



SÖDERTÖRNS HÖGSKOLA | STOCKHOLM

The Right of Access to Information and the Right to Privacy

A Democratic Balancing Act

PATRICIA JONASON
& ANNA ROSENGREN (EDS.)

Working paper 2017:2

This publication, as well as the workshop that gathered the researchers whose articles are included in this volume, are part of a project financed by the Swedish Research Council (Vetenskapsrådet): *Privacy, the hidden aspect of Swedish democracy. A legal and historical investigation about balancing openness and privacy in Sweden*, no 2014-1057.

Södertörns högskola
(Södertörn University)
Library
SE-141 89 Huddinge

www.sh.se/publications

© Authors



Attribution 4.0 International (CC BY 4.0)

This publication is licensed under a
Creative Commons Attribution 4.0 License

Graphic form: Per Lindblom & Jonathan Robson
Printed by Elanders, Stockholm 2017

Working Paper 2017:2

ISBN 978-91-88663-30-6

Contents

On Democracy, the Right of Access to Information and the Right to Privacy

PATRICIA JONASON & ANNA ROSENGREN

5

Ethical Destruction? Privacy concerns regarding Swedish social services records

SAMUEL EDQUIST

11

Medical Records – the Different Data Carriers Used in Sweden from the End of the 19th Century Until Today and Their Impact on Confidentiality, Integrity and Availability

RIKARD FRIBERG VON SYDOW

41

The Right to Access Health Data in France: The Contribution of the Law of January 26, 2016

WILLIAM GILLES

61

The Swedish Black Box. On the Principle of Public Access to Official Documents in Sweden

ANNA ROSENGREN

77

Online Proactive Disclosure of Personal Data by Public Authorities. A balance between transparency and protection of privacy

PATRICIA JONASON

111

Data Protection Authorities in Central and Eastern Europe: Setting the Research Agenda

EKATERINA TARASOVA

139

Media Freedom and Pluralism in the Digital Infrastructure

NICOLA LUCCHI

151

Abstracts

161

About the authors

167

On Democracy, the Right of Access to Information and the Right to Privacy

On December 13th 2016, an international and trans-disciplinary workshop took place at Södertörn University, Sweden. The topic around which the researchers had gathered was *The Right of Access to Information and the Right to Privacy: A Democratic Balancing Act*. The workshop was one of the many events which celebrated the 250th anniversary of the Swedish *Freedom of the Press Act*, the first legal instrument in the world laying down the right of access to official documents. An act, the first version of which was published in 1766, will of course have changed to form and content over the years, but original concepts are still possible to trace. Notably, the current right of access to official documents that all citizens benefit from today, is quite easily recognizable in the explanation from 1766 that various official documents must be “immediately [...] issued to anyone who applies for them”.¹ This right of access has received much well-deserved international acclaim over the years, as it constitutes an important element of democratic systems. By way of example, the Council of Europe stated in its recommendation on access to government records from 1979 that democratic systems are able to “function adequately only if the people in general and their elected representatives are fully informed”, to which it added that “the freedom of information has operated successfully in Sweden for more than two centuries”.²

Freedom of information is not only important for democracy described from a deliberative and pluralistic point of view, but also for democracy in

¹ Hogg, Peter, His Majesty’s Gracious Ordinance Relating to Freedom of Writing and of the Press (1766) (translation), in Mustonen, Juha (red), *The world’s first Freedom of Information Act: Anders Chydenius’ legacy today*, Kokkola 2006, p. 13.

² Council of Europe, Recommendation 854 (1979), *Access by the public to government records and freedom of information*, 1979, p. 1.

terms of the rule of law. The right of access to information certainly provides tools for rendering the public authorities accountable and promote compliance with the law of these actors.³

As the title of the workshop indicates, the right of access and its importance for democracy were discussed in conjunction with the right to privacy. Indeed, these two rights may conflict, not in the least when official documents disclosed by public authorities contain personal information. Additionally the fact that official documents containing personal data are often created – and disclosed – without the knowledge of the registered person also raises questions in terms of privacy rights.

Yet, as has been pointed out by scholars, not only the right of access, but also privacy is of great importance for democracy in the two senses of the terms.⁵ A starting point for the workshop was, therefore, the assumption that the right of access to information and the right to privacy are both necessary preconditions for a democratic society. Researchers from a broad range of fields were invited to discuss how these assumptions should be examined, and how the balance between the two interests should be assessed when conflicting with each other. The objective of the workshop was to broaden our understanding of various national and disciplinary approaches to the democratic balance between the right of access and the right to privacy.

Together, the articles in this volume convey important insights about the necessary and precarious balance between the right of access and the right to privacy. Below, some overarching tendencies and tentative concluding remarks are presented.

Several articles include a historical perspective of legal and technological developments. In some instances, an effect related to democracy taken from a deliberative point of view may be discerned. This is the case with the

³ Blanc-Gonnet Jonason, P. & Calland R. (2013) Global Climate Finance, Accountable Public Policy: Addressing The Multi-Dimensional Transparency Challenge. *Georgetown Public Policy Review*, vol. 18, Number 2.

⁵ See e.g. Regan, Priscilla. *Legislating Privacy. Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995 and MacNeil, Heather. Information privacy, liberty and democracy. *Privacy and Confidentiality Perspectives: Archivists and Archival Records*, Behrnd-Klodt, Menzi L. and Wosh, Peter J. eds. Chicago: The Society of American Archivists, 2005, pp. 67–81; Blanc-Gonnet Jonason, Patricia. Démocratie, transparences et Etat de droit – La transparence dans tous ses états, *European Review of Public Law* (2015). Vol. 27, nr 1. VITALIS, André, *Informatique, pouvoir et libertés*, Economica 1988, 2e édition.

article by Nicola Lucchi, Associate Professor in law, who discusses media freedom and media pluralism. Media freedom deals with editorial independence and access to information for journalists, areas which lately have come under pressure and thus touch upon the theme of right of access of the trans-disciplinary workshop. This could also be said to be the case with media pluralism, the possibility for individuals to satisfy their information needs. In this area, Lucchi identifies the challenges of concentration of power of certain Internet content aggregators and the development of “filter bubbles” that keep certain information outside of reach of the individual. Both in terms of media freedom and media pluralism we may therefore detect difficulties related to access to information, a development which in turn has a potentially negative impact on democracy.

Besides the topic of right of access to information, the privacy in relation to technological development is clearly pointed out in several articles. In two of the articles, we are furthermore reminded that privacy has been high on the agenda long before the digitalisation of our time. This is a theme brought forward by two archival science researchers, Samuel Edquist and Rikard Friberg von Sydow. Edquist studies the political and legal development concerning retention and destruction of social services files, which are documents containing very sensitive personal data on the persons in need of help. Although the current digitalisation certainly brings privacy matters to the foreground, Edquist emphasises how privacy has been a subject intensely discussed for decades. This theme is present also in the article by Rikard Friberg von Sydow on the development of data carriers for medical records during the last 150 years. Both authors contribute to the research on privacy through their historical analyses, showing that privacy matters have been the topic of much debate long before the current technical development.

Another theme deals with the current applicable legislation for protecting privacy. In her article on proactive disclosure, i.e. online publishing by public authorities without the previous request for the release of information, public law expert Patricia Jonason shows that there is some opacity about the legal framework to be applied. Samuel Edquist touches upon a similar topic as he describes the political debate during the last decades regarding retention or destruction of social services files, and shows that the development has been all but straightforward.

The situations described by Jonason and Edquist is a theme similar to the one brought up by historian and archival law expert Anna Rosengren. The object of analysis in the article by Rosengren is the Swedish principle of

public access to official documents (“offentlighetsprincipen” in Swedish). From a literature study, she had identified several factors having an influence on the creation and release of official documents. The high number of factors makes the workings of the principle of public access to official documents a very complex one, to the extent that it becomes largely impossible for individuals to know how personal data about her might be collected, and subsequently released from official documents and further used. Rosengren therefore combined the identified factors with concepts from systems theory regarding the black box, used for systems that cannot be directly observed. The resulting *Swedish Black Box model* was used to shed light over the Swedish principle of public access to official documents, and showed that factors related to technology and routines, not to legislation, could affect the creation and release of official documents.

The analysis of the technological development of medical records by Friberg von Sydow furthermore shows us that privacy has become more difficult to protect in certain ways. The author points out that protecting data from persons not allowed to access it has become more difficult, just as it has become more difficult to hinder and monitor changes of data as compared to earlier versions of data carriers for medical records. On the other hand, Friberg von Sydow shows that it has become increasingly easy for the different types of medical staff as well as for the patient herself to reach the current medical records, in comparison to e.g. the handwritten notes of the physician of previous times. The medical records being easily reachable could be interpreted as a step towards democratisation, rendering the power relationship between the physician and the patient a more even one. The issue of medical records is also the focus of public law expert William Gilles. In his paper, a presentation and analysis of the latest development of the French legislation in the medical field is provided. Gilles, who presents and compares the previous health database system with the new one, underlines the advancements made to improve the benefits of the system for administrative, research and other public purposes while protecting and also reinforcing privacy.

Privacy is furthermore dealt with at an institutional level in the article by social scientist Ekaterina Tarasova. In this article, an in-depth analysis of research on Data Protection Authorities (DPA's) is carried out. Tarasova points out the need for a distinction between formal and informal independence of the DPA's in different countries. As one of the main contributions of the paper, she makes the point that research on DPA's in Central and Eastern Europe in societies with a lower level of trust would be bene-

ficial, as new insights could emerge shedding new light also on the DPA's of western countries. Patricia Jonason also addresses the institutional aspect of privacy protection. In her article on online disclosure of public information she gives much space to the manner in which the Swedish Data Protection Authority, *Datainspektionen*, carries out the balancing between the interest of transparency and the interest of protecting privacy.

Summing up the results from the various articles, our tentative concluding remarks are the following: Firstly, we may conclude that the right of access and the right to privacy and the balancing of the two is a multifaceted and topical theme over time. Articles sometimes show positive development of some of these areas. This was the case with Rikard Friberg von Sydow who described that reaching medical records have become easier with technological advancement, a development which may be interpreted as a step towards democratisation as patients get easier access to their own data. The paper of William Gilles also shows a positive development in the field, as the description of detailed rules for the access to data in health databases indicates that public policies benefit from these rules at the same time as they improve the protection for privacy. In other instances, recent developments seem to indicate lack of predictability regarding what kind of information might be provided individuals about how her personal data is handled. This, in turn, may have a negative impact on democracy. The article by Patricia Jonason, for instance, indicates difficulties to overview the legislation for proactive disclosure. Yet the General Regulation on Data Protection that will be in force from May 2018, is likely to provide an opportunity for the Swedish legislator to rethink the issue of online proactive disclosure by public authorities. The article by Samuel Edquist on the political debate leading up to the current situation of retention of few, and destruction of most, social services acts, also recalls the fact that knowing about how public authorities handle personal data might be difficult. To what extent may we assume that individuals are aware of how their personal data is going to be handled? According to the article by Anna Rosengren on the *Swedish Black Box*, predicting the handling of one's personal data in accordance with the Swedish principle of public access seems an overwhelming task, if not impossible. This lack of predictability might have implications for the rule of law.

Among the conclusions we may draw from the workshop, and the articles emanating from it, is the confirmation of the need to strike the balance between the right of access and the right to privacy. This is certainly difficult, but since the two interests are both of such importance for demo-

cracy, we constantly need to make the effort. The articles in this volume contain information on some of the areas that need our further attention.

Patricia Jonason & Anna Rosengren

Ethical Destruction?

Privacy concerns regarding Swedish social services records

SAMUEL EDQUIST

Every year, in every Swedish municipality, there is a routinised procedure to either destroy or retain records that the social services authorities have assembled regarding individuals under its care. This happens after five years have passed since the last annotation regarding the person involved in the files. The routine is legally based in the Swedish Social Services Act, where there is a sharp line between mandatory destruction for certain records, and mandatory retention of other documents. The basic rule is to destroy the records after five years. However, files for persons born the 5, 15 or 25 any month must be kept, as well as all records in a specific set of Swedish counties and municipalities. Furthermore, certain kinds of social services records must be kept for anyone: if they are associated with investigations on adoptions or parenthood, as well all records on children (under 18) being placed in foster care.¹

In this article, I will explore the development of this system by studying the background of the Social Services Act decided by the Swedish Parliament (the *Riksdag*) in 1980, as well as the further investigations that finally put the rules on destruction and retention of social services records into practice in 1991. Before that, the social services records were generally stored as a whole in the archives. This mandatory disposal of archival records is an effect of a wider tendency from the late 20th century to legally destroy information due to them being considered menacing to privacy. I will show that this is a disputed tendency, and I will present a preliminary model of various interests and agent groups that are put to the front in the debates on these issues. I intend to show the complexity of the questions

¹ The present legislation: SFS 2001:453 and SFS 2001:937, with the relevant sections latest changed in SFS 2015:982 and SFS 2007:1316 respectively.

involved, and how the changing practises and debates in modern history on how to deal with sensitive information engulf several conflicting interests and groups of actors.² It is not only a question of individual privacy versus mass data in the control of large organisations, but also on economy, on the construction of future heritage, and the various interests of professions and other sections of society. The choice between destroying information or keeping it secret, have fostered alliances or conflicts between, and sometimes within, groups such as archivists, academic researchers, journalists, and professionals within social services.³

Destruction of information has generally been justified by economic reasons (saving everything would be impossible), redundancy arguments (the important information should not be drowned in masses of less important records), and by more or less explicit political reasons in order to protect individuals or institutions. Privacy concerns constitute the only official legitimization of politically motivated destruction in Sweden.⁴ Beside social services records, privacy concerns have been legally stipulated over the last decades for several official databases and computer registers, as well as, for example, camera surveillance records.⁵ This measure, which has been called “ethical destruction”,⁶ is chosen when privacy concerns are considered overweighing others such as those of transparency, future research, and the possibilities to reuse information. Furthermore, it is put into practice when secrecy legislation is not considered enough. The decisions on ethical destruction have sometimes led to controversies, with conflicting views regarding the choices between making documents secret (but keeping them) and destroying them. The social services records are especially fruitful to study, being the result of an important institution of society, and since there is a thin line in the legislation between mandatory destruction

² This article is based on initial investigations within the research project *Ethical destruction? Privacy concerns regarding official records in Sweden, 1900–2015*, financed by the Swedish Research Council.

³ See also Bundsgaard 2006.

⁴ See e.g. Riksarkivet, *Om gallring* (1999), p. 7. There are also well-testified examples of unofficial destruction of official documents in order to protect e.g. interests in the military and the intelligence service has though happened, see Wallberg 2005.

⁵ Öman 2006.

⁶ In Swedish *etisk gallring*, which is the most common expression in Swedish archival discourse along with *integritetsgallring*. Even though mainly those opposing the principle have previously used the phrase, I aim at applying it impartially, representing ideas and practices of destruction of records motivated by the ethical concerns of protecting privacy.

and mandatory retention line, the contours of the issue are sharp.⁷ The debates on ethical destruction can be regarded a battlefield between proponents of privacy on the one hand, and on the other hand those of research and keeping evidence of governmental measures. Such controversies are a fruitful starting point for analyses on wider ideological structures within society. Studying differing views of privacy concerns uncover vital aspects of the relationship between individual and society as a whole.

There have been numerous academic discussions on the tensions between privacy, secrecy and freedom of information in various disciplines. As has been stressed by previous researchers, the so-called “information society” has by many been seen as leading to great dangers to privacy, which is often regarded a cornerstone of liberal conceptions of democracy. Thereby, the old question of balancing between the individual and the state is put to the front.⁸ One of the research currents – most prominent in the early development of the field – has been openly normative: it is held that a surveillance society has developed, being a menace to privacy. This research mirrors the discourse on Big Brother and mass surveillance that early on became cornerstones of the privacy proponents, and there has been a visible overlap between academic discourse and public debate. For example, the political scientist Alan Westin’s book *Privacy and Freedom* (1967) became a cornerstone both for public debate and academic research. He explored the new abilities of governments to gather personal information with new computerised systems and increased levels of control, using examples of social security numbers, personality tests, increased information in census data, and other “surveillance techniques”. Typically for the continuing debate, he also mentioned George Orwell’s *Nineteen Eighty-Four* as the iconic dystopia on the horizon.⁹ There are also explicitly normative examples of research with the opposite view – not least within the field of archival science where privacy concerns are typically regarded as dangers to the integrity of archival evidence.¹⁰

⁷ It is evident in contemporary practice that strictly obeying the legislation may be complicated and sometimes even impossible, since actual files are sometimes poorly registered or arranged. For example, files that should be destroyed can be more or less inseparable from files that should be kept, see e.g. Stockholms Stadsarkiv, “Rutinbeskrivning för att gallra och leverera socialtjänstakter 2017”, pp. 9, 10 and 12.

⁸ Bennett 1992, pp. viii–ix.

⁹ Westin 1967, pp. 57–63, 158–168; Flaherty 1989.

¹⁰ E.g. Cook & Waiser 2010.

The major bulk of research – in Sweden as well as in other countries – tend to focus on issues of privacy concerns in connection with the computerised society of the recent decades, especially since the 1960s onwards, and the political regulation of data protection.¹¹ The example of the social services records, however, testify that issues of privacy and the perceived need for ethical destruction of information are not only connected to computers and digital records, which has dominated previous research. Until recent years, the social services records have been in paper format, and yet privacy concerns were high on the agenda. There are strong examples of analogue archival records being used in the past for surveillance, repression and even worse, such as the well-known example of the German Nazi regime using century-old church records for establishing racial belonging.¹²

Handling social services records: from the beginning to the 1960s

The social services sector in Sweden has grown from the former age-old system for housing and handling poor people, traditionally a responsibility for the lowest-level local governments: the municipalities.¹³ With the development of a more formal social services institution as part of the modern welfare system, the question of protecting sensitive information in social services records came to the fore. In 1936, a law was decided on social services registers (*socialregister*), which stipulated absolute secrecy for all outsiders (other than authorities needing access concerning the social matter).¹⁴ In fact, it was only in 1961 that the law was changed giving possi-

¹¹ E.g. Bennett & Raab 2006; Blanc-Gonnet Jonason 2006; Lind, Reichel & Österdahl (eds.) 2015; Lawrence 2016. There are also surveys analysing the subject of privacy in a longer history of ideas perspective, e.g. Schoeman 1992; Vincent 2016. For previous research on data protection issues in Sweden, see also the section *The 1970s investigations and the 1980 Social Services Act*. Today, there are ongoing research projects that border to mine, e.g. Anna Rosengren and Patricia Jonason's project on the overall tensions between openness and privacy in political and legal discourses, and Johan Fredrikzohn's PhD project in the field of history of ideas, about destruction of information in Swedish history.

¹² Vismann (2000) 2008, pp. 126–127.

¹³ See e.g. Pettersson 2011.

¹⁴ SFS 1936:56 section 8. SFS 1937:249 section 14: general 70 years secrecy for documents of this kind.

bility for researchers to get access to the registries.¹⁵ However, so far there were no suggestions – as far as I know – to destroy parts of the material for privacy reasons.

The general growth of the welfare system, as well as the rapidly increasing possibilities to create documents due to enhanced reproduction techniques, resulted in a rapidly growing amount of records. That fostered an increased economic savings discourse concerning archives already in the first half of the 20th century, that the growing amount of archival records had to be handled more efficiently, which would include organised appraisal with increased destruction. In Sweden, a number of government inquiry reports were published in the 1940s and 1950s on the matter, which led to a large number of decisions on record destruction in government archives, as well as a new ordinance on general destruction of certain records types that were regarded having little value.¹⁶ Some of the reports also treated local government archives, and among other things social services records were discussed and considered to be having a large research value. Consequently, the advisory instruction issued by the National Archives in 1958 for municipal archives recommended the files to be generally kept.¹⁷ It should be kept in mind that the National Archives neither then, nor today, had any mandatory authority towards archives in municipalities or the county councils, but their advisory instructions have had a large impact anyway.

The 1970s investigations and the 1980 Social Services Act

In the 1970s, arguments for the destruction of social services records came to the fore, however. They were discussed in a large government inquiry, The Social Inquiry (*Socialutredningen*), which was in function from 1967 to 1977. Its first published report in 1974 voiced a new and upcoming critique that the subjects of social work had been blocked from reading their own files. It advocated a general democratisation of the social services with increased rights for the persons involved. It also mentioned different kinds of registration and thorough investigations, which the clients of social services had not had the possibility to take part of.¹⁸

¹⁵ SOU 1977:40, p. 741.

¹⁶ Nyberg 2005.

¹⁷ SFS 1958:530, III:I; Edvardsson 1981, p. 79.

¹⁸ SOU 1974:39, pp. 102–103 and 636–637.

Furthermore, the inquiry report stressed that the “modern technique of storage and distribution of data”, and all its “registration of personal data” meant serious problems. The notion privacy (*integritet*) was frequently used, and the report emphasised the importance to “have protected spaces in the private lives” and that people should be entitled to social assistance without having to disclose “irrelevant details of one’s life and to have guarantees that no personal data via registers are spread in an uncontrolled manner”.¹⁹ The 1974 report also put forward the idea to avoid recording personal names in the files. While it did not leave any suggestions on the question of retention or destruction of social services records,²⁰ it was visibly an example of the general upsurge of the privacy discourse in Sweden and other Western countries. In Sweden, it soon resulted in the Data Act in 1973, which obliged all computerised personal registers to gain formal permission from a new government agency, the Data Protection Authority.²¹ Thus, the inquiry report integrated the privacy discourse with a general idea of democratising the social welfare system, by limiting the power of experts and professionals and aiming to improve the rights of clients of social services and patients.²²

The final report of the inquiry, published in 1977, developed the privacy discourse and used the term privacy (*den enskildes integritet*) to underline the general importance of privacy in the social services in general. The term was also included in the first section of a proposal for a new Social Services Act, being part of the aim of the law: “the self-determination and integrity” of individuals.²³ And more importantly, the report advocated mandatory destruction of records. It proposed as the general rule that social services files should be destroyed three years after the last annotation within them, as well as strict rules for careful manners of documentation in order to prevent unnecessary personal information being included. The destruction after three years was to be mandatory, due to its purpose of protecting the individual privacy. The time period was considered enough to safeguard the

¹⁹ SOU 1974:39, p. 183 and 244 (“den moderna tekniken för lagring och distribution av data [...] registrering av persondata” [...] “att få vara fredad i sitt privatliv [...] ovidkommande uppgifter om sitt liv och att ha garantier för att inte personliga data via register sprids på ett okontrollerat sätt”).

²⁰ SOU 1974:39, p. 414.

²¹ Ilshammar 2002; Söderlind 2009; Abrahamsson 2007; Flaherty 1989; Markgren 1984.

²² See e.g. Björkman 2001.

²³ SOU 1977:40, pp. 31 (quote) and 652–653. (“självbestämmanderätt och integritet”)

interests of control and legal accountability. Only in two cases should there be exceptions, since records might be necessary as evidences for longer times, namely: records on child support (maintenance allowance), and investigations on fatherhood. However, the report also claimed that further exceptions from destruction might be appropriate, and recommended that the new legislation would give the Government the right to decide on such additional exceptions in order to protect evidence.²⁴

The 1977 inquiry report also discussed the possible research value of social services records. That issue had been discussed already in another investigation made within the National Archives in 1973. In the 1973 report, a general 20-year retention of social services records was suggested, combined with partial longer preservation through sampling in some municipalities and one/two counties. Even though privacy concerns were touched upon, its arguments for destruction were mainly based on economic demands, since the amount of records was rapidly increasing. When the report was sent out for referral, the reactions were mixed. Some universities criticised the suggestion because of impaired research possibilities, even though some could accept the partial retention and discussed alternative sampling models. The municipalities – those financing the archives in question – were more positively inclined towards destruction, while the government archival institutions were more negative. Because of this uncertainty, the social services records were omitted from the final advisory instructions to municipal archives from the National Archives in 1975, leaving further investigations to the on-going Social Inquiry.²⁵

Concerning the needs of retaining certain social services records for the benefit of academic research, however, the 1977 inquiry report did not come to a definite answer. It mentioned the mixed reactions on the previous National Archives proposal, and passed over the question to the Government in order to be solved later. Similar to the case of exceptional retention for evidence and legal reasons, the new legislation should be formulated so that further exceptions for research reasons were possible.²⁶

The suggestions by the inquiry report were largely followed in the Government bill issued in 1979, with the exception that the three years of

²⁴ SOU 1977:40, p. 40, 747–748 and 876. The principle of not recording sensitive information even from the beginning is also noted in Friberg von Sydow 2017, p. 17, concerning medical records.

²⁵ SOU 1977:40, p. 746; Edvardsson 1981, pp. 79–82; SOU 1975:71, p. 113.

