal against the rule in the Duke of Brunswick case (from 1849) by the Court of Appeal, and later by the House of Lords. This rule states that each publication of defamation gives rise to a separate cause of action. In the context of the internet this means that a new cause of action accrues every time defamatory material is accessed. This rule is named the Internet Publication Rule. Times Newspapers brought this case before the European Court of Human Rights, where it contended that this Internet Publication Rule restricts its ability to maintain a publicly accessible internet archive. It pointed to the chilling effect that this rule has upon freedom of expression. The *Times* also contested the finding of the Court of Appeal that the maintenance of archives constitutes an insignificant aspect of freedom of expression, and pointed to the importance of the integrity and availability of historical records to an open and democratic society.

First, the Court found that the maintenance of internet archives is a critical aspect of the important role the internet plays in enhancing the public's access to news and the dissemination of information in general. According to the Court, such archives fall within the ambit of the protection afforded by Article 10 Convention. Further, the Court agreed with the substantial contribution made by internet archives to preserving and making available news and information. Such archives constitute an important source for education and historical research. The Court also recognized the important role of the press in maintaining and making available these archives.

The margin of appreciation in striking the balance between the right of freedom of expression and other competing rights, however, is likely to be greater where news archives of past events rather than news reporting of current affairs are concerned. In this specific case, the Court concluded that the newspaper – as it eventually did – could and should have attached a qualification to the article. This qualification should indicate that a libel action had been initiated in respect of that same article published in the written press. Such a requirement is not considered a disproportionate interference with the right of freedom of expression. There is no requirement however to remove the potential defamatory article. Moreover, the Court did not recognize a right to data removal in this case.

In a comparable case, *Węgrzynowski and Smolczewski v. Poland*, the Court stressed the substantial contribution made by internet archives 'to preserving and making available news and information' (*Węgrzynowski and Smolczewski v. Poland*). Under reference to the above-mentioned case of Times Newspapers, the Court stressed that maintaining and preserving these archives is a valuable secondary function of the press, in light of Article 10 Convention. Furthermore, the Court accepted that it is not the role of judicial authorities to 'engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations.' The Court reiterated that the legitimate interest of the public, in accessing the public internet archives of the press, is protected under Article 10 Convention.

There is a public interest not to forget. First of all, there are archives. These two cases show that the ECrtHR does not accept that personal data have to be removed from internet archives that are kept by the press. It is notable is that in both cases the use of personal data had been found unlawful by national courts because of libel. The Court accepted that this unlawfulness can be rectified by the requirement to publish an appropriate qualification to

المنارة للاستشارات
www.

an article contained in an internet archive. In this way, the Court reconciled the interest of maintaining archives with the interest of respect for private life. The Court certainly did not recognize in these cases a right to be forgotten or to erasure.

Removal vs right to access

When the data subject asks for erasure, does this imply that all data have to be removed? This may interfere with an important right, the right of access. Erasing all information has as a consequence that data containing information about recipients are also being removed. After all, when data are removed there is no possibility to assess to whom personal data have been given in the past. And this right of access plays an important role in the protection of personal data. In Article 8 of the Charter of fundamental rights of the European Union, it is specifically mentioned in section 2, that 'everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'.

How does the right to be forgotten relate to the right of access to information? The first section of Article 15 DPR provides that:

> The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information [. . .].

The right of having personal data erased is not mentioned in this Article.

The Rijkeboer case

In a case where the Dutch Council of State referred to the Court of Justice for a preliminary ruling, the Advocate General in his opinion asked which right is more important, the right of access or the right to erasure (*Rijkeboer, Opinion of AG Ruiz-Jarabo Colomer*). The case is about Mr. Rijkeboer, a citizen who requested the College van burgemeester en wethouders van Rotterdam (the Board of Aldermen of Rotterdam) to notify him of all instances to which data relating to him from the local authority personal records had, in the two years preceding the request, been disclosed. He wished to know the identity of those persons and the content of the data disclosed to them. His request had been partly complied with, in so far that he could only be notified about data relating to the period of one year proceeding his request.

The data were requested from the GBA – a (comprehensive) electronic Register of Births, Deaths and Marriages. The Dutch Law on personal data held by local authorities (the Wet GBA) is the law that gives provisions about these data held by local authorities. This law, the Wet GBA, provides that the local authorities are to retain details of any communication of data for one year following that communication. So the request from Mr. Rijkeboer, to obtain data for a period of 2 years, was denied because of the provision of this act.

This leads to the question: are data to be removed as quickly as possible, or should they be kept for good reasons? Two articles of Directive 95/46 are involved in this case: Article 6, which provides that Member States are to ensure that data are 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected of for which they are further processed', and Article 12, that provides for a right of access to data. According to Article 12:

المنارة للاستشارات
www.

> Member States shall guarantee every data subject the right to obtain from the controller [. . .] confirmation as to whether or not data relating to him are being processed and information at least as to the [. . .] recipients or categories of recipients to whom the data are disclosed, [. . .].

Advocate General Ruiz-Jarabo Colomber calls this the internal tension of the exercising of the right to privacy. He writes that there are powerful reasons for arguing that deletion is the key to the system laid down by Directive 95/46. On the other hand, he writes that access is the true subjective dimension of the directive. Access namely enables individuals to react in defence of their interests. So, he concludes in §32 of his opinion, that in Directive 95/46 the obligation to delete data is secondary to the right of access:

> The articles concerned confer a right which is born when the file is created and dies when it is deleted. Accordingly, the erasure of personal data is merely a moment in the life of the right of access, a feature which is determined and justified by Article 12.