²⁶ SOU 1977:40, pp. 746 and 748.

retention were increased to five years. Just like the inquiry, the importance of privacy was put to the front. Social services must be based on voluntariness, but a prerequisite for that was that people actively dared to contact the social bureaus. “Many” today, however, did not do so being afraid that personal information about them would “be archived for the future”, the bill claimed.²⁷

In the further parliamentary process, the questions on archival destruction and retention were seemingly regarded non-controversial, since no objection was voiced from any representative of the (at that time Socialist) opposition.²⁸ However, in the preceding referral process when various government agencies, municipalities, and private sector organisations had commented to the inquiry report, the opinions were more divided. To start with, many had objected that three years were not enough time for protecting legal interests, which led the Government to set five years instead in the bill.

However, only few had more principal objections on the principle of destroying records primarily for privacy reasons, instead of the usual economic ones. One of those, however, was the National Archives, that stressed that the report meant a new aspect of archival appraisal. They used the term “ethical destruction”, and claimed that this was something new compared to the Data Act, since it was now the question of analogue documents. Many organisations such as universities and Statistics Sweden also claimed that research would become more difficult.²⁹

There was also a critique from some instances that ethical destruction might make it difficult or impossible to prove misdeeds of the past. Some of those particularly named a category of cases that was not exempted, namely, records on children placed in foster care. The Parliamentary Ombudsman (*Justitieombudsmannen*) mentioned that there could be cases where the new destruction rules would make it impossible to find examples of older abuse on children that could be an argument for not allowing a family to house children. If records documenting neglect (*vanvård*) were kept, it could mean that the foster homes in question would not be accepted again, but of course that possibility was swept away if the records were destroyed.³⁰

²⁷ Prop. 1979/80:1, p. 448. (“många [...] rädsla för att personliga uppgifter om dem då kommer att arkiveras för framtiden.”)

²⁸ Bet. 1979/80:SoU 44.

²⁹ Prop. 1979/80:1, pp. 447–448.

³⁰ See also similar views of the national association of social workers and the National

Stockholm Municipality stated that at least 15 years of retention would be appropriate, not only for control, but also for making it possible for people afterwards to find out why they were not raised with their parents, to find out their background.³¹ However, concerning longer periods of retention than three or five years, neither the 1977 inquiry report nor the 1979 bill suggested any such specific time frames concerning those records that were considered worth keeping longer for the benefits of the people involved. Instead, the proposed law sections simply stated that such records must not be destroyed, which in effect means retention for ever or at least until further notice.

The result of the *Riksdag* decision in 1980 became the new Social Services Act (*Socialtjänstlagen*), which came to effect in 1982. However, its sections on destruction and retention of records were put on moratorium by a special transition rule in the law, saying that the new destruction rule must not be used until 1987 for information before 1982. That was made in order to make room for further investigations on preservation for research purposes, but also to more thoroughly investigate the need for exceptions from destruction in the interest of the persons directly involved, so that evidence was kept more than five years. The bill particularly mentioned records on child and youth care, largely agreeing on the criticism e.g. from the national association of social workers (*socionomer*) and The Parliamentary Ombudsman.³² Therefore, a new social data inquiry was set up in 1980.

The 1980s investigations and legislation process

The social data inquiry committee worked for six years, and while waiting for its proposals to result in legislation, the moratorium on the retention and destruction rules of the new Social Services Act was further renewed until 1991, when the question was finally solved, as we will see.³³

The social data inquiry report of 1986 advocated, concerning preserving documents for research needs, keeping all documents regarding persons born 5, 15, and 25 in any month, as well as all records in a single muni-

Archives: Prop. 1979/80:1, appendix 1 pp. 317–318 and 325.

³¹ Prop. 1979/80:1, appendix 1 p. 319.

³² Prop. 1979/80:1, pp. 448–450; SFS 1980:620, transition rule 3.

³³ Prop. 1986/87:43, pp. 3–4; Bet. 1986/87:SoU11; SFS 1986:1393; Prop. 1987/88:76; Bet. 1987/88:SoU11; SFS 1988:129; Prop. 1989/90:93; Bet. 1989/90:SoU18; SFS 1990:295.

cipality (Jönköping). The idea of partial retention by sampling was one of the most vivid topics of discussion concerning archival appraisal in Sweden from the 1960s to the 1990s, where different methods and choices of samples were debated.³⁴ In the case of privacy-menacing information, a somewhat paradoxical combination evolved consisting of destruction for privacy reasons on the one hand, and partial retention for future research, on the other.

As for exceptions concerning the type or nature of records, the inquiry found that child support records no longer had to be exempted from destruction since the parents normally kept them. However, records on fatherhood investigation should instead be sided with records on adoptions from other countries – a category that had not been focused upon in the 1970s investigation. However, the earlier debated topic of children placed in foster care was not considered necessary to be an exception. The five years of retention was enough for justice reasons, it was argued, since after only a few years it would anyway not be possible to demand restitution, because the time limits of penal responsibilities had then passed.³⁵ The motives for keeping evidence of maltreatment were put forward almost purely in a legal context, in order to prevent or prosecute abuse. However, the more identity-motivated interest of maltreated persons who might want to find out his or her background long afterwards was downplayed. It was argued that most parents and children wanted the destruction of records regarding placement in foster homes, even though some would want to find out their background later. The investigators noted that the issue was complex, but they anyway argued against the argument that society should assist people's wishes to seek their "roots":

To the investigation, the meaning has been suggested that people's need to learn about their "roots" would imply an obligation for society to preserve virtually all personal information. We do not share that view, [...].³⁶

³⁴ Edquist 2018 (forthcoming).

³⁵ Ds S 1986:5, pp. 118–126.

³⁶ Ds S 1986:5, pp. 118–119 and 125–126, quote p. 119. ("Det har till utredningen framförts att människors behov av att söka kunskap om sina 'rötter' skulle innebära en skyldighet för samhället att bevara i princip all personanknuten information. Vi delar inte det synsättet, [...].")

In the referral process that followed when the Government asked for opinions on the inquiry report, there were many examples of differing ideas and various interests clashing. A number of government agencies, county councils, municipalities and private organisations were invited to respond, but there were also a number of associations and individuals that sent in their opinions on their own initiative.³⁷ The conflicting views could be on many kinds, for example rivalry within the public sector. Some municipalities were angered by the report's suggestion that the preserved records should be stored in central government archival depots – not in the municipal ones as would normally be the case.³⁸

Some advocated even more total destruction, and argued that it was wrong to keep the records concerning those born on 5, 15 and 25. For example, non-socialist political representatives in Stockholm Municipality stated that academic interests must not have precedence over the interests of privacy.³⁹ From the opposite point of view, the idea of archival sampling on these records was criticised by a local municipal archive, stating that it was illogical to perform ethical destruction and at the same time keeping vast quantities of a part of that material for research purposes. It also stated a general criticism on ethical destruction, especially on doing it retroactively: “if the principles of our own time are applied on older archival material, created in other circumstances, the so called ethical destruction becomes a tool of censorship, a falsification of reality with incalculable impacts”.⁴⁰

Several representatives for the social services professionals warned against destruction on records on adoptions within Sweden, and some also mentioned the case of foster care placements.⁴¹ There were also previously

³⁷ File with registration number V 1967/86, the Archives of the Ministry of Health and Social Affairs (*Socialdepartementet*), main archive 1975– (*huvudarkivet*), series E1A, volume 2161 (part of *regeringsakt* 13 Febr. 1992 no. 1). National Archives, Arninge. Below shortened as: V 1967/86.

³⁸ V 1967/86: opinion nos. B 22 (Uppsala County Council); B 29 (Botkyrka Municipality); B 43 (FALK, an association of archivists in local governments).

³⁹ V 1967/86: opinion no. B 26 (Stockholm Municipality, reservation).

⁴⁰ V 1967/86: opinion no. B 29 (Botkyrka Municipality, p. 6). (“Om vår egen tids principer appliceras på äldre arkivmaterial, tillkomna under andra förutsättningar, blir den s k etiska gallringen ett censuredskap, en verklighetsförfälskning med helt oöverskådlig räckvidd.”)

⁴¹ V 1967/86: opinion nos. S 40 (Ale Municipality), S 45 (E. Holgersson, social worker), S 46 (Södertälje Municipality, the family section), S 50 (petition by social workers). The view of keeping from adopted and placed could be combined with the privacy-related criticism on

adopted individuals that protested against the destruction of records on adoptions within Sweden. That was interpreted as a way of protecting the interests of parents at the expense of those of the children. The latter should have the possibility not to contact their biological parents if they would like to know more about their past, since the only remaining documentation otherwise would be the brief facts of names and dates in the national registration records. The social services records, with information on the actual circumstances in adoption cases, should be kept for them to read in peace.⁴² *Allmänna Barnhuset* – a government-led foundation dealing with child care – also claimed that the interest of children was not taken into account in the referral process, while three organisations of adult clients of social services had been invited.⁴³ The latter generally advocated privacy, stressing that privacy must in principle be placed before research. Therefore they advocated anonymisation of the records to be kept.⁴⁴

Allmänna Barnhuset also put forward that parents and grown-ups (including researchers) were premiered before children concerning placements in foster care. They used the fictional case of the 24 year old Lena who contacts the social services in order to know why she had been placed in foster homes from she was two years old:

If the suggestion of the social data inquiry becomes real, the answer to Lena would be: There are no records concerning you. There were records, but of concern for you and your parents, they were destroyed. If you are born on the 5, 15 or 25, they remain, but not for your sake, but of concern for research needs for data.⁴⁵

retaining for research purposes, see B 26 (Stockholm Municipality, reservation).

⁴² V 1967/86: opinion no. S 44 (former adopted child). ("Ni får inte tvinga barn att ta kontakt med sina biologiska föräldrar bara för att få svar på den fråga som alla vi adoptivbarn bär på: varför lämnades vi bort? Låt oss även i fortsättningen ha den möjligheten att kunna söka svaret i papper i stället för genom ett möte som kanske skadar både oss och våra föräldrar.")

⁴³ V 1967/86: opinion no. B 34 (Allmänna Barnhuset).

⁴⁴ V 1967/86: opinion nos. B 38 (De Handikappades Riksförbund, DHR); S 47 (Handikappförbundens centralkommitté, HCK). Two other client organisations, ALRO and Verdandi, were invited to respond, but did not.

⁴⁵ V 1967/86: opinion no. B 34 appendix 2. ("Om socialdatautredningens förslag blir verklighet skulle svaret till Lena bli: Det finns inga handlingar om dig. Det fanns men av omtanke om dina föräldrar och dig har de förstörts. Är du född den 5;e, 15;e el 25;e [*sic*] finns de bevarade men inte för din skull för att du ska kunna forska om ditt förflutna utan av

On the contrary, among the letters to the government gathered in the large dossier from the process, there is also one from an individual former subject to foster care arguing for his right to have his old personal records removed, just as it had been possible with medical records since 1980.⁴⁶

After a couple of years, the suggestions of the 1986 inquiry were finally made into a government bill in 1990 – in fact the process was integrated with the introduction of the Archives Act. By then, the social services records had been part of the abovementioned discussions on organised sampling for almost twenty years. Centralising the sampling on a national level to encompass many kinds of records for the benefit of future research, was one proposal. The idea was to retain large amounts of data from at least some regions concerning a certain percentage of the Swedish population, in order to allow for research using quantitative and longitudinal methods, a research practice particularly heralded at the time. The end result in the Archives bill of 1990, put into reality in July 1991 for the social services records, was keeping records from all people born on the 5, 15 and 25, as well as everything from the counties of Västernorrland, Östergötland and Gotland, as well as from Göteborg municipality. The temporary moratorium on destroying files in the Social Services Act was lifted, so that the main rule of destroying files after five years was finally put into practise. It was also stated that it was optional for municipalities to destroy such records from the period before 1982 that were equivalent to the ones that must be destroyed from 1982 onwards.⁴⁷

The government bill also largely responded positively to the critique concerning adoptions within Sweden and placements in foster care – such cases were now also included as exceptions, beside those documenting international adoptions and fatherhood (even though most referral bodies had had no objections regarding the original suggestion to destroy such records). The government bill actually used the term ethical in its legitimisation of the need of preserving the documents in question. Contrary to the inquiry report, it placed large emphasis on the importance to find one's roots; it would be “ethically wrong” not to make it possible for persons to get to know his or her origin and background, such as concerning adoption

omtanke om forskningens behov av data.”)

⁴⁶ V 1967/86: opinion no. S 48 (person formerly in foster care). On medical records, see below.

⁴⁷ Prop. 1989/90:72; SFS 1990:789; SFS 1991:26; Edquist 2018 forthcoming.

or separating children from parents.⁴⁸ The word “ethical” was thus used in the discussions both to describe the destruction and the retention of records – even though the phrase “ethical destruction” was mainly used by archivists in a somewhat sarcastic tone.

The example of the social services records show that the demarcations between keeping and destroying had changed during the long process from the early 1970s into the final solution in 1991. Since 1991, the rules have been fairly the same, with some changes in detail concerning types of placements, and adjusting the older notion of “fatherhood” to “parenthood”.⁴⁹ In 2005, similar rules of five year destruction and partial retention was also introduced in the Law regulating Support and Service to Persons with Certain Functional Disabilities (LSS), in conjunction with a reform that stressed the needs for enhanced documentation in a similar manner as stipulated in the Social Services Act.⁵⁰ And in 2008, both these laws introduced the regulations on retention and destruction also in private sector institutions.⁵¹

How archival politics shape the documentary heritage for the future

These examples show that the study of the history of ethical destruction point towards several interesting directions. One obvious result is that the discussions on privacy have affected the structure of archival documentation regarding an important sector of society. It has created a reality where there is a vast amount of archival documentation concerning some individuals and in some parts of Sweden, whereas it is largely absent elsewhere.

As was shown above, there was an increased focus in the 1980s on the need to preserve certain records on justice and ethical reasons, in order to guard the citizens’ rights against the deeds of authorities, family members or foster parents. It also led to additional exceptions from destruction in the Social Services Act. During that decade, there was also a shift in the national

⁴⁸ Prop. 1989/90:72, p. 95. (“etiskt felaktigt”)

⁴⁹ SFS 2001:453 chap. 12; SFS 2005:452; SFS 2006:463; SFS 2007:1315; SFS 2015:982.

⁵⁰ Prop. 2004/05:39; SFS 2005:125; SFS 2005:128.

⁵¹ SFS 2007:1315 chap. 7 section 3a; SFS 2007:1313 sections 23a and 23b.

archival politics, where privacy concerns lost ground while general heritage concerns instead were strengthened.⁵²

A common criticism also in later years up till today has been that ethical destruction makes future rehabilitation against misdeeds in the past impossible; and typically the misdoings discussed are located in a more distant past than in the discussions I have analysed from the 1970s and 1980s.⁵³ That discourse has become strengthened worldwide in the late 20th and early 21st century, targeting historical crimes of various governments, such as genocides and discrimination. In Sweden, such discourses had a large presence from the 1990s, disputing government policy during World War II, government approved forced sterilisation, and the policies toward the Sami and Roma peoples.⁵⁴ Maltreatment of children in foster homes in earlier parts of the 20th century have also come to the fore in various countries, triggering official apologies and investigations.⁵⁵ In Sweden, the latter issue led to government inquiries, a government apology in 2011 and the right for previous victims to apply for indemnity. In that context, it is interesting that the legal unclearness from 1980 to 1991 seems to have led to some non-official destruction of documents, sometimes obstructing proving maltreatment in past social child care. After all, the original version of the law included records on placements in the main category to be destroyed after five years, even though it was never formally in practice until 1991 when the placements and adoptions were included. An investigation report in 2011 on maltreatment in foster care in the 20th century, found that the unclear legal situation from 1980 to 1991 seems to have led to some non-official destruction of records concerning those groups. The effects of such absence of documents should not be exaggerated, however, since existing documentary records from out-of-home care often are hard to use as further evidence on maltreatment witnessed by the victims themselves – beatings and other misdeeds were simply not put on file.⁵⁶

⁵² Rosengren 2016; Edquist 2018 forthcoming.

⁵³ See e.g. Ketelaar 2002, p. 229; Cook & Waiser 2010.

⁵⁴ Misztal 2003, pp. 145–155; Nobles 2008.

⁵⁵ Sköld & Swain (eds.) 2015.

⁵⁶ SOU 2011:61, pp. 21, 111–115, 226–230; Sköld, Foberg & Hedström 2012.

Interests and agent groups

The issues on ethical destruction were characterised by tensions between various interests and agent groups, and tended to follow similar patterns. In the discussions on the social services records presented above, it is at least possible to speak of five types of different interests, having an impact on the opinions expressed concerning access to documents containing personal information. Two of them work for destruction, and three for retention:

The privacy interest primarily aims at protecting personal privacy. Typically, it leads to demands on various levels of secrecy or, if such measures are not considered protection enough, destruction of records.

The economic interest is generally the most common driving force for destruction of documents. This “interest” is normally the result of limited economic resources for archiving; it is seldom a target in itself but rather seen as a (regrettable) necessity.

The openness interest is the view that documents should be kept as evidence, for individuals to control their own contacts with authorities, e.g. medical documents and surveillance acts from the security police. This interest in transparency and accountability also applies for the general right to control the deeds of the authorities, by single citizens or by mass media.

The heritage interest stresses that information should be kept in order to provide the society of the future with the richest possible traces from the past.

The academic interest wants information to be kept in order to help academic research. In social and historical sciences, there is no sharp limit towards the heritage and openness interests. The academic interest is more “purified” when it comes to medical research.

This model should be regarded as a starting point and might be used as an ideal-type model for further investigations, and possibly it can be redefined and sharpened during my further research process. Its main advantage is structuring the main positions in a complex debate with many agents involved. Of course it does not exclude the possible existence of yet other forms of interests, but so far I regard them as the most important.⁵⁷

⁵⁷ For example, destruction in order to remove *redundancy* is not included, since this otherwise normal legitimization of destruction is typically applied on records containing little and/or short-lived informational or evidential value, which is hardly the matter with social services records. An interest type that I have hardly detected at all so far, but that might be found in other materials, can be termed *the “too much information” interest*; the

The debates on privacy issues can also to a large extent (of course not generally) be described as conflicts between a number of collective agents – or agent groups – that have been involved in the discussions on privacy in documents. In the following, I will show some examples on divergences and alliances between and sometimes within various such agent groups, as well as a tendency that certain agent groups incline to cherish certain of the above-mentioned interests more than others.

Archivists and archival institutions seem to have been generally fighting for preservation of documents even if they were a danger to privacy. The Swedish National Archives have generally tended to defend heritage and academic interests but also used the argument that ethical destruction risked wiping out traces of misdeeds in history, creating a beautified picture of the past.⁵⁸ In the Swedish archival profession, there are many signs of a general inclination towards keeping records. Destruction is generally regarded as a necessary means in many occasions, but should only be used for records of lesser archival value – not for any ideological reasons.⁵⁹ This is partly an ethos that is also incarnated in classical archival theory, not least the principle of provenance, which stresses the integrity and organic essence of archives, whereby destruction motivated by ideology is seen as an anomaly.⁶⁰

Archives and academic researchers seem to have been largely united in defending retention interests, for example in the prolonged discussions from the 1960s to the 1990s on archival retention in certain sample regions, for the interest on longitudinal research.⁶¹ Diverging views have been pos-

(age-old) tendency to radically react against what is regarded as general information overload, by heralding forgetting and information destruction, see Lowenthal 2006, pp. 195–196. Retention for organisational or medical needs are other interest types that are more prominent in other cases.

⁵⁸ See e.g. Nilsson 1976, p. 79; Staffan Smedberg, PM 23 Dec. 1986, registration no. 707-87-55, vol. 48, series F1D, Archives of the National Archives (*Riksarkivets ämbetsarkiv*), younger main archive (*yngre huvudarkivet*), National Archives, Marieberg.

⁵⁹ The International Council of Archives' "Code of Ethics" (1996) states that archivists "should protect the integrity of archival material and thus guarantee that it continues to be reliable evidence of the past" and that they "should take care that corporate and personal privacy as well as national security are protected without destroying information". However, it also claims that "they must respect the privacy of individuals who created or are the subjects of records, especially those who had no voice in the use or disposition of the materials". See also Millar 2017, pp. 116 and 119; Rosengren 2017, p. 52.

⁶⁰ See also Rosengren 2016; Rosengren 2017, pp. 29–32.

⁶¹ For an example where an archival institution used a contemporary social history project

sible to detect, however. By way of example archival professionals could sometimes regard academic researchers as ignorant of the necessities of destroying records for economic reasons.⁶² The interest of academic research was also sometimes downplayed by other agents, who implied that it represented a narrow and somewhat elitist position that should not take precedence. In the social services records discussion, for example representatives for the client organisations repeatedly stated that privacy must be placed above that of academic research.

The inclusion of client organisations in the referral process in the 1970s and 1980s should be seen to reflect a change in the welfare system where an older and more authoritarian tendency was questioned, with experts having too much formal power. But as we have seen, there were signs of conflicting views within these groups, for example between different representatives or spokespersons of parents and adopted children. Some stressed the importance of privacy and destruction of sensitive information, others protested and argued that it had to remain as evidence of the past, to know one's background, or to prove wrongs.

The political arena has of course been of vital importance, since the legislation on ethical destruction issues were decided there. However, there was overall somewhat of a consensus regarding these questions, if considering the discussions in the Riksdag. There were only few examples of differences, and then there was a slight tendency that non-Socialists were closer to the "privacy" node while the Social Democrat government bill in 1990 – preceding the Archives Act – made a mark against ethical destruction.⁶³ In the decision process of the 1980 Secrecy Act, a conservative Riksdag mem-

plan that risked being hindered if social services records were destroyed, see the opinion of the Regional State Archives in Östersund on SOU 1987:38 (*Arkiv för individ och miljö*), File with registration number 2970/87, the Archives of the Ministry of Education and Research (*Utbildningsdepartementet*), main archive 1975– (*huvudarkivet*), series E1A, volume 3176 (part of *regeringsakt* 8 Febr. 1990 no. 8). National Archives, Arninge.

⁶² For an example of the research opinion, see e.g. Nygren, Larsson & Åkerman 1982, pp. 179–180, 249, 270–282. See also Edquist 2018 forthcoming.

⁶³ Prop. 1989/90:72, p. 40. See also Flaherty 1989, pp. 123–125, who shows a differing attitude between the Social-Democrat and the non-Socialist governments of the 1970s and 1980s towards the Swedish Data Protection Authority. The observation on general political consensus in Swedish archival politics, with major differences rather showing between agent groups outside the parliamentary arena, has previously been noted by Åström Iko 2003, p. 24.

ber claimed that medical records should not be seen as official documents at all, but rather as "working papers", thus not accessible for any outsider:

The justification for "the principle of public access to official documents" in Swedish law is based on the notion of the citizen's need and right to control authorities. However, there is neither a need nor a right for the citizen to infringe other citizens' privacy.⁶⁴

In the legislation process preceding the Archives Act in 1990, which included the final settlement of the issues on social services records, actually the only initiative taking privacy to the fore was a Liberal proposal demanding that only laws (statutes decided by the parliament) should be able to regulate retention, never ordinances (statutes decided by the Government). They also stated that privacy should be placed above against academic interests. However, their suggestion was turned down and there was only a brief debate on the matter in the Riksdag.⁶⁵

Journalists and amateur historians constitute other agent groups that played a marginal role in the debates on social services records I have covered here, but they were more active in other discussions on ethical destruction. Many journalists have traditionally been advocates for the openness interest, while at the same time, the mass media have often voiced ordinary citizens' perceived privacy interest vis-à-vis authorities and academic researchers.⁶⁶ Amateur historians tend, in other debates on archival appraisal, to praise the heritage interest, not seldom against the academic interest.⁶⁷

In the 1970s and 1980s legislation processes on social services records, there were not only conflicts between retention and ethical destruction. The costs of keeping the rapidly growing amount of documents were also a key factor. These economic aspects had been visible already in the 1930s debate,

⁶⁴ Bet. 1979/80:KU37, p. 47–48 (Gunnar Björck, m). ("Motiveringen för 'offentlighetsprincipen' i svensk lagstiftning baseras på föreställningen om medborgarens behov av och rätt att kontrollera myndigheterna. Något medborgerligt behov av, eller någon rätt, att göra intrång i andra medborgares personliga integritet föreligger däremot inte. [– – –] 'arbetspapper' [...].)

⁶⁵ Mot. 1989/90:Kr17; see also Protocol 1989/90:131, p. 155.

⁶⁶ Many journalists in Sweden have taken part in public debates on freedom of information, secrecy and ethical destruction, see e.g. Funcke 2006; Olsson 2008. See Qwerin 1987 and Söderlind 2009 for examples of mass media coverage of data protection issues.

⁶⁷ Edquist 2018 forthcoming.

when non-obligatory registration of social registries was proposed to limit the budgetary burden of small municipalities.⁶⁸ At the political level, a general drive for savings in the archival sector was possible to discern during the 1970s and a large part of the 1980s. Characteristically, one departmental inquiry in 1981 was called “The archival problem of society” (*Samhällets arkivproblem*), stressing the need to further dispose of records.⁶⁹

As has been mentioned, the economic demand was often put forward as an important argument to destroy records that existed in large volumes, such as those from the social services. It continued to exist alongside the argument related to privacy, which gained strength at a later stage, in the 1970s. Obviously, the two arguments could sometimes be combined. A good example is the reaction from Jönköping municipality on the 1986 inquiry report’s suggestion that Jönköping would be a sample area where all documents should be kept. Jönköping municipality stressed the privacy argument, but the economic consequences of the suggestion were commented upon with particular irritation. The report had not counted on the amount of work and money that would be needed for transferring “several millions of A4 pages” of records from the social services administration to archival paper formats, the Jönköping official fumed.⁷⁰

Concluding discussion, with a glance of future research

This article has given some results and perspectives, and most of them should be viewed as threads to be further examined and elaborated in deepened form. Privacy concerns should be seen as an ideological stance, since they form a particular collection of ideas, values and beliefs of political relevance, in this case a certain tendency to emphasise the rights of the individual in relation to society at large.⁷¹ That perspective has been the

⁶⁸ E.g. Bet. 1936:2LU 18, dissenting opinion (K.G. Westman and G.A. Johansson i Hallagården): “Pappersmängder och skriverier böra ej onödigtvis tynga förvaltningen”.

⁶⁹ Ds U 1981:21.

⁷⁰ V 1967/86: opinion no. B 30 (Jönköpings kommun) (“flera miljoner A4-sidor”). Cf. Rosengren 2017, pp. 31–32, who discusses arguments in the archival literature on records destruction, which normally derives either from there being too many documents, or that they risk menacing privacy. The social services records belong to both categories at the same time.

⁷¹ This has previously been underlined by e.g. Stahl 2007, pp. 35–45; see also Stefanick 2011. The concept of ideology has been defined and used in almost countless ways; I use it in a semi-wide manner where systems of ideas must be linked to aspects of power struc-

most accentuated in this article. However, privacy concerns are of course not the only ideological stance within the debates on ethical destruction. The ideals of retaining information for freedom of information, heritage, and academic research purposes, are also ideological in various ways. It is necessary to at least make an effort to “step outside”, trying to equally treat all conflicting views on how to handle potentially privacy-menacing records without taking sides. The analysis of views on privacy concerns versus the interests of society as a whole, opens up an alternate dimension of political ideas operating across the party-political spectrum. In a similar way as nationalism, religion, and ideas on relations between humans and nature, the ideas regarding privacy cannot easily be connected to the traditional political ideologies, which only make them even more interesting.⁷² The relative lack of discussions in the Riksdag on these matters supports this point.

In the continuation of the research project from which this article is the first, the suggested typologies of conflicting interests and agent groups will be further analysed, and tested whether it has to be expanded or otherwise corrected. The existence of the consultation system normally preceding legislation in Sweden makes a good ground for these kinds of analyses, as shown above with the example of the 1986 social data inquiry report.

It is still in many cases an open question whether increased privacy concerns are related to late modern computers, or if it is rather a phenomenon typical of modernity, or even older than that.⁷³ One may argue that the emphasis on privacy might be linked to the fact that privacy was conceptualised as a topic of its own in the 1960s. During this period, privacy was seldom a topic of public debate, however. Further analyses of the era before the 1970s will hopefully bring more light on this issue. For example, the investigations regarding social services records in the 1930s and 1950s will be more thoroughly studied. What agents were at all involved in the discussions?

tures and politics, but not necessarily to *dominant* social strata or political forces. Cf. Eagleton 1991, pp. 1–31.

⁷² A further analysis should make use of theoretical conceptions that stresses the possibility of parallel layers of ideologies, which makes room for the importance of other spectra than the classical political Right–Left-axis, but still aims at relating the various ideological structures as a totality and part of the actual historical situation with all its contradictions and divergences, e.g. Jameson (1981) 1989.

⁷³ Cf. Vincent 2016; Friberg von Sydow 2017, pp. 13–16.

The further investigations will also include at least two other forms of records, that are both related to the social services records by being largely in paper form (at least before lately), in order to add possible new perspectives on the actual importance of computerisation in the privacy debates. First, the discussions on social services records were often discussed in conjunction with those on medical records in the 1970s and 1980s. A 1968 government inquiry report had suggested to generally keep medical records from inpatient care for 30 years, and for 10 years concerning outpatient care. Previously, the records had been generally kept, but the need for destruction was now entirely motivated by economic reasons.⁷⁴ However, in the 1970s, the privacy arguments also entered into the medical records area. Suggestions to permit individuals to decide on the destruction of their own information in medical records were made in Riksdag proposals in the mid-1970s, and more importantly also in a 1978 inquiry report. The possibility was then legally introduced in July 1980,⁷⁵ and included in the new legislation on medical records 1985, which otherwise stipulated that medical records must be kept for at least three years – changed in 2008 to ten years.⁷⁶ In the discussions, it was claimed that there was a difference between medical documents and social services records since the former were of more direct value for the individual involved, while the latter were mostly interesting for the authorities.⁷⁷

Academic research data is another important intersection for debates on ethical destruction, especially those records that contain sensitive personal information, for example in research in psychology or sociology. There has been a constant discussion in Sweden regarding privacy concerns in certain research data, in politics and in particular cases involving the Data Inspection Authority and the National Archives. In some instances, these issues concerning privacy in research data have come to public attention, for example in 1986, when the sociological research project *Metropolit* was heavily attacked in mass media for its longitudinal registration of personal data from everyone born 1953 in the Stockholm area.⁷⁸

In preliminary surveys, I have detected many signs of conflicts between archives and universities, not the least in cases when researchers, for exam-

⁷⁴ SOU 1968:53.

⁷⁵ SOU 1978:26, pp. 143–146; Ds S 1982:5, pp. 69–70.

⁷⁶ SFS 1985:562; SFS 2008:355 chap. 8 section 4.

⁷⁷ Ds S 1982:5, p. 69.

⁷⁸ Stenberg 2013.

ple, have wanted to protect their informants in questionnaires and medical examinations from ending up in archives. This is partially connected to divergences in the views of the status on research data, with a common conception in the scientific community that researchers "own" their research materials, even though the Swedish legal framework largely regards them as official documents that should be treated thereafter.⁷⁹ Archival professionals have tended to claim that researchers' low awareness of freedom of information and archival legislation leads to instances of "unofficial" ethical destruction. In fact, handbooks on research ethics have mentioned that researchers should be prepared to contemplate destruction of sensitive personal information, if he or she had promised anonymity or confidentially that was not grounded in the secrecy legislation, "and take the punishment it might lead to".⁸⁰ A well-known example is the controversy in 2003–2005 when research material at Gothenburg University connected to the disputed psychiatric diagnosis DAMP was illegally destroyed.⁸¹

Academic researchers thus seem to figure on two sides. In some cases they are the ones creating and keeping the documents seen as menacing to privacy, and in those cases they often tend to endorse the idea of ethical destruction. In other cases, researchers want access to documents created by others, and in these instances, ethical destruction is instead normally resisted. As we have seen, the regulation of contemporary social services records also included the opinions of the academic research professionals that normally advocated retention.

A somewhat metatheoretical point may be put to the front as a concluding remark. In social history research, so-called case files on individuals in official archives, such as medical records, criminal case files, and social services records, have been important source materials for decades, at least since the 1960s and 1970s. Not seldom, these case files have been interpreted in a Foucauldian theoretical framework, analysing the ways experts and other power/knowledge institutions have handled marginalised groups of society. It is regularly emphasised that the very creation of these records and files constituted an important part of the power mechanisms:

⁷⁹ Vetenskapsrådet, *Nationella riktlinjer för öppen tillgång till vetenskaplig information* (2015), p. 22; Martinsdotter, Strömberg & Åström 1997, p. 43.

⁸⁰ Hermerén 1986, p. 178. ("ta det straff som detta eventuellt kan medföra")

⁸¹ See e.g. Mot. 2003/04:K379 demanding legislation changes after the DAMP controversy.

The creation of a case file implies the intervention of institutional and bureaucratic power into people's lives. The (usually middle-class) staff associated with these sources of power, whether professionals or volunteers, generally were concerned to resolve conflicts, bring their clients into conformity with dominant social and political norms, and/or punish political, sexual, and other transgressors.⁸²

Even more specifically, some researchers have made use of Foucault's specific writings on the *dossier*, and the ways these crystallised discourses of power/knowledge framed the individual as an object of power.⁸³ In the quoted example, the authors made use of these records in order to combat a traditional harmonising nation-centred and elitist history-writing, by lifting the marginalised groups to the fore. The archived records used for state surveillance and power techniques, are thus the tool for critical scholars of deconstructing the same power structures.

Similar discourses on power and surveillance have been used by the privacy advocates in the debates concerning mass data, criticising governments for keeping registers and knowledge on individuals as a means of exercising – at least potential – power. For the social historians quoted, the archived information of yesterday is a prerequisite for unveiling certain power structures and mechanisms. For the privacy advocates, however, the same type of archived information today constitutes a danger and should be destroyed. To some extent, then, this may be formulated as a conflict between past and present, between concentrating on revealing privacy-menacing measures in history, and combatting them today.

References

Archives

Archives of the Ministry of Education and Research (*Utbildningsdepartementet*), main archive 1975– (*huvudarkivet*). National Archives, Arninge (Täby).

Archives of the Ministry of Health and Social Affairs (*Socialdepartementet*), main archive 1975– (*huvudarkivet*). National Archives, Arninge (Täby).

⁸² Iacovetta & Mitchinson 1998, quote p. 6; see also pp. 4 and 9.

⁸³ Iacovetta & Mitchinson 1998, p. 10; Strange 1998, pp. 44–45 footnote 7. See also Chrostowska 2006 on Foucault's own interest in *the dossier*, case files on individuals.

Archives of the National Archives (*Riksarkivets ämbetsarkiv*), younger main archive (*yngre huvudarkivet*). National Archives, Marieberg (Stockholm).

Official inquiry reports

[Ds = *Departementsserien*; inquiry reports initiated by government ministries]

SOU = *Statens offentliga utredningar*; Swedish Government Official Reports]

Ds S 1982:5 *Bevarande av journaler m.m.*

Ds S 1986:5 *Gallra och bevara socialtjänstens personregister*

Ds U 1981:21 *Samhällets arkivproble*

SOU 1968:53 *Arkiv inom hälso- och sjukvård: delbetänkande*

SOU 1974:39 *Socialvården: mål och medel: principbetänkande*

SOU 1975:71 *Landstingens arkiv: slutbetänkande*

SOU 1977:40 *Socialtjänst och socialförsäkringstillägg: lagar och motiv*

SOU 1978:26 *Hälso- och sjukvårdspersonalen ansvarsfrågor: samverkan personal-patienter: huvudbetänkande*

SOU 2011:61 *Vanvård i social barnavård: slutrapport*

Statutes (laws and ordinances)

[SFS = *Svensk författningssamling*; Swedish Code of Statutes]

SFS 1936:56 *Lag om socialregister*

SFS 1937:249 *Lag om inskränkningar i rätten att utbekomma allmänna handlingar*

SFS 1958:530 *Riksarkivets cirkulär till rikets kommuner med råd och anvisningar om gallring i kommunernas arkiv*

SFS 1980:620 *Socialtjänstlag*

SFS 1985:562 *Patientjournalallag*

SFS 1986:1393 *Lag om ändring i socialtjänstlagen*

SFS 1988:129 *Lag om ändring i socialtjänstlagen*

SFS 1990:295 *Lag om ändring i socialtjänstlagen*

SFS 1990:789 *Lag om ändring i socialtjänstlagen*

SFS 1991:26 *Förordning om ändring i socialtjänstförordningen*

SFS 2001:453 *Socialtjänstlag*

SFS 2001:937 *Socialtjänstförordning*

SFS 2005:125 *Lag om ändring i lagen om stöd och service till vissa funktionshindrade*

SFS 2005:128 *Förordning om ändring i förordningen om stöd och service till vissa funktionshindrade*

SFS 2005:452 *Lag om ändring i socialtjänstlagen*

SFS 2006:463 *Lag om ändring i socialtjänstlagen*

SFS 2007:1313 *Lag om ändring i lagen om stöd och service till vissa funktionshindrade*

SFS 2007:1315 *Lag om ändring i socialtjänstlagen*

SFS 2007:1316 *Förordning om ändring i socialtjänstförordningen*

SFS 2008:355 *Patientdatalag*

SFS 2015:982 *Lag om ändring i socialtjänstlagen*

Riksdag (parliament) print

[Bet. = *betänkande*; report from a Riksdag committee

Mot. = *motion*; proposal by a member/members of the Riksdag

Prop. = *proposition*; Government bill

Prot. = *Riksdagens protokoll*; records of Riksdag debates]

Bet. 1936:2LU 18 (*Andra lagutskottets betänkande* 18)

Bet. 1979/80:KU37 (*Konstitutionsutskottets betänkande* 37)

Bet. 1979/80:SoU 44 (*Socialutskottets betänkande* 44)

Bet. 1986/87:SoU11 (*Socialutskottets betänkande* 11)

Bet. 1987/88:SoU11 (*Socialutskottets betänkande* 11)

Bet. 1989/90:SoU18 (*Socialutskottets betänkande* 18)

Mot. 1989/90:Kr17 *med anledning av prop. 1989/90:72 om arkiv m.m.*

Mot. 2003/04:K379 *Sekretess och handlingars offentlighet*

Prop. 1979/80:1 *om socialtjänsten*

Prop. 1986/87:43 *om uppskjuten tidpunkt för gallring av socialnämndernas personakter och personregister*

Prop. 1987/88:76 *om uppskjuten tidpunkt för gallring av socialnämndernas personakter och personregister*

Prop. 1989/90:72 *om arkiv m.m.*

Prop. 1989/90:93 *om uppskjuten tidpunkt för gallring av socialnämndernas personakter och personregister*

Prop. 2004/05:39 *Kvalitet, dokumentation och anmälningsskyldighet i lagen (1993:387) om stöd och service till vissa funktionshindrade (LSS), m.m.*

Prot. 1989/90:131 (*Riksdagens protokoll 1989/90:131*)

Other printed references

Abrahamsson, Olle. "Integritetsskyddet i samhällsdebatten". In SOU 2007:22, part 1, pp. 493–535.

Bennett, Colin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, N.Y.: Cornell University Press, 1992.

Bennett, Colin J. & Charles D. Raab. *The governance of privacy: policy instruments in global perspective*. [2nd and updated ed.] Cambridge, Mass.: MIT Press, 2006.

Björkman, Jenny. *Vård för samhällets bästa: Debatten om tvångsvård i svensk lagstiftning 1850–1970*. Stockholm: Carlsson, 2001.

Blanc-Gonnet Jonason, Patricia. "Integritetsskyddet och offentlighetsprincipen i IT-samhället: en jämförelse mellan den svenska och den franska

- modellen.” In Cecilia Magnusson Sjöberg & Peter Wahlgren (eds.), *Festskrift till Peter Seipel*, Stockholm: Norstedts juridik, 2006, pp. 51–76.
- Bundsgaard, Inge. “The Question of Access: The Right to Social Memory versus the Right to Social Oblivion.” In Francis X. Blouin & William G. Rosenberg (eds.), *Archives, Documentation, and Institutions of Social Memory: Essays from the Sawyer Seminar*, Ann Arbor: The University of Michigan Press, 2006, pp. 114–120.
- Chrostowska, S.D. ”A Case, an Affair, an Event’ (The Dossier by Michel Foucault).” *Clio* 35, no. 3 (2006), pp. 329–349.
- Cook, Terry & Bill Waiser. “The Laurier Promise: Securing Public Access to Historic Census Materials in Canada.” In Cheryl Avery & Mona Holmlund (eds.), *Better off forgetting? Essays on archives, public policy, and collective memory*, Toronto: University of Toronto Press, 2010, pp. 71–107.
- Eagleton, Terry. *Ideology: An introduction*. London & New York: Verso, 1991.
- Edquist, Samuel. *Att spara eller inte spara: De svenska arkiven och kulturarvet, 1970–2010*. Uppsala: Institutionen för ABM, Uppsala universitet, 2018 (forthcoming).
- Edvardsson, Carl-Edvard. “Kommunal arkivgallring – 1970-talets Råd och anvisningar.” In *Arkivvetenskapliga studier* 5, eds. Lars Otto Berg et al., Stockholm, 1981, pp. 77–93.
- Flaherty, David H. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill, NC & London: The University of North Carolina Press, 1989.
- Friberg von Sydow, Rikard. ”Patientjournalen mellan integritet och daterisering: En undersökning av SOU 1984:73.” *Arkiv, samhälle och forskning: ny följd* no. 1 (2017), pp. 6–26.
- Funcke, Nils. *Tryckfriheten: Ordets män och statsmakterna*. Stockholm: Carlssons, 2006.
- Hermerén, Göran. *Kunskapens pris: forskningsetiska problem och principer i humaniora och samhällsvetenskap*. Stockholm: Humanistisk-samhällsvetenskapliga forskningsrådet (HSFR), 1986.
- Iacovetta, Franca & Wendy Mitchinson. ”Introduction: Social History and Case Files Research.” In Franca Iacovetta & Wendy Mitchinson (eds.), *On the Case: Explorations in Social History*, Toronto: University of Toronto Press, 1998, pp. 1–22.
- Ilshamar, Lars. *Offentlighetens nya rum: teknik och politik i Sverige 1969–1999*. Örebro: Örebro universitet, 2002.
- International Council of Archives. “ICA Code of Ethics”. Adopted on 6 September 1996. English version. <http://www.ica.org/sites/default/files/ICA_1996-09-06_code%20of%20ethics_EN.pdf>
- Jameson, Fredric. *The Political Unconscious: Narrative as a Socially Symbolic Act*. (First published 1981 by Methuen & Co.) London: Routledge, 1989.
- Ketelaar, Eric. “Archival Temples, Archival Prisons: Modes of Power and Protection”, *Archival Science* 2, no. 3 (2002), pp. 221–238.

- Lawrence, Susan C., *Privacy and the Past: Research, Law, Archives, Ethics*, New Brunswick, NJ: Rutgers University Press, 2016.
- Lind, Anna-Sara, Jane Reichel & Inger Österdahl (eds.), *Information and Law in Transition: Freedom of Speech, the Internet, Privacy and Democracy in the 21st Century*. Stockholm: Liber, 2015.
- Lowenthal, David. "Archives, Heritage, and History." In Francis X. Blouin & William G. Rosenberg (eds.), *Archives, Documentation, and Institutions of Social Memory: Essays from the Sawyer Seminar*, Ann Arbor: The University of Michigan Press, 2006, pp. 193–206.
- Markgren, Sten. *Datainspektionen och skyddet av den personliga integriteten*. Lund: Studentlitteratur, 1984.
- Martinsdotter, Kerstin, Gunilla Strömberg & Karin Åström. "Arkivteoretiska och praktiska aspekter på forskningsmaterial", *Arkiv, samhälle och forskning* 39, no. 2 (1997), pp. 7–46.
- Millar, Laura A. *Archives: principles and practices*, 2nd ed. London: Facet Publishing, 2017.
- Misztal, Barbara A. *Theories of social remembering*. Buckingham: Open University Press, 2003.
- Nilsson, Nils. *Arkiven och informationssamhället*. Lund: Studentlitteratur, 1976.
- Nobles, Melissa. *The Politics of Official Apologies*. Cambridge (UK): Cambridge University Press, 2008.
- Nyberg, Louise. "... Tvånget att försaka. Bedömningsgrunder för gallringsbeslut." In *Information, förvaltning och arkiv – en antologi*, Härnösand: Landsarkivet, 2005, pp. 126–156.
- Nygren, Rolf, Jan Larsson & Sune Åkerman. *Samhällsdokumentation inför framtiden: en bok om samhällsforskningens framtida materialtillgång*. Stockholm: LiberFörlag i samarbete med Delegationen för långsiktigmotiverad forskning, 1982.
- Olsson, Anders R. *Att stänga det öppna samhället : Om ett politiskt missbrukat begrepp: personlig integritet*. Enhörna: Tusculum Förlag, 2008.
- Pettersson, Ulla. *Från fattigvård till socialtjänst: Om socialt arbete och utomparlamentarisk aktivitet*. Lund: Studentlitteratur, 2011.
- Qwerin, Gunilla. *Metropolit i massmedia: en studie av hur Metropolitprojektet bevakades och beskrevs av TV och Stockholmstidningarna*. Stockholm: Allmänna förlaget, 1987.
- Riksarkivet. *Om gallring – från utredning till beslut*. Riksarkivets rapportserie 1999:1. Stockholm: Riksarkivet, 1999.
- Rosengren, Anna. "Openness, Privacy and the Archive: Arguments on openness and privacy in Swedish national archival regulation 1987–2004." Working paper 2016:4. Huddinge: Södertörns högskola, 2016. Available at <http://urn.kb.se/resolve?urn=urn:nbn:se:sh:diva-30888>.
- Rosengren, Anna. "Offentlighetsprincipen i teori och praktik." *Arkiv, samhälle och forskning: ny följd* no. 1 (2017), pp. 27–58.

- Schoeman, Ferdinand David. *Privacy and Social Freedom*. Cambridge (UK): Cambridge University Press, 1992.
- Sköld, Johanna, Johanna Hedström & Emma Foberg. "Conflicting or complementing narratives? Interviewees' stories compared to their documentary records in the Swedish Inquiry on Child Abuse and Neglect in Institutions and Foster Homes." *Archives and Manuscripts* 40, no. 1 (2012), pp. 15–28.
- Sköld, Johanna & Shurlee Swain (eds.). *Apologies and the legacy of abuse of children in care: international perspectives*. Basingstoke: Palgrave Macmillan, 2015.
- Stahl, Bernd Carsten. "Privacy and Security as Ideology." *Technology and Society Magazine*, IEEE 26, no. 1 (2007), pp. 35–45.
- Stefanick, Lorna. *Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World*. Edmonton: AU Press, Athabasca University, 2011.
- Stenberg, Sten-Åke. *Född 1953: Folkhemsbarn i forskarfokus*. Umeå: Boréa Bokförlag, 2013.
- Stockholms Stadsarkiv. "Rutinbeskrivning för att gallra och leverera socialtjänstakter 2017". Available at <http://stadsarkivet.stockholm.se>
- Strange, Carolyn. "Stories of Their Lives: The Historian and the Capital Case File." In Franca Iacovetta & Wendy Mitchinson (eds.), *On the Case: Explorations in Social History*, Toronto: University of Toronto Press, 1998, pp. 25–48.
- Söderlind, Åsa. *Personlig integritet som informationspolitik: debatt och diskussion i samband med tillkomsten av Datalag (1973:289)*. Borås: Valfrid, 2009.
- Vetenskapsrådet. *Nationella riktlinjer för öppen tillgång till vetenskaplig information*. Vetenskapsrådets rapportserie. Stockholm: Vetenskapsrådet, 2015.
- Vincent, David. *Privacy: A Short History*. Cambridge (UK): Polity Press, 2016.
- Vismann, Cornelia. *Files: Law and Media Technology*. Translated by Geoffrey Winthrop-Young (in German 2000, Akten: Medientechnik und Recht). Stanford, CA: Stanford University Press, 2008.
- Wallberg, Evabritta. "Att undvika offentlighetsprincipen: Inträdesanförande i Kungl Krigsvetenskapsakademien avd V den 8 december 2004." *Kungl. Krigsvetenskapsakademiens handlingar och tidskrift* no. 1, 2005, pp. 61–72.
- Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1967.
- Åström Iko, Karin. "I allmänhetens tjänst: Arkivverket, tillgängliggörandet och brukarna." *Arkiv, samhälle och forskning* no. 1, 2003, pp. 18–37.
- Öman, Sören. "Särskilda registerförfattningar." In Cecilia Magnusson Sjöberg & Peter Wahlgren (eds.), *Festskrift till Peter Seipel*, Stockholm: Norstedts juridik, 2006, pp. 685–705.