He writes that he is convinced that the right of access is to ensure that a data subject is aware of the information that is held about him, and that the right of access is a basic pillar of the directive.

In its ruling, the ECJ first pointed out that this case concerns two categories of data (*Rijkeboer*). The first category concerns personal data kept by the local authority. These data are called the basic data and they may be stored for a long time. The second category concerns information on recipients or categories of recipients to whom those basic data are disclosed. These data relate to the processing of the basic data. The ECJ observed in §54 that the right of access must relate to the past. If that were not the case, it argued, a data subject would not be in a position to exercise his or her right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for the damage suffered. Timely or premature erasure of personal data can harm the data subject's right. This case shows that erasure of data can violate the data subjects' rights, and that storing data can strengthen the rights of data subjects.

A right to be forgotten and erasure for public authorities

Article 17 DPR provides a right to be forgotten and to erasure. The provision of Article 17 DPR does not seem to bring a new right for data subjects. Directive 95/46 also provides in Article 12 for a right to have personal data removed. The right to be forgotten and erasure is thus not an entirely new right. The data subject has the right to ask for erasure of data when four different grounds apply. These grounds are that the data are no longer necessary, the data subject withdraws consent, objects to the processing, or the processing of the data does not comply with the DPR.

For public authorities, there are two catches to this article. One is that the right of civilians is not served by erasing his or her personal data. This is shown in the Rijkeboer case. The other catch is that public authorities are, under an obligation to publish public information. The public has, a right to receive information.

Public authorities that are processing personal data will process these data mainly because of a legal obligation or a task carried out in the public interest. In a lot of these cases the public authority has the competence to make legally binding decisions about persons. When the public authority, after deciding, immediately removes the personal data, for the reason that the data are no longer necessary in relation to the purpose they were collected, it may harm the citizen's (legal) position. The citizen is not able to examine whether the decision is taken on the right assumption or facts.

المنارة للاستشارات
www.

Public authorities may make information containing personal data public on the basis of freedom of information laws, or other statutory obligations. In that case, section 2 of Article 17, may apply. A controller is obliged, according to this provision, to have all links to published data erased, or to inform third parties that the data should be removed. When a freedom of information law provides a valid legal ground to publish these data, the public authority should be able to rely on that ground. This provision might have a 'chilling effect' on public authorities fulfilling their tasks under freedom of information laws.

Conclusion

In this article, the right to be forgotten and erasure is examined in the case of data processing by public authorities. Every processing of personal data falls within the scope of Union law, unless specifically prejudiced. This article considers data processing by public authorities, except the data processing that takes place concerning national or common security, and data processing by competent authorities.

Processing personal data by public authorities differs from the processing carried out by other (legal) persons. Public authorities have special powers and competences. They take decisions that change the legal status of people, whether they like that or not. In this situation, when a public authority exercises its public power, there is no free choice to make data available to the authority. That leads to the conclusion that the ground of consent should not be used as a legal ground for data processing by public authorities when exercising public powers.

Important for the right of data subjects is section 3 to Article 6 DPR. A similar provision does not exist in Directive 95/46. This provision will guarantee that processing of data by public authorities will only then take place when provided for in a law. My expectation is that this provision will compel public authorities to rethink their databases and the reasons they collect and store personal data, when laid down by law.

As far as an interest exists for individuals in having their personal data removed, there is also a public interest in not removing data. First of all, this is laid down in different national Acts on Archives, such as the Dutch Act on Archives. In this act, a public interest is recognized in keeping data stored from several years to eternity. The public interest in keeping (government) data stored comes from the interest of cultural heritage and the interest in keeping (government) data. There is also an interest in keeping data that have played or may play a role in public debate.

Case law from the ECrtHR shows that this Court does not accept that personal data have to be removed from internet archives kept by the press. It is notable that in both cases mentioned the use of personal data had been found unlawful by national courts because of libel. The Court accepts that this unlawfulness can be rectified by the requirement to publish an appropriate qualification to an article contained in an internet archive. In this way the Court reconciles the interest of maintaining archives with the interest of respect for private life. The Court certainly does not recognize in these cases a right to be forgotten or to data removal.

In the case of Rijkeboer, the ECJ ruled against erasure of data in favour of a right of access. Without stored data, a data subject is not in a position to exercise his right to have data presumed unlawful of incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for the damage suffered. Timely or premature erasure of personal data may harm the data subject's right. This case shows that erasure of data can violate the data subjects' rights, and that the data should have been kept.

المنارة للاستشارات
www.

The right to be forgotten and to erasure is, in the case of data processing by public authorities, not an obvious improvement of the rights of the data subjects. The situations in which this right can be invoked will be limited. The rights of civilians are in some cases not served by erasing data. On the other hand, there is a right for the public to receive information in public debate. Internet archives play an important role. The right to be forgotten risks that it precludes a general right of not forgetting, and an individual interest in keeping data.

Conflict of Interest Disclosure

No potential conflict of interest was reported by the author.

Note

1. http://kadaster.nl/window.html?inhoud=/english/.

References

Case C-553/07 *Rijkeboer* [2009] ECR I-3889.
Case C-553/07 *Rijkeboer* [2009] ECR I-3889, Opinion of AG Ruiz-Jarabo Colomer.
European Commission. 2012. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) 25-1-2012, COM(2012) 11 final 2012/0011 (COD)/.
Joint Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk* [2003] ECR I-4989.
Times Newspapers ltd v UK ECHR 2009-I 377.
Węgrzynowski and Smolczewski v Poland App no 33846/07 (ECtHR, 16 July 2013).

www.