Medical Records – the Different Data Carriers Used in Sweden from the End of the 19th Century Until Today and Their Impact on Confidentiality, Integrity and Availability

RIKARD FRIBERG VON SYDOW

Medical records have been used during all medical history, since Egyptian medicine almost 2000 years before Christ, and since the famous physician Hippocrates in Ancient Greece (Tweel/Taylor, 2010, p.1, Nilsson, 2007, p. 12). During the 20th century medical records have undergone a tremendous change in appearance. What has changed is not really the type of information in the medical records themselves, but rather the quantity and the quality of information, the type of data carrier that has been used, and how access to the records has been managed. Medical records have gone through many different phases, from the notebook of the individual physician, during the late 19th and early 20th century, when medical files were rare and only appeared in larger hospitals, to the period of the medical paper file, peaking from the 1950s until the 1990s. During this period, medical records grew thicker in a changing and more information dense health care, as more professions than physicians wrote down how they treated the patients, and as more tests were done on every patient. In the 1990s the most recent change started, as the file changed from being in paper form, using paper as data carrier, to being in digital form using different server solutions to store patient information. During the 20th century medical files grew from being around one page in the beginning of the century, four to five pages in the 1950s, and what can be described as a larger pile of paper towards the end of the century (Nilsson 2007, p. 143). This indicates a fast growth of information regarding patients during this century. Today several sources create the medical records: information from the patients themselves, information from different examinations, observations, tests and sampling. The source of information can also be persons related in some way to the patient, such as a child, a parent or a spouse (Sandén 2012, p. 16).

I am interested in how the changes that medical records have gone through have affected the confidentiality of the records, the integrity of the information they contain, and the availability of the records (for both patients and others). This is what will be investigated below.

Today well managed medical records that contain information regarding a patient's care, are regarded as a precondition for a good and safe care of a patient (Sandén 2012, p. 15). The concept I will use to analyze the changes over time regarding medical records is the CIA Triad, which is commonly used in the contemporary information security discourse. To use a method of analysis from contemporary information security on a partly historical material, might be unusual. I believe though, that there are gains in doing so. We will have a possibility to find problems related to information security that have affected information now in the archives. This, in turn can give us a clue as to how reliable these archival sources are to researchers today. By comparing different periods, we will also gain insights into what might influence and motivate contemporary information security. How will this be done? My investigation will be presented in the form of an essay. First I will explain some important terms from the discipline of information security that will be used in the analysis. Second, I will use these terms on medical information during three different time periods that I define below. The focus will be on the administrative routines regarding medical records in Sweden. Towards the end of the essay I will discuss the differences between the different time periods as well as the kind of problems we might face with medical information in the future.

There is to my knowledge, no other research that uses information security methods as a means of analyzing medical information and compare different time periods and ways of handling medical information. There is of course other research on medical records. I have used Inga Nilsson's doctoral thesis from Lund University 2007 "Medicinsk dokumentation genom tiderna – En studie av den svenska patientjournalens utveckling under 1700-talet, 1800-talet och 1900-talet" to gain historical insight regarding the development of medical records in Sweden. Parts of the discussion I am interested in have been presented in Ulrika Sandéns doctoral thesis from Umeå University 2012 "Sekretess och tystnadsplikt inom offentlig och privat hälso- och sjukvård – ett skydd för patientens personliga integritet" (Sandén 2012). Sandén discusses, among many other issues regarding medical records, how the recent changes in technology have changed the discourse of secrecy and confidentiality, using e-mail, text

messages and social media as examples (Sandén 2012, p. 43). Both these dissertations are used as sources and background material in this essay.

Confidentiality and other important terms

Medical records consist of information. Information regarding a patient's health. This will be the case in any period of time – from the antiquity to our time. It could not be in any other way at least as we understand medical records (and information) today. This makes it possible for us to use the terminology of information security to investigate the changes that have occurred in the use of medical records during the 20th century. In contemporary information security, the CIA Triad is one of the concepts used to describe aspects of information connected to security. CIA (sometimes in the order CAI to distinguish it from the US intelligence agency) is an acronym for confidentiality, integrity and availability (Andress 2015, p. 6).

Confidentiality refers to our ability to protect data and information from persons who are not allowed (or authorized if we are working in a formal organization) to view it (Andress 2016, p 6). In our contemporary digital world confidentiality is kept in organization by password protected systems, encrypted e-mails and by access control systems that keep the non-authorized away. Earlier in history similar systems were used, though being analog. Analog encryption, safes and vaults were common examples of such analog systems. However, the systems should not be considered the most important aspect in keeping the confidentiality; it is really the persons working inside an organization that constitute the soft spot of every security system.

Close to confidentiality is another term, privacy. Privacy has been defined in many different ways over time and is really hard to define in a convincing way. Raymond Wacks who has written multiple works on the subject has described an acceptable definition of privacy as “frustratingly elusive” (Wacks 2015, p. 42). I will sometimes also use another term, personal information. In the discourse of health records, this term situates itself closer to the patient than to the security system or to the ethics of the medical staff. Personal information – information connected to a person – might be private but with different degrees of privacy depending on what kind of information in the health record that we are referring to. Personal information could be described in a two axis system in which “desire to control” and “quality” are the two factors used to describe it. Desire to control is connected to ourselves as persons, to how we value a piece of per-

sonal information. Quality is how dense and exact the information is (Wacks 2015, p. 46). In the context of medical records, we can use two examples. If I broke my leg skiing last year there will be a large amount of (personal) information regarding this in my medical records. The information might be very dense and exact, thus of high quality. But my desire to control it might be small – how embarrassing is a broken leg? But maybe I was treated for a sexually transmitted disease last year. The information in my medical record regarding this might be very brief. The result of a urine test and a prescription of antibiotics. Not dense, not exact, but there might be a high desire to control it from my position. Personal information is a valuable tool of analysis – it regards both a normative function (desire to control) and a descriptive function (quality) as axis in the evaluation (Wacks 2015, p. 46).

There is also another term we need to be acquainted with that relates to confidentiality. In this text I will use the term “leak” (of personal/private/confidential information) to refer to a breach of confidentiality. A leak can happen in any information system that tries to introduce confidentiality and it will happen in any information system without confidentiality. Leaked information has, depending on motivation and resources, a possibility to spread. These possibilities have varied over time, as will be described later in this text. Confidentiality can, in short, be defined as the protection against unauthorized access to information and the protection against leaks of information.

Integrity is the next term in the CIA Triad. In information security, this relates to the possibility to hinder and monitor changes in information and data (Andress 2015, p. 6). If changes are made we need to know who did them and when. An information system that values integrity will produce documentation of how and when changes of the information have been made. We also need protection connected to our information so that only people who are authorized have the possibility to do these changes. The security measures needed to keep the integrity are close to those mentioned above regarding confidentiality.

Availability is the last part of the CIA Triad. Data and information are available when we can reach them (Andress 2015, p. 7) and the availability of the information is measured by how reachable it is. In a digital environment, the availability can be depending on the up-time of our servers, or the quality of our data connections. But also the rules of secrecy connected to confidentiality may have an impact on availability. In an analog environment, however, rules of secrecy and administrative opening hours, among

other things, regulate availability. In connection to confidentiality, availability can be seen as the possibility for an authorized person to reach the information. If medical records are available to more persons than those authorized persons there is a breach of confidentiality.

Medical records from the end of the 19th century to today

This essay will focus on a time-frame that begins towards the end of the 19th century, around 1880, and ends in our contemporary period in the 21st century. I will also do some observations of what we could be facing in the future, based on what is happening today. The time-frame will be divided into three different parts, connected to differences in records management and in the medical professions. These differences are partly connected to the data carrier that was in use. Data carrier, or data media which is another term often used, is a medium that can hold data or information. Examples are papers or hard drives. I use data carrier in a slightly wider sense, also including parts of what we could call the information system – the paper file, the notebook or the digital file. The three different periods of time I will use are overlapping and not in any way absolute. I will try to make an illustration of what can be considered a normal administrative procedure during each period. The first period is called “the notebook and the proto-file” and starts at the end of the 19th century. During this period, the information connected to the medical care of patients was scarce, but a change started to happen in larger hospitals. Two data carriers dominated information management in the medical profession, the portable notebook in which the professional could write notes about their patients, and the early paper file, which I call a proto-file. The proto-file is more connected to a hospital environment than the notebook and consists of different forms about the patient that eventually would make up a file. The next period starts after the Second World War and is called “the filing cabinet”. During this period, which lasts until the 1990s information in medical care grows. Systems are created to manage information and laws are written to secure it. The main data carrier during this time is the paper file. The third period starts in the 1990s and continues until our days. I will call this period “the digital file” after its main data carrier – digital files of various types connected through an information system. Digitalization of medical information started as early as in the 1950s but it was not until the 1990s the whole medical record became digitalized, not only statistics and separated data. With this overview, it is now time to turn

to the results of the first period dominated by the notebook and the proto-file.

The notebook and the proto-file 1880–1950

Outside the hospital environment, we can only speculate how information about patients and their medical conditions was treated. Of course, physicians and other health professionals outside of the hospitals took notes about their patients. These are sometimes preserved in archival institutions. One example is the midwife diaries (*Barnmorskedagböckerna*) in which midwives took notes regarding births they were involved in. A database search in the National Archival Database of Sweden shows that the earliest midwife diaries that have been preserved originate from the end of the 19th century and the latest from around 1950. They are very few in numbers, reminding us that the only documents kept in the archives are records that have been delivered to the archives in the first place. We simply don't know what happened to those diaries that were not delivered to the archives. They might have been destroyed or maybe they were kept in private possession.

We have a better grasp of those medical records that were created and kept in a hospital environment. These records were regulated in the hospital instructions. The earliest instructions preserved which mentions medical records is from the Royal Seraphime Hospital in Stockholm and dates from 1851. This instruction only mentions that the responsible physician should write the journal of his patients, and that the head physician should sign it when the patient was dispatched or deceased (Nilsson 2007, p. 73). In 1863, The Royal Health Commission (Kungliga Sundhetskollegiet) published directions regarding what information that should be included in each patient's journal. Some of these were obvious from a patient's perspective (name, disease et cetera) and some of them maybe less obvious (profession, paid fee et cetera). They were to be used by all larger hospitals in the country and were presented together in a printed form (Nilsson 2007, p. 75).

During this period two kinds of data carriers were in use: the notebook and what I call a proto-file. As mentioned earlier, I use the term proto-files for forms that could make up a file when stored together. Sometimes, we may guess, files were created by putting together different forms connected to the care of the same patients. At least the opportunities to do so were present. The task now is to analyze these two different data carriers by applying the different concepts of the CIA Triad.

Regarding confidentiality, what kind of unauthorized access or information leak could occur within the premises during this period? Two kinds of data carriers exist during this period, both consist of paper, and the information is handwritten to the surface. The data carriers are used in slightly different circumstances. The notebooks, the midwife diaries being one example, were carried from patient to patient. There is a possibility that they could be lost during the way, dropped, forgotten in a patient's home, or stolen in some way. If this happened they could be read by those who found them. The only possibility to copy the information during the period, copying being a prerequisite for a leak to occur, would be by hand. This is a process that takes a lot of time and effort from the person doing it. From a physical point of view the proto-file is a little safer as it is kept in a hospital and not moved around the way notebooks are. There is a possibility that they were kept under lock and key when not in use. If this was the case, the possibility of confidentiality rises. Regarding the possibility to copy the information, the situation is similar to that of the notebook.

As for integrity – the possibility to know if any information stored in the data carrier has been compromised or changed – the situation is quite similar for the proto-file and the notebook. They are both written by hand, which makes the possibilities to change the information low. The notebook was somewhat of a personal item, and, so, was usually written by one hand only. The proto-file could be written by more than one person, making the possibility of unauthorized changes a little more likely. Of course, there could be forgeries of the handwriting used, but this calls for quite a lot of effort from the perpetrator's perspective.

As for availability of the information to the medical staff, both these data carriers are location-bound. The information stored in them can only be available at one location at any given time. If the notebook or the proto-file is lost, all information regarding the patient is lost too. From the patient's perspective, the availability of the information is low. There is no evidence that patients had access to their own medical records. But, during this period, the density, the amount, of information kept in medical records was very low compared to today. Information could thus have been transferred through conversation among the medical staff.

The filing cabinet (1950–1990)

The next period starts somewhere between the year 1900 and 1950. The change happened gradually so we will use 1950 as the definitive year when the period has begun. The period 1900–1950 is within the time-frame

during which the modern concept of record management is introduced in Sweden and when standardizations of forms and paper-size are introduced (Järpvall 2016, p. 68ff). The archival concept of provenance – that records created by an organization should be kept together as one archival unit – is introduced in Sweden by *Riksarkivet* (the National Archives) in 1903. At the same time the first common records inventory-system, the *allmänna arkiv-schemat* (“the common archive inventory”) is introduced (Smedberg 2012, p. 246f). This is the period of time when order and accountability are introduced in a wider perspective in record management in Sweden. This is also when office work is standardized and organized in an effective way, making it possible to transfer information effectively. This development peaks in the 1950s when the punch card machine becomes so standardized that it could be used in ordinary office work. A number of other machines and standardizations during this time made administration more effective than ever. According to media historian Charlie Järpvall, who has investigated the effectiveness of the paper medium in 20th century Sweden, these changes had a major impact on the possibility of transferring information using paper as a data carrier (Järpvall 2016, p. 108). Information could therefore be transferred in a much more effective way than before through photocopying or using typewriters. This will have a major impact on how we will view the medical records when we analyze them using the CIA Triad later on.

Towards the end of the period, in 1985, the use of medical records is standardized in a more regulated way through the *Patientjournallagen* (1985:562), the new Swedish law regarding medical records. *Patientjournal-lagen* was introduced after a long inquiry in which older routines and regulations already in use in Swedish hospitals were investigated and evaluated. The integrity of the patient was the focus of this evaluation. I will use the inquiry that was made prior to the law, SOU 1984:73 “Patientjournalen – Huvudbetänkande av journalutredningen”, as my main source of information about regulations and routines and I also use its description of the historical development as a background.

After the Second World War two changes occurred regarding medical records that had a major impact regarding the use of the records. First, in 1947, Sweden introduced the personal identity number, a unique identification number for every citizen. The number consisted of six digits stating the date of birth (YY-MM-DD) and three digits connected to the person’s birthplace. The last of the three birthplace-connected digits was even for female persons and uneven for male persons. In 1967 an extra digit, a

checksum that could be derived from the rest of the personal identity number, was added whereas the connection to birthplace was removed in 1990 and replaced by a random number (SCB 2016, p. 4ff). Medical records were soon sorted using the patients' personal identity numbers, thus removing the problem of sorting records when more than one patient had the same or similar names (Nilsson 2007, p. 147). The second important change is that medical professionals stopped writing medical records by hand. Instead the typewriter was used, which, in general, made the text in the records easier to understand (Nilsson 2007, p. 147).

Medical information increased during this period (Nilsson 2007, p. 143). The proto-file had become a file, and the file was increasingly thicker. According to Cornelia Vismann a file is "a repository of authoritarian and administrative acts" (Vismann 2008, p. xiii). These files, being an amalgam of decisions, data and information regarding a patient materialized in the form of a collection of paper bound together by a cover, one file for each patient. Medical care had become more and more advanced and dense in information. The staff was larger, with more experts involved contributing with their piece to the information puzzle of the medical records. From the beginning only physicians documented their information regarding the patients. During the 1950s and 1960s physical therapists and nurses were among the new professions that contributed information to the medical records. Before, the physicians wrote all documentation themselves. Now there were secretaries employed at the hospitals taking notes and transcribing recorded investigations of patients (SOU 1984:73, p. 65ff). The typewriter had a key role in this work. It was the main production instrument creating the records. But several other technical achievements connected to information were introduced in the medical sphere, alongside the typewriter. Early computer registers were used, although complete medical records in digital form were not used until the end of this period (SOU 1984:73, p. 146f). The photocopier was invented as early as the 1930s but was not introduced on the market until the 1950s (Encyclopedia Britannica: Photocopier). It could be used to make copies when records were needed in more than one place at the same time. It also made it practically possible to give the patient a copy of his or her medical records which the new Patient-journallag stated should be done upon request (Patientjournallag 1985:562, § 16). In 1980, something crucial regarding patients' rights was introduced. If approved by the *Socialstyrelsen* (The National Board of Health and Welfare), patients could have their medical records destroyed (SOU 1984:73, p. 15). When the inquiry was released in 1984, 331 patients had

applied to have their medical records destroyed. Only 164 decisions had been made due to low work-capacity. Fifty percent of these were connected to psychiatric care. In most cases destruction was granted. In 66 cases Socialstyrelsen decided not to destroy the records, and in 18 cases the records were partly destroyed (SOU 1984:73, p. 180).

If we apply the tool of analysis, the CIA Triad, what can we say regarding aspects of confidentiality during this period? There are some differences compared to the period described earlier. Firstly, there are more professionals taking part in the care of the patients, the effect being that more persons have access to the medical records. They would all have to follow the same rules of confidentiality, but the risk that information could leak without a possibility to trace information leakage, is indeed larger. The files not used would, hopefully, be under lock and key, in a safe archive space, the only persons that could reach them being those having the key. There are no possibilities to check if anyone has accessed the information. Even if mandatory signing of medical records could be a way of tracing who has been reading which record, there is no way of determining if the signatures reflect who has actually read the record. Secondly, the photocopier gives us both a possibility to copy the medical record (to access it or to give access to unauthorized persons) and a possibility to spread the information, thus creating an information leak. If we want to access our own records, there will be measures to increase confidentiality. There will be a clerk or other types of authorized personnel between us and the record, and if the system is working they will check our identity before giving us access. This procedure will be different in the next period that we will examine.

There are some problems connected to integrity during this era that we need to discuss. The technology both adds the possibility to control the integrity and to compromise it. The personal number increased integrity by adding proof that a file was connected to a single individual. This could have been a problem earlier, when only names were used to identify a person and sorting was done using the last name. Personal numbers could now be used as an authenticity method improving both the control and the sorting of records (Nilsson 2007, p. 119, p. 133). But some of the other technologies could compromise the integrity. The photocopier, mentioned above as a possible confidentiality breach, could create multiple copies creating the problem of deciding which version of a file was used last. Before, handwriting was mentioned as a possible proof of integrity, creating the possibility of checking if the same person had done multiple entries. The typewriter changed this, making it hard to decide who had made different

entries, especially over a longer time. In a serious situation, there would have been a possibility to investigate at least which typewriter that had been used. This had been done in a famous case from 1952, when slanderous letters were spread to compromise candidates in a bishop-election to the diocese of Strängnäs. When a suspect (one of the candidates) was found, the typewriters in his workplace were analyzed, checking the types for differences that would match the text in the letters. Proofs were found, and the suspect was later convicted (Brottets Krönika 1954, p. 579ff). But, without possibility to a thorough examination and analysis, handwriting is a much easier way to prove integrity.

Regarding availability there were possibilities for patients to access their medical records before the new law in 1985 if they applied at the hospital (SOU 1984:73, p. 57ff). They also had the possibility to have their records destroyed, thus making availability impossible for both patients and staff (SOU 1984:73, p. 179ff). A problem with destruction of records is that it cannot be made undone. There is always a possibility that the patient regrets the destruction afterwards, especially if any mistreatment done during one period of time could be grounds for financial compensation later. The medical staff had less control of availability of the medical records during this period, compared to the earlier one. The increased number of staff using medical records made the disappearance of records a threat. According to the inquiry made before the new medical records law of 1985 up to 20% of the medical records could not be found when the staff needed to use them. This was recognized as a problem that compromised patient safety (SOU 1984: 73, p. 145).

The digital file (1990–)

Today medical records have gone through a radical digitalization, just like many other types of records. This process gained speed during the 1990s and the borders are somewhat fuzzy between the period I call “The filing cabinet”, and this later period. The digitalization was foreseen in the inquiry that led to the medical records law of 1985, mentioned earlier. In 2008 a new law, Patientdatalag (2008:355) was introduced, making the changes obvious in the title, as the word “record” (journal) from the previous law was replaced by “data”. Today the main medium used to keep medical records is larger digital information systems (Sandén 2012, p. 75).

The digitalization of medical records gives the medical personnel some obvious advantages. It is possible to reach the record, stored on a server, from terminals in multiple places through a terminal/server system. With

the increase of bandwidth, it might be reachable from any place, in the world, if the system is connected to the Internet. This makes it possible for many different parts of the health care system to use the same original, digital, record, accessing it on a server from more than one terminal. No copies need to be made. In the legal process leading up to the *Patientdatalag* (2008:355), the idea was actually mentioned that the patients could be the owner of, and was to grant the caregivers access to, their own medical record. In the end, this suggestion was not included in the law (Prop. 2007/08:126, p. 78). Instead a protection against the spread of information between different caregivers was implemented called “sammanhållen journalföring” (integrated medical record). If a patient wants his or her medical record protected from being shared to other caregivers this should be granted (Sandén 2012, p. 193).

Unauthorized data access is one of the problems occurring in this period. It can be divided into two types of unauthorized data access, external unauthorized data access and internal unauthorized data access. This is a distinction usually made by computer security specialists, normally for the two different ways a computer system can be attacked. The attack is external if the perpetrator has no privileges in the system from the beginning. In an internal attack the perpetrator has such privileges most likely in the form of a login and a password (Beta Telelink 2017). In SOU 1984:73 external unauthorized data access was not mentioned at all as the computer systems were not being tied to any kind of public network at this time. Internal unauthorized data access was mentioned however and the solution suggested to remedy the problem was education for the staff regarding the information that could be accessed (SOU 1984:73, p. 78). Since the beginning of this period internal unauthorized data access in connection to medical care has been fairly common. This is connected to the fact that medical staff has authorized access to medical records system whereas the only records that they are actually allowed to access are those belonging to patients that they are involved in the medical care of (Sandén 2012, p. 99). In a case from 2016, a nurse accessed her former partner’s medical records from her workplace while he was suffering the consequences of an accident. She claimed that she had his permission and he claimed that he had never given it to her. The court’s verdict was that she was guilty of unauthorized data access, and that this was regardless of any given permission. Access to the system was given to her as an employee, and as such she had no relation to the care of her former partner. Accessing the records would therefore be illegal regardless of any permission from the patient (Luleå TR 1868-16).

One verdict from late 2016 stands out a bit, both because of the number of medical records accessed and because the case could be described as “semi-internal” unauthorized data access. The verdict is from a case in which a physician had gained access to a large amount of digital medical records from a Swedish hospital. He accessed these records after his employment at the hospital had ended, and after he had moved to a location outside of Sweden. Keeping his login account (and also hacking a couple of other employees’ accounts) he gained access to both former patients’ and former colleagues’ medical records. During the trial the physician claimed that he needed the records for his research (Stockholms TR 4093-15). Unauthorized data access is regulated both in the Patientdatalagen and in chapter four, paragraph 9c of *Brottsbalken* (The Swedish Penal Code) thus making it a crime that you actually can be punished for (Brottsbalken 1962:700). In the end, the physician was sentenced to probation and he also had to pay compensation to the patients affected by his unauthorized access.

A recent change connects the digitalization with the legal possibilities for a patient to access his/her own medical records. Today, this can be done in most *Landsting* (the Swedish main local caregivers) through the Internet with an electronic identification. This kind of access has been debated both in the press and by the lawmakers. This is because there is a slippery slope between the use of this service by the elderly on the one hand, and on the other, the access to the records that might be given to their younger relatives (sons and daughters et cetera) who help them accessing their medical records online. I call this a slippery slope because for some of the elders, the help from more digitally able younger relatives might be the only way to get access to their medical records when these are digitalized. The question discussed is whether the relatives are supposed to have the possibility to view their elder relatives’ medical records, a dispute that has not yet been settled legally. Writing this, the matter will be settled in *Högsta Förvaltningsdomstolen* (The Swedish Supreme Administrative Court) during 2017 (Andersson, 2016). Even though there is an upcoming settlement in the case, the problem is not entirely solved. The access to the medical records is regulated by an electronic identification, a file on your computer and a code, or through an application on your smartphone and a code. It might be relatively easy for a relative, or anyone with connections to the patient, to gain access to code + file/application, depending on the patient’s personal experience of, and attitude towards, digital security. To the very least it is more likely than before that someone else will gain access

to your medical records. As long as the paper file was used you had to show up at the hospital and present yourself to a clerk, proving in person that you were actually you. These meetings in person are now replaced by an application and a code.

Now we will turn to the analysis using the CIA Triad. Some changes in confidentiality are connected to the digitalization. The possibility of both internal and external unauthorized data access must be seen as an increase regarding the problems of confidentiality. This, in turn, can be a problem for the patient's privacy. Contrary to earlier periods, there might also be a problem regarding the confidentiality of information in general. The possibility to process and store (and leak) large amounts of information is much more substantial today than during the period of the paper file. A leak of information that you would need a truck to accomplish when the information was stored on paper, can happen very easily today as the information can be stored on a USB flash drive that fits in your hand. You don't even need to show up to gain access. This is also the case regarding access to individual patient's files through the Internet and electronic identification mentioned earlier. It seems as though the loss of a human connection (the clerk) might cause a loss of confidentiality.

As for integrity, there might be some issues with the early digitalization. The personal identification number can be used as a natural key in a database. A natural key is a point of reference that can be the connecting item in a database, at the same time as it is readable and understandable to humans (C2, 2017). This can be seen as a positive aspect of the digitalization process because traceability increases when markers of identification (like a personal identification number) can be used both outside and inside the digital information system. But at the same time there are problems with digitalization and integrity. This is linked to the fact that changing data through unauthorized or authorized access has become much easier than when paper files were used. And the amount of data preserved can make it very hard to track all changes that have been made. Another, although less common, problem with the design of the Swedish personal identification number is linked to the fact that a person might have the same number as another if the first owner dies (and the number is reused), or if the first owner lives to be over one hundred years old. This is a factor that the system designer must consider when using Swedish personal identification numbers, which are given to people both at birth and when they migrate to Sweden and are granted citizenship. This needs to be considered especially

if a number is to be used in the information system after the owner dies (Ludvigsson et al 2009, p 5).

As for availability, this aspect of the CIA Triad certainly has increased. The possibility to reach your own medical records over the Internet from your home is something very different in comparison to getting a copy of your paper file. The online record is dynamic – you can see the changes soon after they have been done. The staff also gains availability as the file is reachable from all locations with a computer connected to the hospital network. This is, of course, if the system does not crash. Several times digitalized medical records systems have crashed with great consequences for the work of the medical personnel. During the fall of 2016, COSMIC, the medical records system of one of Sweden's largest hospitals, Akademiska Sjukhuset in Uppsala, crashed. During more than a week operations were canceled, visits postponed and queues rising. The staff had to use paper and pen, which was enough to provide care, but very problematic when all health care processes presupposes support from a digital system (Nilsson, 2016).

Conclusions and problems of the future

We will now revisit the different periods to try and trace what kind of differences, regarding the components of the CIA Triad that have been discovered. After this summary of the main results I will discuss some problems connected to medical records that we might see more of in the future. All of these problems are connected to the digital era that we live in today.

What kind of changes in the confidentiality of medical records have occurred during the investigated period of time? We started in an era where the only people with general access to the medical records was the medical staff. Patients on the other hand had little or no access. The amount of information regarding a patient's care was much lower during this period compared to today. In general, the first period must be seen as providing a higher level of confidentiality than the second and the last. The only flaw in confidentiality was if the records were lost. From the introduction of office machines such as typewriters and photocopiers in the period of the filing cabinet, the possibilities of a leak increased rapidly and reached its highest level in the last period, the digital file. Summing up we must say that the automation has had some drawbacks if we consider the possibilities for information to remain confidential.

Regarding integrity, i.e. the ability to check if information has been changed, we have a similar development as with confidentiality. The earliest system I described was characterized by a high level of integrity. Written by hand the documents are unique in design and hard to forge. As soon as the different office machines are introduced this changes, however. The amount of information increases, and forgeries and other problems related to duplicability are harder to detect. We can argue that integrity increases when the personal number is introduced – at least it hinders some integrity flaws that can appear through errors like sorting records the wrong way or mixing different patients' records. In the digital era, the integrity of medical records is increased by the possibilities to use checksums and log files to spot if the information has been changed. However, the amount of information is huge and if the system is flawed in some way problems of integrity might be very hard to trace.

Availability is the only concept of the CIA Triad that actually increases unproblematically during the period I have examined. "Unproblematically" if we believe that the possibility to access medical information fast is never a problem. From being available to the medical staff only, the medical records can nowadays be reached from your home through the Internet. It is also much easier for the medical staff to reach it, giving them the possibility to read the same record at the same time, though not being in the same place. This is of course only true if the computer system works – the main distortion to availability today is linked to problems with up-time. Digital files that are not possible to use due to an information system not working properly is a serious problem in contemporary clinical medicine, and might make certain medical care impossible.

But is the information regarding our medical care more or less private today than during earlier periods? That actually depends on more factors than the medical records. One of these factors is connected to how (and to whom) we speak about our own, or about our relatives', medical difficulties. Similarly, if we are in a medical profession, it depends on how we speak about our patients' medical difficulties. One discussion connected to this, and mentioned earlier, is the distinctions between confidentiality, privacy and personal information. Regarding medical records the term personal information is most useful. How we, ourselves, treat our personal information is up to us personally to decide about. We can consider the information to be private or not. If we want to release it, in speech or in text, it is our own decision. The possibility to release our own personal information is not connected to any specific period of time or to any specific data carrier. The

important factor is that if a release takes place it is our own decision. However, possibilities to spread personal information will be larger in the period of the digital file, because of the powers of our contemporary information networks.

There are at least three interesting phenomena that are new to the subject of digital medical records, and that we don't know the full extent of yet. These phenomena have been discussed to some extent in the debate regarding medical records, and they are all connected to confidentiality. The first phenomenon relates to data that the patient themselves collect through a Fitness Tracker, a bracelet that monitor your movement, your heart rate and other pieces of information connected to your body. Fitness Trackers could be connected to your medical records in the future. The Trackers have mostly been discussed in connection to insurance, as they contain the type of information any company that provide health insurance could be interested in (SOU 2016:41, p. 402). Several interesting factors could be analyzed through the CIA Triad here, if the information from Fitness Trackers was connected to medical records. One such factor deals with the extent to which the patient is aware of what he or she is adding to the record while using a connected tracker, with the level of privacy of the information, as well as with the period of time the data will be preserved in the digital records system. There are also integrity issues connected to giving access to the records system to different Trackers. This is more of a computer security issue than an actual information security issue, however, and the problems are more of a technical kind.

Another phenomenon that is discussed among medical professionals is "Patient Targeted Googling", PTG (Baker, 2014). PTG is an expression used for medical professionals using the Internet to read and gather information about a patient. This information gathering could be made for a number of reasons, just curiosity being one possible cause. It must be seen as an intrusion of the privacy of the patient, but is difficult to regulate. The phenomenon therefore constitutes an interesting grey area of professional ethics. In the future, problems related to the Internet as an "extra layer of information" connecting different sources, might grow in number and include more professions than those in the medical field.

The final phenomenon discussed here that might give us a headache in the future is a possible increase in external unauthorized data access. This could happen when more and more repositories of medical records are connected to the Internet, and it has happened, for sure more often than we know about. In 2016, there were reports of over 10 million hospital records

being for sale through the anonymous Darknet-network. The records supposedly originated from external unauthorized data access (through hacking), but we don't know if anyone actually bought them (Techtarget, 2016). Connected to all these problems is the concept of doxing. Doxing is the act of publishing personal information about individuals online with the purpose of intimidating them. Doxing could violate both confidentiality, if the information is from a system with limited access, and privacy if it is connected to personal information. The term comes from the hacker culture where "dropping documents" or "dropping dox" connected to individuals was a way of making them lose the anonymity they had behind their hacker name. The phenomenon first emerged in the early 1990s, in Bulletin Board Systems and the early Internet, but has now spread and is quite common (Douglas 2016). It can be compared to writing a person's phone number on the wall of a public toilet, but doing this on thousands of toilet walls at the same time. Doxing could be very problematic if someone would use stolen or leaked medical records which often contain information that we consider private. Doxing is also related to the concept "Personal information" discussed earlier, as it is a mixture of general information about a person (where the person lives et cetera), and more private information (what the person has done, which alias the person uses on the Internet). As explained earlier, leaks can occur from any information system, analog or digital. But in the Internet era, it is much easier to spread information than before. The medium (the Internet), and how easily the medium can transfer information, is in this case more important than the message (the personal information) to use McLuhan's famous expression (McLuhan 2003, p. 7, p. 253).

It is always hard to predict the future, but it certainly seems that the amount of information, both personal and other, will continue to grow. In turn this growth is likely to affect all parts of the CIA Triad, not in the least, as seen in my examples above, that of confidentiality. How we will deal with these problems of information security and information growth is something we must decide in the near future.

Bibliography

- Andersson, Joakim (2016) "Anhörigas journaltillgång upp i högsta instans"
Available online 2017-10-22.<http://lakartidningen.se/Aktuellt/Nyheter/2016/12/Anhorigas-journaltillgang-upp-i-hogsta-instans/>
- Andress, Jason (2015) "The Basics of Information Security – Understanding the Fundamentals of InfoSec in Theory and Practice", Oxford: Syngress

- Baker, Maria J, George, Daniel R & Kauffman, Gordon L (2014) "Navigating the Google Blind Spot: An emerging need for professional guidelines to address Patient-Targeted Googling", J Gen Intern Med 30(1):6–7
- Beta Telelink (2017) "Unauthorized access", Available online 2017-06-06. <http://itsecurity.telelink.com/unauthorized-access-2/>
- Brottsbalken (1962:700)
- Brottets krönika (1954) "Biskopsbrevet", Stockholm: Medéns Förlag ABC2 "Auto key versus domain key", Available online 2017-06-06. <http://wiki.c2.com/?AutoKeysVersusDomainKeys>
- Douglas, David M (2016) "Doxing: a conceptual analysis", Ethics and information technology, 6/2016
- Järpvall, Charlie (2016) "Pappersarbete – Formandet av och föreställningar om kontorspapper som medium", Lund: Lund University
- Ludvigsson, Jonas F, Otterblad-Olausson, Petra, Pettersson, Birgitta U, Ekbom, Anders (2009) "The Swedish personal identity number: possibilities and pitfalls in healthcare and medical research" European Journal of Epidemiology. 24:659–667
- Luleå Tingsrätt, Verdict B1868-16, 2016-09-29
- McLuhan, Marshall (2005) "Understanding Media – The Extension of Man" London: Routledge
- Nilsson, Inga (2007) "Medicinsk dokumentation genom tiderna – En studie av den svenska patientjournalens utveckling under 1700-talet, 1800-talet och 1900-talet", Lund: Lund University
- Nilsson, Sophia (2016) "Stora problem för vården i Uppsala efter kraschat journalsystem", Computer Sweden, Available online 2017-06-06. <http://computersweden.idg.se/2.2683/1.664717/upsala-journalsystem-krasch>
- Patientdatalag (2008:355)
- Patientjournallag (1985:562)
- Prop 2007/08:126 "Patientdatalag mm", Stockholm: Regeringen
- Sandén, Ulrika (2012) "Sekretess och tystnadsplikt inom offentlig och privat hälso- och sjukvård – ett skydd för patientens personliga integritet" Uppsala: Iustus Förlag
- SCB (2016) "Personnummer", Stockholm: Statistiska Centralbyrån
- Smedberg, Staffan (2012) "Sverige" in Jörvall et al, Det globala minnet, Stockholm: Riksarkivet
- SOU 1984:73 "Patientjournalen – Huvudbetänkande av journalutredningen"
- SOU 2016:41 "Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommitén"
- Stockholms Tingsrätt, Verdict B4093-15, 2016-10-27
- Techtarget (2016) "Nearly 10 million hospital patient records for sale on dark net web market". Available online 2017-02-17. <http://searchsecurity.techtarget.com/news/450299408/10-million-hospital-patient-records-up-for-sell-on-dark-web-market>

- Tweel van den, Jan G & Taylor, Clive R (2010) "A brief history of pathology: Preface to a forthcoming series that highlights milestones in the evolution of pathology as a discipline", *Virchows Archiv*, vol 457, issue 1
- Vismann, Cornelia (2008) "Files – Law and Media Technology" Stanford: Stanford University Press
- Wacks, Raymond (2015) "Privacy – A very short introduction", Oxford: Oxford University Press
- The Encyclopedia Britannica was used to gain information regarding the history of the photocopier.

The Right to Access Health Data in France: The Contribution of the Law of January 26, 2016

WILLIAM GILLES

France is currently making deep reforms on its legislation to adapt to the issues of the Digital Revolution. In matters pertaining to data, this evolution becomes even more necessary, since, for a long period, the legal framework of these subjects was based on statutes adopted at the end of the 1970's. On one side, the Law of January 6, 1978 on data protection – entitled Law on Information, Technology, Data files & Civil Liberties¹ – regulates automated processing of personal data and non-automated processing of personal data contained in files. The purpose of the Act is to prevent detriment to Human Rights, Privacy or Public and Individual Freedoms². On the other hand, the Law on Access to Information of July 17, 1978³ establishes the means of access to data detained by the Public Administration. Later modified by the Order of June 6, 2005⁴, the Law authorizes explicitly everyone to reuse the data for purposes other than those of the public service which produced and collected them.

Almost four decades old, and originated from a drastically different technological context, these texts began to look outdated, despite the evolutions required especially by the transposition obligation stemming from European Law. Regarding Personal Data processing, changes were made years late, especially with the Law of August 6, 2004⁵, that transposes the Directive 95/46 CE on data protection⁶. Regarding the Law on access to information

¹ In French, loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

² In this sense, see, for example, Article 1 of the Law No. 78-17 of January 6, 1978.

³ Law No. 78-753 of July 17, 1978. In French, loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

⁴ Order No. 2005-650 of June 6, 2005.

⁵ Law No. 2004-801 of August 6, 2004.

⁶ Directive No. 95/46/EC of the European Parliament and of the Council of 24 October

of July 17, 1978, this statute has been subject to two major modifications, in 2005⁷ and 2015⁸, in order to allow France to transpose the two Directives on public sector information⁹. Yet, one must note that the essential part of this text has recently been revoked in order to become a part of the Code of the Relations Between the Public and the Administration enacted at the end of 2015¹⁰.

However, major legal changes are coming. Naturally, one must mention the Regulation on personal data¹¹ that has recently been adopted by the EU¹², and which the Member states of the European Union will apply Spring 2018¹³. Nonetheless, although the European Union establishes common rules applicable to all Member States on data issues, each State still has a lot of leeway to regulate its own data. For France, specifically, the Digital Republic Law of October 7, 2016, participates to a reform of public and private data law¹⁴. With this text, the French government wishes to turn France into a pioneer in Data Law. In that respect, France decided to exceed its European law obligations on the Right to Reuse Personal Data by reinforcing the Right to Publication¹⁵. The law also strengthens Personal Data Protection beyond European duties that France has, by granting people the right to dispose freely of their personal data (right of self-determination

1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

⁷ Order No. 2005-650 of June 6, 2005.

⁸ Law No. 2015-1779 of December 28, 2015.

⁹ Order No. 2005-650 of June 6, 2005.

¹⁰ See Order No. 2015-1341 of October 23, 2015, and Order No. 2016-307 of March 17, 2016.

¹¹ The text can be accessed at: <http://www.numerama.com/politique/135243-reglement-europeen-sur-les-donnees-personnelles.html>.

¹² See European Parliament legislative resolution of April 14, 2016 about the position of the Council on first reading, given the adoption of the European Parliament and Council rule on personal data protection regarding the processing and free traffic of personal data.

¹³ See Article 91 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

¹⁴ The Law also includes other determinations, such as the loyalty of internet platforms in order to fight the digital divide. See Law No. 2016-1321 of October 7, 2016 for a Digital Republic.

¹⁵ See W. Gilles, "La loi pour une République numérique ou le droit des données publiques entre ombres et lumières", Minutes of the « Premier Colloque Italo-français sur le droit du numérique » (forthcoming).

over its personal data¹⁶) or by creating the right for a person to decide what will happen to his/her personal data after his or her own decease¹⁷. Although the law of October 7, 2016, intends to change profoundly the Data Rights and to strengthen the right to open data¹⁸, it does not, however, truly tackle the issue of health data. This does not mean the legislator isn't interested in this topic. The reason why the Law for a Digital Republic is rather silent about the issue is because the French government decided to tackle this problem in a different text, the Law for Modernizing the French Health System, adopted in January 2016. Thus, these reflections on the opening of Health Data in France is inserted in this broader reform scenario, that relies on the New National System of Health Data, or in French "Système National des Données de Santé" (SNDS).

1. The Creation of a National System of Health Data (SNDS)

With the creation of the SNDS, the implementation of Health Data opening will be made easier as these datasets become accessible on a centralized database. Created by the law of 26 January 2016¹⁹, the SNDS entered into force on 1st April 2017²⁰ to replace the *Système National d'Information Inter-régimes de l'Assurance Maladie* (SNIIRAM) that was created in 2008²¹ which in turn replaced the former "*Système national Interregime*" (SNIR).

The SNIIRAM was a National System for Inter-regime Information of Health Insurance, and the main database of individuals' Health Data. The SNIIRAM was only one of the several French medical and administrative databases, which allows the management of over 1.2 billion treatment forms, 500 million medical acts and 11 million hospital stays²². The SNIIRAM was an information system that relies on a national medical and administrative database presented on a "pseudonymized" format²³ in order

¹⁶ See Article 54 of the Law No. 2016-1321 of October 7, 2016 for a Digital Republic.

¹⁷ See Article 63 of the Law No. 2016-1321 of October 7, 2016 for a Digital Republic.

¹⁸ This law has amended the French existing legal framework on freedom of access to information to add the right to reuse public information.

¹⁹ Article 193 of the Law No. 2016-41 of January 26, 2016 for Modernizing the French Health System.

²⁰ See the Decree No. 2016-1871 of 26 December 2016.

²¹ See Article 21 of the Social Security Financing Act for 2008 (loi de financement de la sécurité sociale pour 1999).

²² See Health Bill, Impact Study, October 14, 2014.

²³ Meaning that the database use pseudonyms as identifier instead of real names. See A.

to respect the right to privacy. Its technical management was carried out by the National Health Salary Workers' Health Insurance Fund (Caisse Nationale de l'Assurance Maladie des Travailleurs Salariés – CNAMTS)²⁴. This data warehouse was supplied by all organizations that manage a health insurance database (especially with the information coming from the treatment forms).

This information system was created to foster the awareness of the costs of all the health insurance regimes, as well as the transmission of relevant information to health services providers on their activities and revenues, and when applicable, also on their medical prescriptions²⁵. The aim, as of 2005²⁶, was also to support the definition, the implementation and the evaluation of Public Health Policies. In other words, the data processing of the SNIIRAM helped improve treatments, Health insurance management and health policies, but also allowed to transmit to health professionals information that concerns their activity.

To do so, this database had information that allows access to characteristics of statements of refund, access to information related to health cares performed and the history of procedures (the detailed acts, goods and services submitted to refund; dates of procedures and of refunds; identification of the institution, of the professional and how the costs were borne; amount, contribution and the service's coefficient)²⁷. This same database had also the number of "pseudonymity" of the insured and of the beneficiaries, as well as data related to gender, year and month of birth, city and department of residence and, when applicable, the date of death of the patient.

Pfitzmann and M.Hansen, *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*, Feb. 15, 2008, available at:

http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf.

²⁴ See Article 5 of the Decision of July 19, 2013.

²⁵ See Article L161-28-1 of the Social Security Code, created by the Article 21 of the Law No. 98-1194 of December 23, 1998, as amended by the Law No. 2004-801 of 6 August 2004.

²⁶ This amendment was made by Article 24 of the Law No. 2004-806 of August 9, 2004, regarding public health policy.

²⁷ See Decision of July 19, 2013, regarding the implementation of the National Inter-Regimes Information System on Health Insurance

At the end of 2015, the data collected in accordance to SNIIRAM allowed the collection of three different categories of data²⁸. For one part, 15 sets of datamarts had been obtained. Consisting of aggregate data for a specific purpose, datamarts allow a follow-up of a given theme, such as the follow-up of expenses (Damir), the analysis of medical cares provided by medical staff belonging to the liberal sector or provided by private institutions, the follow-up of medical devices, or even biological and pharmaceutical data. On another note, the SNIIRAM allowed to generate a general sample of beneficiaries (Échantillon Générale des Bénéficiaires – EGB) with up to 1 hundredth of the protected population²⁹, meaning 660 thousand people. This dataset was useful for longitudinal studies and analysis of the individual evolution of beneficiaries of health services in the city and at the hospital. In conclusion, the SNIIRAM constitutes a database of individual beneficiaries (DCIR³⁰) that raised an interest in conducting studies regarding the use of healthcare.

In a broad sense, the SNIIRAM includes data coming from other national databases, such as the “Programme de Médicalisation des Systèmes d’Information” (PMSI)³¹, or Medicalization Program of Information Systems in English. This national database regarding hospital activities was managed by the Technical Agency of Information on Hospitalization

²⁸ For more on this topic, see the SNIIRAM factsheet on the Health Insurance’s website, last updated on December 14, 2015: <http://www.ameli.fr/l-assurance-maladie/statistiques-et-publications/sniiram/structure-du-sniiram.php>.

²⁹ L. De Roquefeuil, A. Studer, A. Neumann, Y. Merlière explain that « the EGB is a representative sample of the beneficiaries whom are protected by the regimes of Health Insurance. Its survey ratio, around 1/100, allows to sample a sufficiently large population (around 500,000 people of the general regime) to answer the majority of the questions regarding the sanitary behavior of the population. Therefore, it is possible to study the amount that the patients need to take in charge; their consumption of healthcare services according to different criteria (age, gender, taking-in-charge by the ALD, affiliation to the CMU-C, etc.); to monitor a population who suffers from an ALD such as diabetes (13,000 persons, according to the EGB sample of 2007), grave chronic respiratory insufficiency (2,500 persons) or Alzheimer’s (2,000 persons). See L. De Roquefeuil, A. Studer, A. Neumann, Y. Merlière “L’échantillon généraliste de bénéficiaires : représentativité, portée et limites”, *Pratiques et Organisation des Soins* volume 40, n° 3, July - September 2009.

³⁰ This database is called DCIR for “*Datamart Consommation Inter Régimes*”.

³¹ The PMSI allows the healthcare institutions to dispose of quantified and standardized information on their activity as a form of measuring their medical production. For more on the PMSI, see M. Morkos “Le PMSI, Qu’est-ce que c’est ?”, *Hospitalia*, n° 8, October 2009 ; J. Raymond, “Des balbutiements à aujourd’hui. L’histoire du PMSI”, *Hospitalia*, n° 8, October, 2009.

(Agence Technique de l'Information sur l'Hospitalisation – ATIH)³². Thus, the PMSI and the SNIIRAM were two different databases. However, as of 2007³³, the PMSI database provided the SNIIRAM with a copy of the medical and administrative information it gathers³⁴ regarding hospital stays.

Furthermore, the extended version of the SNIIRAM also partially includes several data regarding decease, such as the data on vital status of persons or on their date of decease. This information is gathered in the National Repertoire of Identification of Private Persons (Répertoire National d'Identification des Personnes Physiques – RNIPP) and in the National System of Identity Management (Système National de gestion des Identités – SNGI), managed respectively by the INSEE³⁵ and the CNAV³⁶.

With the extended SNIIRAM, France had one of the biggest medical-administrative databases in the world. In this regard, a study of impact made in 2014 for the Health Bill emphasized that there are similar databases abroad (General Practice Research Database³⁷ in the United Kingdom and its 4 million files; the bases of Medicare, of the insurance companies and of Veterans in the United States). Although some of these databases are even more precise and exhaustive, since they contain information on the results of medical examinations, of medical diagnostics, or even of risks factors such as alcohol or tobacco consumption, body mass; none of these databases detain “as much medical information interrelated on such vast population³⁸” as the extended SNIIRAM. This exhaustive exposure of the population, the quality of the data contained, the chronological precision of the

³² Created in 2000, after the merger of the Pole of Expertise and Reference on National Health Nomenclature (Pernns), the Center of PMSI Information Processing (CTIP) and the PMSI Mission of the Health Ministry; the Technical Agency of Hospitalization Information (ATIH) is a public institution of the State, of administrative nature, which collects, hosts and analyses data from Health Institutions, but also generates technical measures for the funding of the institutions, conducts studies on the costs of the establishments, and even devises and maintains Health nomenclatures. See <http://www.atih.sante.fr/l-atih/presentation>.

³³ P.-L. Bras, with help of A. Loth, *Rapport sur la gouvernance et l'utilisation des données de Santé*, September 2013.

³⁴ P.-L. Bras, *op. cit.*

³⁵ The “Institut National de la Statistique et des Études Économiques” (INSEE) is the French National Institute for Statistics and Economic Research.

³⁶ The “Caisse nationale d'assurance vieillesse” (CNAV) is the main National Old Age Pension Fund in France.

³⁷ <https://www.cprd.com/home/>.

³⁸ See Health Bill, *Impact Study*, October 14, 2014.

data and their inter-linkage constitute the advantages of the French database³⁹.

However, these French databases suffered from significant gaps. Particularly, their management was considered “deficient”. The number of actors (CNAMTS⁴⁰, COPIIR⁴¹, SNIIRAM^{42,43}, CNIL⁴⁴, Ministry of Social Security, Health Data Institute) intervening in the governance and management of the entirety of this database was very high, where no authority assumed a position of leadership.

To fill in this gap, the Law of January 26, 2016, created a “National Health Data System” (Système National des Données de Santé – SNDS), name which indicates that the new information system isn’t centered anymore on databases linked to health insurance. In fact, although the SNDS relies on pre-existing databases and systems (SNIIRAM⁴⁵, PMSI⁴⁶, data on the cause of decease⁴⁷) put together in a unique information system, it does engage as well other newly constituted databases (data from the medical

³⁹ Ibidem.

⁴⁰ The “Caisse Nationale de l’Assurance Maladie des Travailleurs Salariés” (CNAMTS) is the main National Health Salary Workers’ Health Insurance Fund in France.

⁴¹ The “Comité d’orientation et de pilotage de l’information interrégime” (COPIIR) is the steering committee of the “Système National d’Information Inter-régimes de l’Assurance Maladie” (SNIIRAM) which is the main database of individuals’ Health Data in France.

⁴² See above.

⁴³ When the SNIIRAM was created, the Social Security Budget Law for 1999 established that the three main regimes of mandatory health insurance (General Regime, MSA and RSI) should jointly define by protocol the modalities of management and information gathering of this Information System. The Ministry of Social Security should approve the protocol through a decision, after recommendation from the CNIL.

An Inter-Regime Information Orientation and Management Committee (COPIIR) was created to allow the management of the SNIIRAM. The COPIIR defines by protocol the forms of management and intelligence of the SNIIRAM. For this purpose, it defines, particularly, the list of institutions authorized to use the data from the SNIIRAM and indicates the data that they can use. Managed by the General Director of the CNAMTS, the COPIIR is composed by three categories of agents, where each one disposes of a third of the voting rights (the three main regimes of mandatory health insurance, the State and the representatives of health professionals).

⁴⁴ The “Commission Nationale de l’Informatique et des Libertés” (CNIL) is the French National Commission for Data Protection and Liberties.

⁴⁵ Data mentioned on Article L. 161-28-1 of the Social Security Code.

⁴⁶ Data mentioned on Article 6113-7 of the Public Health Code.

⁴⁷ Data mentioned on Article 2223-42 of the General Code of Territorial Communities.

and social sector⁴⁸, which is a representative sample of complementary health insurance refund data⁴⁹)⁵⁰.

Furthermore, it is important to emphasize that the National System of Health Data pursues the purpose of making available data that can be applied to the achievement of six objectives: 1) inform the public about healthcare, medical-social taking-in-charge and its quality; 2) define, implement and evaluate health and social protection policies; 3) study expenses on health, health insurance and medical and social expenses; 4) provide information to health or medical and social professionals, structures and establishments regarding their activities; 5) guarantee the sanitary surveillance, guard and security; 6) contribute to research, studies, evaluation and innovation in the domains of health and medical-social taking-in-charge⁵¹. These six objectives are also the purposes of data processing permitted by the legislator.⁵²

Finally, although the governance of this new system is entrusted to the new National Health Data Institute (Institut National des Données de Santé – INDS), gathering all stakeholders⁵³ in a group of public interest and equally in charge of guarding the quality of health data⁵⁴, the CNAMTS⁵⁵ stays essentially in charge of the management of the new information system. The National Fund of Health Insurance has received, due to this, the attribution of responsible for data processing of the SNDS⁵⁶. Therefore, the objective of de-complexification of the old procedure, pursued by the Law of January 26, 2016, isn't totally reached: the new law conserves one

⁴⁸ Article L. 247-2 of Family and Social Action Code determines that “the department homes of handicapped people should use a common information system, which should be interoperable with those of the departments, of the National Funds of Family Allocations, and of the National Fund for Scholarship for Autonomy; according to the conditions defined by decree.”

⁴⁹ See Paragraph 5 of Article 1461-1 of the Public Health Code.

⁵⁰ The list of data that the National Health Data System gathers and makes available is mentioned in Section I of Article 1461-1 of the Public Health Code.

⁵¹ See Section III of Article 1461-1 of the Public Health Code.

⁵² See Section III of Article 1461-1 of the Public Health Code.

⁵³ Namely, the State, the institutions that represent the ill and the users of the healthcare system, the health data producers and the public and private users of health data (including health research institutions). See Article 1462-1 of the Public Health Code.

⁵⁴ Article 193 of Law No. 2016-41 of January 26, 2016.

⁵⁵ *La Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS), or in English, the French National Health Insurance Fund for Employees.*

⁵⁶ See Section II of Article 1461-1 of the Public Health Code.

part of the former complexity because the governance is entrusted to the National Health Data Institute, when the technical management lies essentially with the CNAMTS, when it could have been possible to entrust everything to the newly formed grouping of public interest.

2. The Reform of the Health Databases Access Procedures

The creation of a new national health database to allow a better management of information in the domain isn't the only gap the legislator has sought to fill in 2016. It has also sought to reform the procedures of access to the Database on Health Data, where the datasets have been considered, in the former statute, as too numerous and complex, but still "indistinct and disputable"⁵⁷. In fact, "some provisions [can] appear to be protective; others, on the contrary, [seem to] create excessive obstacles to the need for research and public information; and others [mostly exist for] a logic of reciprocity between the bodies involved or of distrust towards the improper use that could be made of the data"⁵⁸.

Furthermore, these access procedures to the SNIIRAM database did not allow a clear distinction between "the anonymous data that should be of free access, and the personal data that should be regulated"⁵⁹ and the multitude of access circuits that made researchers' access "too difficult and sometimes not sufficiently regulated"⁶⁰. This conception isn't in accordance any more with France's will of promoting the opening of its health databases, which intends to be done while protecting the rights of the beneficiaries of health services.

Regarding the anonymization of data, the Law of January 26, 2016, evolves by strengthening healthcare beneficiaries' rights. In fact, the legislator has expressly established, from the start, that "the data received and processed by the National Inter-Regimes Information System on Health Insurance should preserve the anonymity of the persons who benefit from healthcare service"^{61,62}. The Law of January 26, 2016, also indicates, however,

⁵⁷ See P.-L. Bras, with the help of A. Loth, *Rapport sur la gouvernance et l'utilisation des données de Santé*, September 2013.

⁵⁸ See P.-L. Bras, with the help of A. Loth, *Rapport sur la gouvernance et l'utilisation des données de Santé*, September 2013.

⁵⁹ See Health Bill, Impact Study, October 14, 2014.

⁶⁰ Ibidem.

⁶¹ See Article L. 161-28-1 of the Social Security Code in the version created by Article 21 of

that “the data received and processed by the National Inter-Regime Information System of Health Insurances preserves the privacy of the persons that have received healthcare services”⁶³. In other words, the legislator does not establish anymore one single obligation of anonymity, but instead the obligation of preserving privacy. This evolution implicates a number of measures aiming at the regulation of the usage of data from the SNDS. Therefore, the processing of data from the SNDS should henceforth be authorized by the National Commission for Data Protection and Liberties (Commission Nationale de l’Informatique et des Libertés – CNIL). Likewise, the Law of January 26, 2016, limits the storage of personal data in the National Health Database to the maximal period of twenty years⁶⁴.

The legislator has also intended to protect ill patients from any data access that could harm them. In this regard, the Law of January 26, 2016, establishes that from now, the SNDS should be used to take decisions regarding private persons⁶⁵. The regulation of the SNDS data usage also imposes to the profit-based private entities the obligation to resort to independent laboratories to perform studies that use the SNDS⁶⁶. Likewise, the Law of January 26, 2016, forbids the processing of SNDS data that aims at promoting certain health or sanitary products⁶⁷ among health professionals or health institutions; or that intends to remove certain guarantees from health insurance contracts or that could result in a modification of the membership contribution or insurance premiums of an individual or group of individuals presenting the same risk⁶⁸.

Other measures serve to protect personal data and to better secure their processing.

Law No. 98-1194 of December 23, 1998.

⁶² The forms of exercising anonymity at the SNIIRAM are defined in Article 5 do the Decision of July 19, 2013, regarding the implementation of the National Inter-Regimes Information System on Health Insurance.

⁶³ See Article L. 161-28-1 of the Social Security Code in the version modified by Article 193 of Law No. 2016-41 of January 26, 2016.

⁶⁴ See Paragraph 4 of Section IV of Article L. 1461-1 of the Public Health Code.

⁶⁵ See Paragraph 1 do Section IV of Article 1461-1 of the Public Health Code.

⁶⁶ See Section II of Article L. 1461-3 of the Public Health Code. On this topic, see the paragraph defining the specific regime applicable to the professionals who produce and commercialize certain sanitary or cosmetic products to insurance intermediaries or credit institutions, insurance or re-insurance institutions, mutual or pension institutions.

⁶⁷ The full list is stated at Section II of Article L. 5311-1 of the Public Health Code. See *infra*.

⁶⁸ See Section V of Article L. 1461-1 of the Public Health Code.

Amongst these measures, it is important to note in first place those that guarantee the anonymization of data. On this topic, one must indicate that data stored in the SNDS never is linked to identifying information, such as name, registration number (such as the NIR⁶⁹ or the social security number), etc. In fact, the SNDS does not contain the names or surnames of people, nor does it contain their NIRs or address. Furthermore, the file allowing the storage and management of the health professional registration numbers is separated from other data of the SNDS⁷⁰. The Health Law of 2016 has therefore implemented a system of “separate identity management” such as set out in the European Regulation of Personal Data Protection⁷¹. In fact, the legislator has decided to entrust a distinct body, separated from the “National Health Data System” (Système National des Données de Santé – SNDS) and those in charge of data processing, the responsibility of the personal data that present a risk of direct identification. The list of data that presents such characteristics is defined by a decree from the Council of State (Conseil d’État) after a recommendation from the CNIL. The device that allows the reidentification of person from the SNDS database is entrusted solely to this agency, which is separated from those who are responsible for the SNDS and those responsible for data processing, guaranteeing its security⁷².

Although the legislator has intended to protect the privacy of the persons whose data is stored in the SNDS by implementing a “separate identity management” device, it has also established the possibility to obtain a person’s identity in two exceptional cases. Consequently, the CNIL can authorize the access to the identification data generated by this separate body, in one case, if the access to this data is necessary to protect the person from a grave danger she is exposed to or to participate in a research; or, in a second case, if the processing of this data is necessary, without alternative solution, for the realization of research, study or evaluation, provided the use of this data is proportionate to the expected results.

Secondly, the legislator has sought to guarantee the security, confidentiality and integrity of the data of the SNDS, and has likewise established the traceability of the access and other processings. In this regard, the Public

⁶⁹ The Numéro d’inscription au repertoire de l’INSEE (NIR) corresponds to the French National Health Insurance Number.

⁷⁰ See Section I of Article L. 1461-4 of the Public Health Code.

⁷¹ See Health Bill, Impact Study, October 14, 2014.

⁷² See Section II of Article L. 1461-4 of the Public Health Code.

Health Code establishes that “the access to this data is done in the conditions that guarantee the confidentiality and integrity of data and the traceability of access and other treatments, all of which must be in accordance to a referential defined by a decision of the ministers in charge of Health, Social Security and Technology, which will be taken after a recommendation from the National Commission for Data Protection and Liberties (Commission Nationale de l’Informatique et des Libertés – CNIL)⁷³.

The traceability of the access should strengthen the confidentiality of data from the SNDS by identifying the exact person authorized to process the data in the entities that benefit from permanent access, the accesses performed, their dates, and the information concerned.

Likewise, the confidentiality of health data is protected by the obligation of professional secret and should be respected by the persons that are authorized to access the SNDS. The persons who are in charge of personal data processing that violate the professional secret will incur the sanctions of article 226-13 of the Penal Code⁷⁴. This section establishes the imprisonment and a 15 000-euro fine for anyone who reveals a secret information for which he/she is a depositary.⁷⁵

However, the Health Law of 2016 hasn’t only strengthened the protection of its healthcare beneficiaries’ privacy, but has also created in the Public Health Code a new section which defines the forms of access to health data⁷⁶.

The Health Law of 2016 organizes the access to database on two different channels, depending on the type of data, to better guarantee their protection.

The first channel is the most open. It concerns the data that is not subject to direct or indirect identification. These datasets are accessible and reusable freely by all. Open data becomes, therefore, the standard for the non-identifiable datasets. This opening concerns also aggregate statistics, like datamarts⁷⁷, and the individual data that is rendered sufficiently imprecise to prevent the identification of a person after the deidentification

⁷³ See Paragraph 3 of Section IV of Article L. 1461-1 of the Public Health Code.

⁷⁴ See Paragraph 2 of Section IV of Article L. 161-1 of the Public Health Code.

⁷⁵ Article 226-13 of the Penal Code.

⁷⁶ See Article 193 of Law No. 2016-41 of January 26, 2016, on the Modernization of the French Health System, which creates Section VI in Book IV of the first part of the Public Health Code.

⁷⁷ See *supra*.

process. In fact, if the health data that figures in the SNDS are de-identified, it remains possible, sometimes, for those who detain supplementary information of the people concerned, to reidentify these people by crossing the de-identified data with the information they detain. These datasets that are potentially identifiable *a posteriori* are not included in the opening of data, the legislator has established that the reuse of data accessible and reusable by all “should not aim at or result in the identification of the people concerned by these data”⁷⁸.

The second channel is more restrictive, which makes sense, since it concerns health data that is potentially identifiable, despite the de-identification process they were submitted to. In fact, as explained above, some health data, although they do not carry names, surnames or social security number, can become identifying information *a posteriori* when the people who detain other information use it to violate the anonymization process, by crossing the de-identified information with the information they detain. The limit of access to the potentially identifiable information to expressly authorized persons is, therefore, a form of protecting people’s privacy. It is in this perspective that the French legislator has sought to restrict the access to potentially identifiable data, by determining the possibility of obtaining access only if intended to achieve one of the following purposes.

First, the potentially identifiable health data processing can be authorized by the CNIL, in accordance with Chapter IX of the Law n 78-17 of January 6, 1978, for the purposes of research, study or evaluation attending to one of the six objectives of National System of Health Data (SNDS)⁷⁹ and pursuing public interest. One supplementary requirement has been added to certain professional sectors for which there could be an interest to access the SNDS and to process potentially identifiable health data under the guise of conducting health research.

To limit these risks, sub-section V of article L. 1461-1 of the Public Health Code forbids the data processing of the National System of Health Data that pursues one of these two goals: 1) the promotion of certain products of sanitary or cosmetic purposes⁸⁰ towards health professionals or

⁷⁸ See, in this regard, Article L. 1461-2 of the Public Health Code.

⁷⁹ See *supra*.

⁸⁰ This concerns products destined to humans and of cosmetic purposes, as mentioned in Section II of Article L. 5311-1 of the Public Health Code, particularly: medications; contraceptive and contragestive products; biomaterials and medical devices; in vitro diagnostic medical devices; labile blood products; organs, tissues and cells prepared and conserved by

establishments; 2) the removal of guarantees from insurance contracts and the alteration of the membership contributions or insurance premiums of an individual or group of individuals that present the same risk⁸¹.

Furthermore, the Law of January 26, 2016, has regulated these forms of access to the SNDS⁸²: on one side, for the professionals that produce or commercialize certain products of sanitary or cosmetic purposes⁸³; on the other hand, for credit institutions, insurance or reinsurance bodies, mutual societies and pension funds⁸⁴, and insurance intermediaries⁸⁵. In order to have access to data of the SNDS for research purposes, these professionals must show that the forms of implementation of the data processing render impossible any type of use of data as described in section V of article L. 1461-1 of the Public Health Code, either by resorting to a research laboratory or to a studies office, both public or private⁸⁶.

Second, the authorization to process potentially identifiable health data can be consented, by decree from the Council of State after a recommendation from the CNIL, if the access to SNDS's personal data is strictly necessary for the performance of an objective of public service; nonetheless respecting rigorously the protection rules applicable to these sensitive data. The sole bodies that can be allowed to access the SNDS are State services, public institutions or bodies responsible for an objective of public service (indicated in a list established by the Council of State⁸⁷, mentioning the specific public bodies authorized to process data from the SNDS). This

human milk banks; products destined to the maintenance and application of contact lens; procedures and apparatus destined to the disinfection of the places and vehicles that receive infected people; non-corrective eye lens; cosmetic products; micro-organisms and toxins; tattooing products; software used by medical biology laboratories to manage exams or validate, interpret, communicate or archive results; devices that aren't strictly for medical purposes used in medical biology laboratories for the performance of medical biology exams; software that help prescriptions and software that help dispense.

See Article L. 5311-1 of the Public Health Code.

⁸¹ See Section V of Article L. 1461-1 of the Public Health Code.

⁸² See Article L. 1461-3 of the Public Health Code.

⁸³ Products mentioned in Section II of Article L. 5311-1 of the Public Health Code, see *supra*.

⁸⁴ This concerns institutions mentioned in Paragraph 1 of part A and Paragraph 1, 2, 3, 5, and 6 of part B of Section I of Article L. 612-2 of the Financial and Monetary Code.

⁸⁵ Professionals mentioned in Article L. 511-1 of the Insurance Code.

⁸⁶ See Section II of Article L. 1461-3 of the Public Health Code.

⁸⁷ See Article L. 1461-7 of the Public Health Code that determines the need for a decree from the Council of State, issued after a recommendation of the CNIL.

decree should indicate, for each service, institution or authorized body the extent of the authorization, the conditions of access to the data and the conditions of management of access.

In these two hypotheses, only persons specifically designated and authorized by the responsible for data processing will be able to access the data from the National Health Database, in accordance with the forms established by decree from the Council of State. This access to the SNDS and the matching with their own data will only be authorized for the cases where these actions are strictly necessary for research, study or evaluation purposes or for the accomplishment of a public service objective.

From the analysis of these elements, it seems that the Health Law of 2016 pushes for a significant evolution in terms of health data opening. However, it is important to keep in mind that the purpose of the opening of health data access constitutes a true challenge for the legislator and for the relevant actors in its implementation, especially from the perspective of the protection of personal data, privacy and respect to objectives of public service, which traditionally characterize the French system.

The Swedish Black Box. On the Principle of Public Access to Official Documents in Sweden

ANNA ROSENGREN

1. Introduction¹

The Swedish principle of public access to official documents has gained much well-deserved acclaim for its contribution to openness and democracy, notably by granting citizens insight into the decision-making process of politicians and public authorities². The Freedom of the Press Act – one of Sweden’s constitutional laws – contains the regulation of the principle, the origins of which may be traced to an ordinance from 1766.

The Freedom of the Press Act is described as the very first freedom of information (FOI) law in the world,³ and the long history of FOI has often been proposed as an important explanation of Sweden’s propensity towards openness.⁴ This openness is clearly detected in the current wordings of the Act which states that “[e]very Swedish citizen shall be entitled to have free access to official documents, in order to encourage the free exchange of opinion and the availability of comprehensive information”.⁵ Later, the Act states that “[a]n official document” “shall be made available” “at the place where it is held, and free of charge, to any person wishing to examine it”.⁶ The feature that everyone may take part of official documents is often referred to as the “principle of public access to official documents” (in Swedish, the considerably shorter “offentlighetsprincipen” is used), and is often referred to as a “cornerstone” of the Swedish democratic system.⁷

Swedish official documents are regarded as part of the archive of the public authority preserving the document, and as such are public in the absence of secrecy regulation.⁸ The Swedish Freedom of the Press Act functions in a way which is somewhat automatic,⁹ as the fulfilment of a number of criteria (that it is a “document” in the meaning of the law, that the document has been “received” or “drawn up” by a “public authority” and is “held” by the authority) renders a document “official” and part of the

archive.¹⁰ As previously mentioned, official documents may be protected by secrecy regulation for several reasons, but the “default” situation may nevertheless be expressed as openness.¹¹ In case of absence of secrecy regulation, if the secrecy period has been surpassed, or because of exceptions to the secrecy regulation, the Swedish Act may thus have considerable effect also on privacy, although this aspect has received considerably less attention than its importance for openness. Interestingly, a recent Swedish official government report has stressed the importance of “the right of personal integrity” as an “important factor also for other central [...] rights” “constituting the foundation in a democratic society”.¹²

The Swedish situation differs from countries where exceptions to the release of official documents are in vigour for reasons of privacy. One of the reasons to “refuse access to a document” is that the release might “undermine the protection of privacy”.¹³ As mentioned above, the Freedom of the Press Act is a constitutional law, which partly explains the situation in Sweden.¹⁴ Furthermore, legislation that has been added to the Act has led to a situation which, for instance, allows online publication of databases of personal data from official documents, including publication of sensitive personal data. A well-known example is the commercial database Lexbase which contains official documents in the form of “[a]ll the judgements from all courts of first instance in the entire country”.¹⁵ A combination of laws contribute to the situation: the Freedom of the Press Act makes it possible for the company to retrieve documents having the status “official”, exceptions to the Swedish interpretation of the EU directive on the protection of personal data explains why the EU directive is not applicable, and a constitutional law permitting the publication of databases on the internet provides the possibility for online publication.¹⁶

The benefits that the Swedish principle of access allows for in terms of openness, may thus have drawbacks for privacy. It may, therefore, be said that the principle is contributing to democracy through openness, at the same time as it may have detrimental effects on democracy through negative effects on privacy. This makes the workings of the principle of public access into a research topic of great interest.

In relation to archival science, various models have been used to describe the creation of documents and their subsequent evolution. The life cycle perspective and the Records Continuum Model (RCM) are two models that are often mentioned in this respect. The life cycle perspective is described as a linear process with a clear distinction between an active phase for “records”, and an inactive phase for “archival documents”. The RCM, on

the other hand, is often used to describe a process which is more fluid and where records may have not only one, but several active phases as they are used for different purposes. Some researchers argue that the life cycle perspective describes the process relating to official documents in Sweden, others that the RCM bears strong resemblance with the Swedish situation. In this study, researchers' arguments concerning the two models are presented, and in addition the analysis is deepened for certain aspects of the models. The in-depth analysis, in turn, indicates that neither model is entirely applicable to the Swedish case. Instead, concepts from black box theory are proposed to shed light over the Swedish principle of public access to official documents.

The argument for introducing black box theory is linked to the fact that the literature on the Swedish principle of public access suggests several factors which may affect the creation and release of official documents, making it difficult to predict the total amount of accessible documents at a specific point in time. The Swedish system therefore seems to bear resemblance with black box theory, which stipulates that knowledge about a (non-observable) system may be obtained by analysing the relation between input brought to the system, and the corresponding output emanating from the system.

2. Purpose and outline

The purpose of the study is to deepen our understanding of the Swedish principle of public access to official documents by introducing elements from black box theory into a model, here called The Swedish Black Box, and to test the applicability of the model by comparing two situations describing how school children handed in their texts to teachers in 2003 and 2016.

The article is outlined as follows. As an introduction, a short note is made regarding "models" in general, and how they are treated in this article. In the section Life cycle perspective next, the theoretical foundation of the life cycle perspective is presented, together with arguments from researchers on why the perspective is suitable to describe the Swedish situation. A similar presentation is then dedicated to the RCM in The Records Continuum Model: after a description of the RCM in theory, arguments from researchers are brought forward on the issue of why the model fits the Swedish case. Thereafter, a more in-depth comparison between the models and the Swedish case is made, based on the analysis of literature from previous research. From this comparison, it seems that neither model is

entirely suitable to describe the Swedish situation. Rather, from the analysis of the research literature, it appears that the Swedish principle of access to official documents contains features which suggest similarities with black box theory, which is therefore presented in the next section Towards a new model: introducing black box theory. Features of the Swedish principle of access, as indicated in the literature, are then added to the theory, creating a model which is called the Swedish Black Box. The model is suggested as a means to deepen our understanding of the Swedish principle of access, and in the next section⁴. The Swedish black box – testing the model, two official government reports on the same topic – access to official documents in primary schools containing personal information about children – from two different points in time, 2003 and 2016, are used to test the Swedish Black Box.

3. In Pursuit of a Suitable Model

An important note to be made here, is that “models” in this article are used as metaphors, as figures of thought. Rather than trying to regard the life cycle perspective, the RCM and black box theory as analytical frameworks used to convey how things actually work, they are used as figures of thought to shed light on a complex situation. This is much in line with how Glenn Dingwall describes the life cycle perspective as a metaphor.¹⁷ Similarly, Frank Upward, archival scientist instrumental in developing the RCM, stresses the need for “modelling complexity”.¹⁸ As outlined above, the purpose of the article is to deepen our understanding of the Swedish principle of public access to official documents. The Swedish principle of public access is thus the (complex) object of analysis, and in the article, different models are used with the aim of shedding new light on this phenomenon.

Life cycle perspective

According to the life cycle perspective, a document follows a linear process containing a number of separate and sequential stages from its creation to disposal or preservation.¹⁹ The origin of the perspective is often traced to the seminal work of American archival theorist Theodor Schellenberg, *Modern archives*. According to this work, two major phases are discernible: record and archive. The initial phase starts with the creation of records “in pursuance of its [the public authority’s] legal obligations or about the transaction of its proper business”. The purposes behind the creation of records are

described as serving as evidence and as being of informational value.²⁰ The second phase is reached by those records deemed “worthy of permanent preservation for reference and research purposes” after an appraisal process.²¹ Finding ways to dispose of paper documents was a critical task due to the strong growth of paper documents in the beginning of the 20th century, and retention periods were established for various types of institutions and records in accordance with “[b]usiness needs and financial and legal obligations”.²² Linked to the status record is the term “primary value”, which tells something about the importance of the record in the eye of the creator. In the same way, the “secondary value” is linked to the archive status and refers to research, or more generally, to “values to other agencies and to non-government users”.²³

The life cycle perspective may thus be described as linear and consisting of distinguishable stages occurring in chronological order. Is this a proper way of describing the Swedish case? In his article from 2007, information systems scientist Erik Borglund proposes that Swedish public archives are characterised primarily by the life cycle perspective.²⁴ He argues that the perspective is relevant in the case of paper documents, as he sees that such documents follow an “administrative process”, as they are moved to archives that are gradually more remote from the persons that handled them originally.²⁵ Archives and information scientist Proscovia Svård arrives at the same conclusion in an article from 2013. Based on an empirical investigation of two Swedish municipalities, her study showed that the organisation at the municipalities was divided into active records management carried out by registrars on the one hand, and the municipal central archives on the other.²⁶ The organisation thus place “the archivists at the end of the information/records management process”, despite the absence of a distinction between records and archives in Sweden.²⁷

The Records Continuum Model

As outlined above, researchers have concluded that the situation in Sweden may be seen in terms of the life cycle perspective regarding the division of duties between registrars and archivists. The argument has also been raised, however, that the absence of a distinction between records and archival documents in Sweden would render the Records Continuum Model (RCM) a more proper description of the Swedish situation.²⁸ The RCM will now be presented in more detail and compared to the life cycle perspective.

With the arrival of computers and electronic data, it became apparent that the stages of the life cycle perspective were increasingly difficult to separate.²⁹ What, then, characterises the RCM? According to archival scientist Sue McKemmish, “[c]ontinuum ideas [...] challenge traditional understanding which differentiate between ‘archives’ and ‘records’ on the basis of selection for permanent preservation in archival custody, and which focus on their fixed nature”.³⁰ In opposition to the “separate dimensions of space and time” of earlier models,³¹ continuum thinking stresses the accessibility of records, rather than their fixedness in space.³² Instead, the continuum thinking sees a record as ‘always in a process of becoming’, as new contexts may provide new meanings to it.³³ In the model as it was presented by Frank Upward, the ever increasing distancing in time and space of a record from its original context constitutes a core element.³⁴

The RCM is described as consisting of four interrelated dimensions: create, capture, organise, pluralise.³⁵ The first dimension, create, is the “locus” where all “the business of action (all action) happens”,³⁶ the “business activities that generate the records”.³⁷ This point (in space and time) is thus the origin from which a record will be further distanced in “space-time”.³⁸ The second dimension, capture, is described as a situation in which “all the elements required for robustness are present” and explicit.³⁹ Organise, the third dimension, “relates to documents and records (including records in a database sense) being organized so that others not directly involved in specific business and social processes, [...] can access and use what has been created and captured”.⁴⁰ The fourth and last dimension, pluralise, continues the distancing in time and place from the original creation of a record. In this fourth dimension, information “forms societal totalities”, and “involves the use of information in ways which are less predictable or controllable”.⁴¹ As a parallel to the evidential and informational values that a record could serve in the life cycle perspective, the RCM is described as bringing the evidentiary, transactional and contextual nature of records into the foreground.⁴² In addition, Frank Upward speaks of identity, referring to the “authorities by which records are made and kept”, and recordkeeping containers which constitute the objects created to store records.⁴³

The static division into current records and historic archival documents of the life cycle perspective is thus replaced in the RCM by a view of records as constantly evolving and possible to access by increasingly larger audiences, and for new purposes. Is this a situation which correctly describes the situation in Sweden? Researchers have argued that Sweden follows the RCM

as no distinction is made in Swedish legislation between current and historical documents, between records and archival documents.⁴⁴ This is a valid argument, as a document becomes official "as soon as it is created, i.e. prepared according to certain criteria or received and held by a public authority".⁴⁵ A transfer to the archive is thus not necessary to render a document official in Sweden, and the absence of a division between current records and historical archival documents is therefore a characteristic shared by the RCM and the Swedish model. Another similarity pointed out by Proscovia Svård deals with the possibility to use the same records many times and for new and changing purposes. In Sweden, this is the way that public records should be viewed according to the Swedish E-Delegation, in charge of promoting e-government development.⁴⁶ In other words, public records should be regarded as a "national resource", and as such should be used and re-used in different contexts and by "different stakeholders".⁴⁷ The possibility of re-using public records is thus a feature of the RCM which is recognizable in Sweden.

Comparisons with the situation in Sweden

As we saw above, similarities have been identified between the life cycle perspective and the situation in Sweden in terms of the division of duties between registrars and archivists. On the other hand, the absence of a distinction between current records and historical archival documents has been identified as a characteristic shared by the RCM and the Swedish case. In this section, the life cycle perspective and the RCM will be compared in more detail with the situation in Sweden. As for the life cycle perspective, focus will be placed on two parameters present in both the life cycle perspective and the Swedish case: amount of documents and time. Regarding the RCM, the creator and genre of documents as well as the role of records and unit of analysis, have emerged as interesting areas of comparison.

Comparing the life cycle perspective to the Swedish case

The parameters "amount of official documents" and "accessibility in time" regarding the life cycle perspective and the Swedish case will thus be the topic here. As previously indicated, records are created within public authorities, according to the life cycle perspective. During this phase as records, the public has no access to them, in general. In the graph to the left below, this phase is indicated by the box with a thick border. The second phase – which may take place years or decades after the creation of the

record⁴⁸ – is initiated through an appraisal process. The appraisal results in the destruction of the record, or the transfer to the archive. For those documents that are transferred to the archive, the archival documents are “being made accessible”⁴⁹ to the public in the absence of secrecy regulation. After the initial phase as records, a box with less height represents this smaller amount of archival documents. The second phase with archival documents is furthermore represented by a thin border which symbolises that the public has access to them in the absence of secrecy regulation.

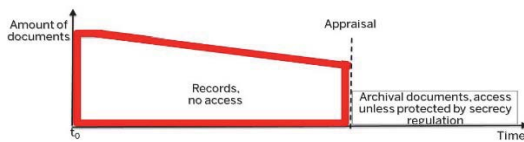


Figure 1: The Life Cycle Perspective

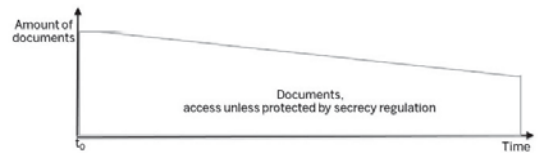


Figure 2: The Swedish Principle of Public Access to Official Documents

The visual representation of the principle of public access to official documents in Sweden, in the graph to the right, contains both similarities and differences compared to the life cycle perspective. In both the life cycle perspective and the Swedish case, legislation grants that documents may be disposed of. In Sweden, all official documents will thus not be preserved forever, but may be disposed of after a specified length of time has passed.⁵⁰ The slope in the two graphs thus represent the decreasing number of documents, as compared to the number at t_0 .

The two graphs also show two striking differences. Firstly, the Swedish case in the graph to the right has no initial records phase. As previously mentioned, Swedish documents that fulfil a number of criteria are part of the archive.⁵¹ Instead of two separate phases, the situation in Sweden is thus represented by just one box of archival documents. Secondly, a consequence of the existence of just one box with archival documents, is the possibility that a large number of documents may be immediately accessible in the absence of secrecy regulation in Sweden,⁵² as compared to the life cycle perspective. In the illustration to the right, this is represented by the one box having a thin border.

Comparison between Sweden and the RCM

Differences between the life cycle perspective and the Swedish principle of public access to official documents thus appear in terms of the amount of documents accessible to the public in the absence of secrecy regulation, and the time at which this may occur. Turning now to the RCM, it is possible to discern several areas containing differences between the RCM and the Swedish situation: regarding agency of the creator and genre of documents, role of records and unit of analysis.

Agency of the creator and genre of documents

As we saw above, the RCM indicates that documents emanate from the “particular activities” of individuals or from “business activities”, and that it focuses on “the importance of individual actions”. It has furthermore been pointed out that the RCM refers to a certain “genre of documents”, “privileging the creation of specific types of documents”.⁵³ In a similar vein, we saw above how identity was described as a role which “relates to the authorities by which records are made and kept”.⁵⁴ A characteristic in these examples of the RCM is thus related to the agency of the creator, and to a specific range of documents “made and kept” by it. In Sweden, the agency of the creator just as well as the range of documents may be less distinct than in the examples above, however. Examples from the literature may demonstrate this. Kallberg suggests that “it is the legislation [...] that stipulates what records are needed to fulfil the legislative requirements”.⁵⁵ In this case, national legislation would thus constitute the factor which ultimately determines what records are produced, rather than the agency of the creator. A somewhat different suggestion is made by Proscovia Svärd. She describes how public authorities engage in a “vast number of complex processes”, “resulting in enormous amounts of records which are public”.⁵⁶ In this description, the processes and activities in which the organisation might engage do not appear entirely distinct or easily predictable, and the ultimate factor giving rise to official documents may be described as resulting from changes in these complex processes and activities. Returning to Kallberg, the view that legislation determines what documents are created is supplemented by another suggestion later in the thesis. Kallberg states that it is:

questionable if the top management at the municipalities and the politicians have enough knowledge of the definitions of official documents and the fact that the format is unimportant for the management according to the legislation.

There seemed to be no awareness that documents created within business systems have equal legal status as documents created in electronic document and records systems.⁵⁷

In the quotation, Kallberg refers to the "definitions" which determine whether a document is "official" or not. She points to the fact that management at times seems unaware of the definition and its consequences, e.g. that official documents may arise in any format and in any system. The factor behind the creation of documents in this example is thus the criteria in the Freedom of the Press Act. From the example, we may also conclude that the introduction of new systems, such as the business systems mentioned in the quotation, may give rise to new official documents. Technological development implemented by public authorities is therefore also to be regarded as a factor that might affect the creation of documents.⁵⁸ Kallberg points at yet another way of creating official documents, as she stresses that it is important that the staff at public authorities understand "the purposes of why and how the information is captured before it is even seen as a record".⁵⁹ It would thus appear that changes in the routines of the public authorities might lead to the creation of new official documents, a fact which Kallberg cautions the public authorities to consider beforehand.

Summing up, the literature on the RCM in a Swedish context has identified how changes in several different factors might have a potential impact on the creation of official documents. The factors identified here are legislation, processes and activities, criteria, technology and routines. In relation to the more theoretical texts on the RCM, according to which the authority/creator makes the records, the process behind the creation of documents in Sweden seems less distinct and predictable due to the large number of factors which may have an impact on the creation of new official documents.⁶⁰ The observation made by Kallberg that "exploring the beginning of the life of a record is essential [...]", thus seems very much to the point.⁶¹

Role of records and societal level

Related to the topic of creator and genre of documents is the aspect of the various roles – often described as evidentiary, transactional and contextual – that records may serve. As pointed out by Erik Borglund, Swedish legislation does not demand that documents are of evidential or transactional purposes.⁶² Certainly, Swedish official documents will often serve e.g. evi-

dential purposes, but this is no legal requirement.⁶³ Regarding the role or purpose, the RCM is thus not entirely applicable to the Swedish case, according to Borglund. Regarding the focus of the RCM on society at large, finally, we may conclude that it draws on the structuration theory of Anthony Giddens.⁶⁴ In turn, this theory focuses on structures in society on a general level,⁶⁵ making the RCM primarily oriented towards how “record-keeping processes create and reconstitute collective structures”.⁶⁶ The societal focus was a limitation of the RCM according to Huvila et al., whose research area is personal information creating and reconstituting “the individual self”,⁶⁷ rather than the society. A point to be made here is that it is possible to reconstitute not only society but also the “the individual self” from the Swedish principle of public access. The Freedom of the Press Act makes no distinction between official documents such as protocols from public authorities, and official documents containing data on individuals. As official documents are immediately accessible to everyone unless protected by secrecy regulation, we may deduce that they may be used to reconstitute not only society, but individuals as well.

Summary and discussion

We have seen above that the Swedish model creates many official – and thus accessible, unless protected by secrecy regulation – documents in a way which may be hard to predict. In comparison with the life cycle perspective, the Swedish model has a way of creating official documents which is more “automatic” and may grant access at an earlier point in time. As for the comparison with the RCM, the literature suggested that both the agency of the public authority and the role or purpose of records are less pronounced in the Swedish system. It was also indicated that the focus on societal structures of the RCM contrasts with the Swedish model which would, it seems, also allow for the reconstitution of individual selves. More specifically, the literature indicated that a number of changes in factors might affect the creation and release of official documents, the identified factors being legislation, processes and activities, criteria in the Freedom of the Press Act, technology and routines.

It would thus appear that the Swedish model contains many official documents, and that it is difficult to predict how they arise, and their quantity at any given moment. This indicates similarities with the black box theory which stipulates that knowledge about a (non-observable) system may be obtained by analysing the relation between input (stimulus) brought

to the system, and the corresponding output emanating from the system. A more detailed description of the theory is presented next.

Towards a new model: introducing black box theory

Black box theory is part of the open system theory, which stipulates that a system interacts with its environment through information, material or social transfers.⁶⁸ A system, in turn, consists of “complexes of elements standing in interaction”.⁶⁹ A basic assumption of the black box theory is that the functions of the system under scrutiny cannot be (fully) investigated by the observer. Therefore, the system is often referred to as a “black box”.

Knowledge about the system is drawn solely from the conclusions that the observer may draw about the “behavior of the system” derived from the repeated reactions of various stimuli.⁷⁰ The way an observer may get information about the system is explained in general terms in the following way:

The child who tries to open a door has to manipulate the handle (the input) so as to produce the desired movement at the latch (the output); and he has to learn how to control the one by the other without being able to see the internal mechanism that links them. In our daily lives we are confronted at every turn with systems whose internal mechanisms are not fully open to inspection, and which must be treated by the methods appropriate to the Black Box.⁷¹

A system is not necessarily static, however. Open systems theory often deals with so-called steady states, but the human body, for instance, undergoes changes from “embryonic development, growth, aging, death”.⁷² Various external factors may therefore affect the system so that its functions will vary over time.

Combining the basic concepts regarding the black box theory on the one hand, with the information from previous research about factors that may affect the creation and release of official documents on the other, we have the possibility to describe the Swedish model visually as in the graph below. The combination of the black box theory and the information on changes of factors is here called the Swedish Black Box, and is a model which may help us get a better understanding of the Swedish principle of public access to official documents. The model describes the Swedish principle of public access as an open system which interacts with its surroundings in various ways. By way of example, citizens send in their annual tax declarations (“input”) to public authorities that will hold the tax declarations as official

documents in the system. The tax declaration will be provided as output from the system if a person requests it while held by the public authority, under the condition that the declaration is not subject to secrecy regulation.⁷³

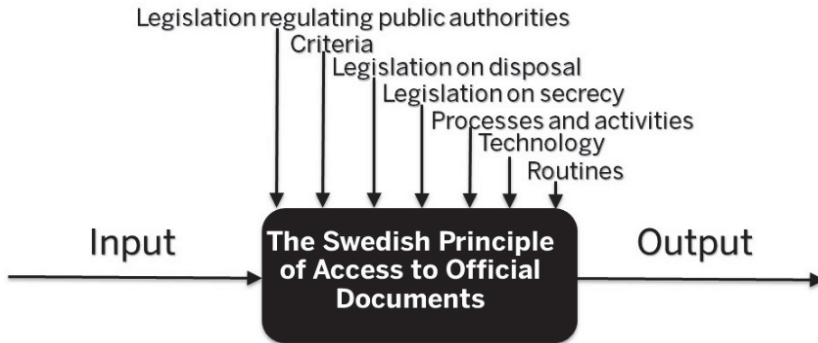


Figure 3: The Swedish Black Box

As suggested by the literature, the system is affected by several external factors. One such factor is the legislation regulating the activities of the public authorities. Other factors are processes and activities of the public authorities, the criteria of the Freedom of the Press Act, technology and routines of the authorities. To this may be added legislation on disposal of official documents discussed earlier, as well as extensive Swedish legislation limiting the access of official documents. In the graph above, factors related to legislation have been grouped together (legislation regulating public authorities, criteria, legislation on disposal, and legislation on secrecy). Thereafter the remaining factors – processes and activities, technology and routines – have been added. Given the large number of factors which may affect the “system”, it is likely that it will appear complex and hard to predict for the citizen.

4. The Swedish black box – testing the model

To test the applicability of the Swedish Black Box, the source material official government reports (government reports) was chosen. Sweden has a long parliamentary tradition of using government reports as a way of ensuring broad support for current issues and their proposed solutions.⁷⁴ It might be argued that the legal language in government reports has attracted

less attention by researchers than, for instance, laws and ‘the written legal text proper’.⁷⁵ The reports are often written jointly by several different politicians and experts, and so present a large number of arguments and counter arguments. Furthermore, they may contain drafts of subsequently introduced (or rejected) legislation. In summary, government reports constitute a rich source to analyse to better understand important societal issues at the time of writing.

Two government reports from 2003 and 2016 treating the topic of personal information for school children were chosen. An important reason for choosing this topic is found in the second report which states that “[c]hildren must be considered especially important to protect against improper infringement of their personal integrity [...]”.⁷⁶ The authors speak of “digital tattoos” of personal information that may follow the children throughout their whole lives, preventing the children from making a fresh start when changing schools, for instance.⁷⁷ Given the importance of protecting children, analysing to what extent the Swedish principle of public access to official documents allows access to personal information on children is therefore of great interest.

An important aim of the first report, *Secrecy in the interest of the pupils*, published in 2003, was to identify the existence of official documents in public schools, and to assess whether such documents were freely accessible or protected by secrecy regulation.⁷⁸ The report discussed these issues for documents drawn up by schools in relation to the care of school children (“elevvård”), in relation to education performed by the schools, for documentation to and from the school (“skriftväxling”), as well as for “other documents”.⁷⁹ In this last section, we find the topic of special interest to this study: documents prepared by school children as part of their education. The second report from 2016, *What about the personal integrity?*⁸⁰ had a much broader scope and did not exclusively cover the educational system. Its focus was the recent technological development and the risks it entails for personal integrity in different areas. The report follows the same structure for all areas: identification of elements which might entail risks for personal integrity, the legislation in place to protect personal integrity, and the overall assessment of the authors on the remaining risk for the personal integrity.⁸¹ Schools constitute the first area to be analysed.⁸² Other reports would also have been possible to choose. In particular, the government report from 2007, *The protection of the personal integrity should be mentioned*, as well as a report from 2011, *The documents of the school*,⁸³ which deal with similar issues. Choosing the 2003 and 2016 publications

means that thirteen years will have elapsed between the two reports, a period which is characterised by rapid technological development, among other things. It is likely, therefore, that one or more changes in the factors suggested in the literature will be possible to identify, and this is the reason the 2003 and 2016 reports were selected.

For both government reports, the analysis is made applying the same case. It is a type of case which occurs on a very regular basis in primary education: texts being handed in by children to the teacher for assessment. In this way, school children provide input to the “system” by handing in their texts, and we may ask if the 2003 and 2016 reports discuss whether such documents may also be retrieved from the system, thereby providing output. When comparing the government reports, published thirteen years apart, will we be able to identify any of the external factors above as having undergone changes, thereby having had an impact on the system?

Before turning to the analysis of the first report, it is worthwhile mentioning that the Swedish principle of public access to official documents is applicable only to schools that are considered public authorities, and does not apply to private schools.⁸⁴ The 2003 report clearly states that the task of the authors excluded private schools.⁸⁵ This was not the case in the 2016 report.

The 2003 report

As an initial observation, the authors of the 2003 report conclude that Swedish regulation on primary education contains few explicit demands related to documentation. Schools are obliged to make assessments in writing about children that do not reach the goals, and to report grades.⁸⁶ In addition to the legally required documentation, the authors describe that teachers often make notes regarding the progress of the children, and that such notes are official documents.⁸⁷ In the case of making notes, processes and activities or routines of the schools, rather than, for instance, legislation, seem to be the external factors creating official documents. This seems to be the case also for the written texts that children hand to their teachers for assessment. On this issue, the authors write:

Under shorter or longer periods of time, schools will often hold written material that has been drawn up by the pupils as part of their school tasks. /.../ The material will often be returned to the pupils after an assessment of the result has been carried out, but during the period it is in the care of the teacher [...] the material must be regarded as being held by the school in the sense which is indicated in 2 ch. 3 sentence the Freedom of the Press Act. Documents that are

held by a school are official there, if they may be regarded as drawn up or received by the public authority.⁸⁸

The quotation above indicates that the authors explicitly discuss the various criteria in detail. In the opinion of the authors, the texts handed in by the school children are to be interpreted as “received by” the public authority, and as long as the texts are also held by the authority they are official documents that may be “released to any person requesting them”.⁸⁹ Once the assessment is made by the teacher, the texts are normally “handed back to the pupils”.⁹⁰ From the description we may conclude that once the text has been returned to the child, the document is no longer “held” by the representative of the public authority, and so can no longer be released to persons requesting them. It is here noteworthy, that returning official documents without keeping a copy is not permitted in the absence of specific regulation. Such regulation is often in place, however, making it possible to return texts to the pupils.⁹¹

On the topic of secrecy regulation, finally, the report concluded that Swedish legislation contains no possibility to limit access to official documents containing personal information on children as long as these documents are related to education.⁹² All test results, project submissions etc. that the children produce are therefore “almost without exception, probably official”, even if containing very sensitive information.⁹³ If it can be claimed that a document pertains to the school health or the care of children, access may be limited, though.⁹⁴

It should be noted that the arguments presented by the authors convey a legally complex situation. This is evident from the expression “almost without exception, probably official”, and other phrases of similar content.⁹⁵ Four out of six authors were highly trained legal experts, and yet they indicate difficulties in understanding the workings of the Swedish principle of public access to official documents.

The 2016 report

Turning now to the report published in 2016, we may recall that the emphasis was on the technological development and ensuing risks for personal integrity in different areas, the school being one of them. The authors of the report make no explicit description on how official documents are created or the legislation that regulate the activities of the authorities. In general terms, the authors describe that the “principle of public access to official documents” has historical roots from the 18th century and is regarded as a

“cornerstone for the democracy in Sweden”.⁹⁶ The criteria of official documents are not discussed, but the authors do describe how the technical development poses new challenges to the principle of public access to official documents:

As digitalisation becomes more widespread, new consequences of the principle of public access to official documents arise. The better and cheaper the technical possibilities to disseminate and process data, the larger the commercial value of the personal information kept by the public authorities. Therefore, many companies want access to the information. /.../ Once companies have received information in accordance with the principle of public access to official documents, they can disseminate and process the information for purposes that are completely different from those for which the public authorities collected them in the first instance.⁹⁷

From the quotation, it appears that the challenges to the principle of access are linked to the commercial value of the “personal information kept by the public authorities”. It would seem that the large amount of official documents kept at the public authorities have come to pose threats, as large quantities of those documents can now be easily transmitted from the authorities to the commercial companies. Implicit in the quotation is also the fact that control is lost over the information once it has been released. Using a term from the RCM, the authors of the report indicate that the Swedish principle allows for the dimension “pluralise”. In addition, the authors mention how companies may publish databases with sensitive personal data on the internet in accordance with a constitutional law, thereby effectively circumventing legislation aiming at the protection of personal integrity.⁹⁸ We recognize this case from the introduction to this paper.

As the authors analyse the situation in schools, they conclude that the use of technological tools is widespread; for instance, approximately two thirds of the municipal primary schools use digital platforms.⁹⁹ They conclude that very large volumes of data are collected about the children without anyone having an overview, and that the data might be used for other purposes.¹⁰⁰ As for secrecy regulation, the authors conclude that Swedish legislation does not allow for any limitation on the access to official documents created as part of the education, the exception being if it is possible to claim that the information is linked to the school health or special care of pupils.¹⁰¹

Summary and discussion:

The Swedish Black Box and the case of school children

Thirteen years had elapsed between the two reports presented above. During this time, the use of technological tools of different kinds had taken a great leap in Swedish schools. Let us now make a thought experiment, so that the same question is asked to the two reports from 2003 (situation 1) and 2016 (situation 2). The question is this: if a pupil hands in a text to the teacher for assessment, and a person requests the release of the text in accordance with the Swedish principle of public access to official documents once the assessment is ready, will the text be released?

In situation 1 in 2003 (graph to the left below), we may deduce from the report that documents are still primarily in paper format. The pupil hands in the text to the teacher for assessment (arrow “Input”), and as long as the text is “held” by the public authority, it is considered an official document. The legislation contains no provision which would allow for limiting the release of official documents, however sensitive, unless it might be argued that it is linked to the school health or care of children. This is all in accordance with what is clearly stated in the report. However, secrecy regulation is of no importance in this instance, as the paper document is returned to the child after assessment. Therefore, when the person requesting the release comes to the “system” in situation 1, there is no arrow for “Output” as the official document is no longer contained in the system.

Situation 1



Figure 4: Visualisation of situation 1.

Situation 2



Figure 5: Visualisation of situation 2.

In situation 2 in 2016, documents are described as primarily processed through various digital tools; about two thirds of the schools use various digital platforms. In this situation, we may envisage how the child hands in the text by posting it in the digital platform for assessment by the teacher (arrow “Input”). It is likely that the assessment is carried out in the digital

platform. The secrecy regulation is the same as in situation 1, i.e. it has no provision for limiting the release of official documents unless part of the school health or care of children.¹⁰² As long as the digital texts are not disposed of, we may deduce that they are still “held” by the public authority.¹⁰³ If this is the case, the release of the document must take place however sensitive the information. In situation 2, therefore, the graph has an arrow “Output” from the system which will provide the text written by the child to the person requesting it. We should also recall, that approximately one third of the schools in 2016 were estimated not to have implemented digital platforms. We may therefore imagine, that a person requesting the release of a text handed in by a child in a public school not using digital platforms in 2016, would retrieve nothing from the system. This means, that in 2016, the system might respond as in situation 1, or as in situation 2, depending on whether the school had implemented digital platforms or not.

How, then, may we describe the difference between the two situations? What factors have changed? Recalling the seven factors from Figure 3: The Swedish Black Box, there is no indication of changes in legislation regulating the activities of public authorities, nor have any changes of the criteria making up an official document been implied. It is possible that public schools in situation 2 have updated their routines regarding disposal of digital documents in accordance with legislation. In case the schools have not implemented such new routines, the factor legislation on disposal of official documents would also remain unaltered. This is also true for legislation on secrecy, which, according to the 2016 report, still stipulates that documents pertaining to education must be released however sensitive the information. The processes and activities of public schools also seem unchanged; the school children hand in their texts, and teachers assess them. Regarding technology and routines, things are different, however. Technological development has allowed the implementation and use of new tools, such as the digital platforms used by many schools according to the 2016 report. This implementation of new technology, in turn, led to new routines if the teacher assessed the text digitally instead of in a paper format. If the school did not dispose of the digital document, the official document would continue to be “held” by the school as part of the digital platform. In summary, technology and ensuing changes of routines led to changes in the functions of the system, the outcome of which was to increase the number of official documents possible to retrieve from the system.

It is noteworthy that these changes were not related to legislation. The analysis therefore indicates that it might be difficult to foresee the workings of the Swedish principle of public access to official documents. In addition to the absence of changes of legislation, we may identify a few more reasons why the Swedish principle might be difficult to predict. One such reason is the fact that the principle is only fully applicable to schools that are deemed to be public authorities. The level of protection of the personal integrity of school children will thus depend on whether the school is public or private. An official government report from 2007 stated that pupils in private schools “normally run no risk that such data [regarding love relations or problems in the family] are released, and therefore have a better protection against infringement of their personal integrity than pupils in public schools, in this respect”.¹⁰⁴ The authors added that this seemed a breach against the Convention of the Right of the Child, according to which all children should have the same protection.¹⁰⁵ To the extent that it is not clear for parents and school children what might happen to the children’s personal data kept in public and private schools, this is another reason why the principle might be difficult to clearly understand and predict.¹⁰⁶ This goes also for the fact that Swedish schools have increased their level of documentation of individual pupils, a fact which has been identified as a potential problem for the personal integrity of the children.¹⁰⁷ The report from 2007 further emphasised how the documentation was made digitally to a larger extent, making it easier to “collect, compile and diffuse information about individuals”.¹⁰⁸ Again, this seems to make it difficult for individuals to foresee how much of their personal data that might be accessible through the Swedish principle of public access.

5. Conclusion and discussion

In this article, basic concepts on black box theory were combined with information from previous research about factors that may affect the creation and release of official documents in Sweden. The term “black box” is used to describe a system which is not possible to observe directly. Instead of directly analysing the system, the observer will therefore have to provide input to the system, and study the resulting output. The combination of black box theory and factors affecting the creation and release of official documents were merged into a model, here called the Swedish Black Box, to shed light over the principle of public access to official documents in Sweden. The model was applied to two official government reports from

2003 and 2016, respectively. Both reports treat aspects of the educational system. The answer to the same fundamental question was sought in the two reports: if a pupil hands in a text to the teacher for assessment and a person requests the release of the text in accordance with the Swedish principle of public access after the assessment, will the pupil's text be released?

In the situation of 2003, the texts did not fulfil the criteria "held" by the public authority once they had been returned to the pupils, and a person claiming her right of free access to official documents would thus receive no "output". In the second report from 2016, many schools had implemented digital systems for receiving written texts. After assessment by the teacher, it is likely that the texts would still be "held" digitally by the public authority. A person claiming her right of access in this situation would therefore receive "output" from the system in the form of the written text of the child. Not all schools were reported to use digital platforms, however. Persons requesting the release of a pupil's text after it was being handed back in paper format were thus likely not to receive any output. In 2016, therefore, the system might give two kinds of output, depending on the implementation of technology of the schools. This is an indication that it may be difficult for individuals to predict how much of their personal data that might be accessible through the Swedish principle of public access. This is further emphasised by the difference in legislation between public and private schools. Pupils in private schools "normally run no risk that such data [regarding love relations or problems in the family] are released", only pupils in public schools, a fact which has led the authors of a government report to suspect a breach against the Convention of the Right of the Child, according to which all children should have the same protection. Increased levels of documentation of individual pupils in Swedish schools and transfer from paper to digital processing, are other developments which make it difficult for individuals to foresee how much of an individual's personal data that might be accessible through the Swedish principle of public access.

It might therefore be argued that the Swedish principle of public access to official documents contrasts with the concept of rule of law. The latter concept means that individuals should be able to know about the rules of a country, and in consequence thereof be able to plan their lives in accordance with the rules.¹⁰⁹ Through the means of "public, prospective laws, with the qualities of generality, equality and certainty, [...]", such knowledge is possible to obtain.¹¹⁰ The rule of law, in turn, is regarded as a cornerstone of democracy.¹¹¹ That individuals are able to know what official

documents with their personal data might be produced and released is therefore quite easy to regard as important from a democratic perspective, as well as from the perspective of personal integrity.

This article has focused on one single area – texts written by school children – and so is very limited in scope. The Swedish principle of public access has been regarded as a system, the functions of which depends on a number of factors, making it complex and hard to look into – hence the term black box. Recalling, for instance, how legal scholars have identified numerous instances when court proceedings were necessary to interpret criteria making up Swedish official documents, the system does seem complex, and to merit investigation into more areas.

¹ For very insightful and constructive comments on a previous version of this paper, I wish to extend my warmest thanks to Rob Day, School of Engineering, Jönköping University, Samuel Edquist, Department of ALM, Uppsala University, Patricia Jonason, School of Social Sciences, Södertörn University, Proscovia Svärd, School of Historical and Contemporary Studies, Södertörn University.

² See e.g. Council of Europe, *Recommendation 854 (1979), Access by the public to government records and freedom of information*, 1979, p. 1.

³ Björkstrand, Gustav & Mustonen, Juha. Introduction: Anders Chydenius' Legacy Today in *The world's first Freedom of Information Act: Anders Chydenius' legacy today*, Mustonen, Juha ed., Kokkola: Anders Chydenius Foundation, 2006, p. 4.

⁴ See e.g. Holmgren, Martin. The Swedish Principle of Public Access to Official Documents – in Relation to Archival Theory and Electronic Data Processing. *The Principle of Provenance*, Abukhanfusa, Kerstin & Sydbeck, Jan eds. Stockholm: Swedish National Archives, 1994, p. 70, see also p. 66; Knudsen, Tim. *Offentlighed i det offentlige: om historiens magt*. Aarhus: Aarhus Universitetsforlag, 2003, p. 118; Saarenpää, Ahti. Data protection: In pursuit of information. Some Background to, and Implementations of, Data Protection in Finland. *International Review of Law, Computers & Technology* no. 1 (1997), p. 49.

⁵ SFS 1949:105 *Tryckfrihetsförordning, Freedom of the Press Act*, ch. 2, 1 §. "Foreign nationals" have the same access, unless stated otherwise, SFS 1949:105, ch. 14; Bohlin, Alf, *Offentlighetsprincipen*. Stockholm: Norstedts Juridik, 2010, p. 19.

⁶ SFS 1949:105, ch. 2, 12 §.

⁷ As the stance was gradually taken in Sweden that official documents were to be preserved as the default option, the link between democracy and the principle became more apparent. Rosengren, Anna. *Openness, Privacy and the Archive: Arguments on openness and privacy in Swedish national archival regulation 1987–2004*, Södertörns högskola, Working paper 2016:4. For literature on the principle and democracy, see e.g. Rapaport, Edmund & Samuelson, Per. Storing of Public Data for Research – The Swedish Case. *Government Publications Review*, 1991, Vol. 18(1), p.66; Gränström, Claes. *Arkivteori. Arkivvetenskap*, Ulfspärre, Anna Christina ed. 1:12 ed. Lund:

Studentlitteratur, 1995, p. 12. I shall refer to the “principle of public access to official documents” as “the principle of public access” or “principle”, in addition to expressions such as “the Swedish model”, “the Swedish situation” etc. The translation of “offentlighetsprincipen” is taken from *Personal data protection: information on the Personal Data Act*. Stockholm: Ministry of Justice, 4th revised edition, 2006, p. 13. This is also the term used by Kallberg. Kallberg, Maria. *‘The Emperor’s New Clothes’. Recordkeeping in a new context*. Mid Sweden University, Faculty of Science, Technology and Media (diss), 2013, p. 2.

⁸ SFS 1990:782 *Arkivlag* 3 §. As will be discussed later, secrecy regulation is comprehensive and covers seven areas identified as sensitive in the *Freedom of the Press Act*, ch. 2. Among the areas are national security, fiscal policy and “the protection of the personal or economic circumstances of individuals”. First and foremost, the secrecy regulation consists of *The Public Access to Information and Secrecy Act* (SFS 2009:400 *Offentlighets- och sekretesslagen*). This act is supplemented by the *Swedish Personal Data Act*, (SFS 1998:204 *Personuppgiftslag*) the Swedish interpretation of the EU directive on the protection of personal data, as well as laws regulating access to public data in the form of personal information in electronic registers. These secrecy regulations, in turn, contain numerous exceptions, see e.g. note 14 below.

⁹ Fredrikzon, Johan. *Särskilt betydelselösa. Informationsöverflöd och arkivgallring i Sverige vid mitten av 1900-talet*. Stockholms universitet, Institutionen för litteraturvetenskap och idéhistoria, magisteruppsats, 2014, p. 36. See also Rydén, Reine. *Hur ska nutiden bevaras?* *Arkiv, samhälle och forskning* 2011:2, p. 13.

¹⁰ SFS 1949:105, ch. 2. See also Bohlin 2010 p. 24 and Magnusson Sjöberg, Cecilia, *Rättsinformatik: inblickar i e-samhället, e-handel och e-förvaltning*. Lund: Studentlitteratur, 2011. p. 329. Exceptions to this rule exist, so that e.g. private correspondence is excluded, SFS 1949:105, ch. 2, 8 §. The criteria are not always easy to interpret. Furthermore, a distinction is often made between “cases” and other types of activities of public authorities. Certain documents related to “cases” are deemed public once the case is closed and it is decided that the related documents should be archived, SFS 1949:105, ch. 2, 8 §. On numerous occasions court proceedings have been necessary to determine whether a criterion was to be regarded as fulfilled or not, and whether a document was part of a “case”. See e.g. Bohlin 2010 and Magnusson Sjöberg 2011 for examples of interpretations requiring court proceedings.

¹¹ An example of the propensity to openness is the name of the main secrecy protection law, *The Public Access to Information and Secrecy Act*, which puts public access first. See also Bohlin 2010, p. 189 and Österdahl, Inger. Between 250 Years of Free Information and 20 Years of EU and Internet. *Etikk i praksis*, 2016, Vol.10(1), p.27. Researchers have discussed the somewhat unique situation in Sweden, see e.g. Larsson, Torbjörn. How open can a government be? The Swedish experience. *Openness and Transparency in the European Union*. Deckmyn, Veerle & Thomson, Ian eds. Maastricht: European Institute of Public Administration, 1998, p. 47; Gränström, Claes, Lundquist, Lennart & Fredriksson, Kerstin. *Arkivlagen. Bakgrund och kommentarer*. 2 ed. Stockholm: Norstedts Juridik, 2000, p. 67; Bohlin 2010 p. 283; Geijer, Ulrika, Lenberg, Eva, Lövblad, Håkan. *Arkivlagen. En kommentar*. Stockholm: Norstedts juridik, 2013, p. 77.

¹² SOU 2016:41 *Hur står det till med den personliga integriteten?*, p. 61. "Rätten till personlig integritet" "är därmed en viktig faktor även för andra, centrala" "rättigheter", "som är grunden för ett demokratiskt samhälle." Translation by the author.

¹³ The example is taken from *Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents*. Article 4 Exceptions "1. The institutions shall refuse access to a document where disclosure would undermine the protection of: [...] (b) privacy and the integrity of the individual, [...]". A similar example is provided from France: *Livre III: Accès aux documents administratifs et la réutilisation des informations publiques*, Section 1, Article L311-6: "Ne sont communiqués qu'à l'intéressé les documents administratifs: 1° Dont la communication porterait atteinte à la protection de la vie privée, [...]".

¹⁴ As Österdahl points out, the Swedish version of the EU directive on the protection of personal data, *Personuppgiftslag*, states that the Swedish constitutional law should prevail in case of conflict with the *Personuppgiftslag*. Effectively, the directive on the protection of personal data is thus circumvented. Österdahl 2016, p. 30. For an analysis of arguments in Swedish government reports leading to the exceptions to the protection of personal data, see Rosengren, Anna. *Offentlighetsprincipen i teori och praktik. Arkiv, samhälle och forskning*, 2017:1, pp. 26-57.

¹⁵ Österdal 2016, p. 32.

¹⁶ See Österdahl 2016. To this might be added the Swedish *Archival Law*, which stipulates that official documents be preserved to "provide the right of free access to public records, the information requirements for the jurisdiction and administration, and research requirements", SFS 1990:782, 3 §. Translation by Mira Barkå. Barkå, Mira. *Legal framework for records management and archives. Public authorities and private financial institutions in Sweden*. 3rd Workshop on Archival Legislation for Finance (ALFF) in Europe, year unknown.

¹⁷ Dingwall, Glenn. Life cycle and continuum: a view on recordkeeping models from the postwar era. *Currents of archival thinking*, Eastwood, Terry & MacNeil, Heather, eds. Santa Barbara: Libraries Unlimited, 2010, p. 142.

¹⁸ Upward, Frank. Modelling the continuum as paradigm shift in recordkeeping and archiving processes, and beyond – a personal reflection. *Records Management Journal*, Vol.10(3), 2000, p. 121.

¹⁹ Dingwall 2010, p. 142.

²⁰ Schellenberg *Modern archives: principles and techniques*. Melbourne: Chesire, 1956, p. 16.

²¹ Schellenberg 1956, p. 16.

²² Dingwall 2010, pp. 140-141; quotation p. 144.

²³ Schellenberg 1956, p. 16.

²⁴ Borglund 2007, p. 54. The argument raised is that metadata is applied to paper documents only upon arrival to the archive, not at the birth of the document.

²⁵ Borglund 2007, p. 54.

²⁶ Svärd, Proscovia. Enterprise Content Management and the Records Continuum Model as strategies for long-term preservation of digital information. *Records Management Journal*, Vol. 23, No 3, 2013, pp. 170-171.

²⁷ Svärd 2013, p. 171.

²⁸ In accordance with the translation of the Ministry of Justice, the term “official document” is used (see note 7). This is also the stance taken by Kallberg (2013, p. 2), whereas other researchers have used “record” to designate “official documents” (Borglund, Erik & Engvall, Tove. Open data? Data, information, document or record? *Records Management Journal*, 24(2), 2014, p. 169.

²⁹ Atherton, Jay. From Life Cycle to Continuum: Some Thoughts on the Records Management–Archives Relationship. *Archivaria* 21, Winter 1985-86, p. 47; Upward 2000, p. 128; Cumming, Kate. Ways of seeing: contextualising the continuum. *Records Management Journal*, 20(1), 2010, p. 47.

³⁰ McKemmish, Sue. Placing records continuum theory and practice. *Archival Science* 1(4), 2001, p. 335. On obsolete division into records managers and archivists, see also Atherton 1985-86, p. 47.

³¹ Upward 2000, p. 128.

³² Upward 2000, p. 119.

³³ McKemmish 2001, p. 335.

³⁴ Upward, Frank. Structuring the records continuum – Part two. Structuration theory and recordkeeping. *Archives and Manuscript*, Vol. 25, No. 1, 1997, p. 16.

³⁵ Upward, Frank & McKemmish, Sue. Teaching recordkeeping and archiving continuum style. *Archival Science*, 6, 2006, p. 222.

³⁶ Reed, Barbara. Reading the records continuum: interpretations and explorations. *Archives and Manuscripts*, Vol. 33 (1), 2005, p. 20.

³⁷ Svård 2013, p. 165.

³⁸ Upward 2000, p. 121.

³⁹ Reed 2005, p. 20.

⁴⁰ Upward & McKemmish 2006, p. 223.

⁴¹ Upward 2000, p. 122.

⁴² McKemmish 2001, p. 335; Huvila, Isto, Eriksen, Jon, Hausner, Eva-Maria & Jansson, Ina-Maria. Continuum thinking and the context of personal information management. *Information Research*, Vol. 19, No. 1, 2014, p. 4.

⁴³ Upward 2000, p. 124.

⁴⁴ Svård 2013, p. 170; Kallberg 2013, p. 2. Similarly, Erik Borglund states that “modern archival practice” [“modern arkivpraktik”] uses the RCM. Borglund 2007, p. 54.

⁴⁵ Kallberg 2013, p. 11. It is appropriate to recall note 10 and the fact that a document related to a “case” is deemed public once the case is closed and it is decided that the document should be archived. As a result, it may be difficult to determine whether documents pertain to a “case”, and whether the criteria in general have been fulfilled or not, as shown e.g. in the works of Bohlin 2010 and Magnusson Sjöberg 2011.

⁴⁶ Svård 2013, p. 161.

⁴⁷ Svård 2013, pp. 161, 171. Re-use of official documents is an issue linked to a EU directive on the re-use of “public sector information”. For the implementation of the EU directive in Sweden, see Jonason, Patricia. The transposition of the PSI Directive into the Swedish legal system. *Public Sector Information - Open Data: What is fair: Free Access or Fees?*, Balthasar, Alexander & Sully, Melanie (eds.). Facultas, Wien, 2014, pp. 53-63.

⁴⁸ Edquist, Samuel. *Arkiven, bevarandet och kulturarvet*. Stockholm: Riksarkivet, 2014, p. 1.

⁴⁹ Dingwall 2010, p. 143.

⁵⁰ See e.g. Geijer, Lenberg & Lövsblad 2013, p. 64; 178-179, as well as SFS 1990:782 *Arkivlag* 10 §.

⁵¹ See note 8, 9 and 10.

⁵² Again, this is subject to documents not pertaining to a “case”, see note 10.

⁵³ McKemmish 2001, p. 335; Huvila et al. 2014, pp. 4, 13.

⁵⁴ Upward 2000, p. 124.

⁵⁵ Kallberg 2013, p. 6.

⁵⁶ Svärd 2013, p. 167.

⁵⁷ Kallberg 2013, p. 119.

⁵⁸ Cf. Magnusson Sjöberg who argues that “the more advanced the technical environment of a public authority, the more information will be deemed available to, and thereby held by, the authority” (“ju mer avancerad en myndighets tekniska miljö är, desto flera uppgifter kommer att anses tillgängliga och därmed förvarade hos myndigheten”). Magnusson Sjöberg 2011, p. 329. Translation by the author.

⁵⁹ Kallberg 2013, p. 119.

⁶⁰ According to Swedish law, all public authorities are required to describe “the organization and activities” and “registers” and other ways of searching official documents (SFS 2009:400 *Offentlighets- och sekretesslag*, ch. 4, 2 §; translation by the author). Previous research has indicated how changes of several factors may give rise to new official documents, however. Such changes of factors will, in all likelihood, make it difficult to understand what official documents are held by a Swedish public authority. To this may be added, for instance, that private health institutions fulfil legal requirements and report sensitive personal data to national quality registers. The private health institutions are no public authorities, and so produce no official documents themselves. However, laws, and sometimes ordinances issued by the government, may stipulate that private health institutions breach secrecy regulation and report health data to public authorities. As it is not always clear to what extent the patient is informed about how sensitive health data may be reported to public authorities, it is difficult for the citizen to be aware of and predict what data on her may become official documents. Information on health organisations, secrecy and breaches of secrecy in health organisations from Sandén, Ulrika. *Sekretess och tystnadsplikt inom offentlig och privat hälso- och sjukvård: ett skydd för patientens personliga integritet*. Umeå: Umeå universitet, 2012, ch. 4.

⁶¹ Kallberg 2013, p. 119. The comment is made in relation to “strategic recordkeeping.”

⁶² Borglund 2007, p. 50.

⁶³ As previously mentioned, the Swedish *Archival Law* stipulates that documents be preserved, among others, for “the information requirements for the jurisdiction and administration”, but no formal requirement is indicated in the law on the evidential nature of the documents.

⁶⁴ As presented by Upward 1997.

⁶⁵ Upward 1997, p. 25.

⁶⁶ Huvila et al. 2014, p. 13.

⁶⁷ Huvila et al. 2014, p. 13.

⁶⁸ Bunge, Mario. A General Black Box Theory. *Philosophy of Science*, Vol. 30, No. 4 (Oct., 1963), p. 346. This is in contrast to closed systems, which are considered “isolated from their environment.” von Bertalanffy, Ludwig. *General system theory: foundations, development, applications*. New York: Braziller, 1969, p. 39.

⁶⁹ von Bertalanffy 1969, p. 33.

⁷⁰ Bunge 1963, p. 346; Ashby, W. Ross. *An introduction to cybernetics*. London: Chapman & Hall, 1956, p. 88.

⁷¹ Ashby 1956, p. 86.

⁷² von Bertalanffy 1969, p. 122.

⁷³ Occasionally, the “input” may be less obvious than in the case of a citizen sending in her tax declaration to a public authority, as illustrated by the transfer of health data from private to public health organisations, see note 60.

⁷⁴ Friberg, Anna. Experterna och språket. Begreppshistoriska perspektiv på statens offentliga utredningar. *Dolt i offentligheten: nya perspektiv på traditionellt källmaterial*, Förhammar, Staffan, Harvard, Jonas & Lindström, Dag (eds.). Lund: Sekel, 2011, pp. 48-49. See also the discussion in Rosengren, Anna. *Åldrandet och språket. En språkhistorisk analys av hög ålder och åldrande i Sverige cirka 1875-1975*. Huddinge: Södertörns högskola, 2011, p. 44.

⁷⁵ Landqvist, Hans. *Författningssvenska: strukturer i nutida svensk lagtext i Sverige och Finland*. Göteborg: Acta Universitatis Gothoburgensis, 2000, p. 37 (quotation in Landqvist from Hiltunen 1990).

⁷⁶ SOU 2016:41 p. 198 ”Barn måste anses som särskilt viktiga när det gäller att skyddas mot otillbörliga intrång i den personliga integriteten [...]” Translation by the author.

⁷⁷ SOU 2016:41 pp. 66-67.

⁷⁸ SOU 2003:103 *Sekretess i elevernas intresse. Dokumentation, samverkan och integritet i skolan*, pp. 7-8; 11; 81. Translation by the author.

⁷⁹ SOU 2003:103 section 7.3-7.6.

⁸⁰ SOU 2016:41 *Hur står det till med den personliga integriteten*. Translation by the author.

⁸¹ SOU 2016:41 pp. 11-22.

⁸² SOU 2016:41 p. 11.

⁸³ SOU 2007:22 *Skyddet för den personliga integriteten kartläggning och analys*; SOU 2011:58 *Skolans dokument – insyn och sekretess*. Translation by the author.

⁸⁴ Nilsson, Marco. *Juridik i professionellt lärarskap. Lagar och värdegrund i en svenska skolan*. Malmö: Gleerups Utbildning 2016, pp. 11, 16; Boström & Lundmark 2016, p. 154.

⁸⁵ SOU 2003:103 p. 11.

⁸⁶ SOU 2003:103 pp. 43-45.

⁸⁷ SOU 2003:103 pp.105-106.

⁸⁸ SOU 2003:103 p. 110: ”Under kortare eller längre tid förvarar skolor ofta skriftligt material som har upprättats av eleverna inom ramen för skolarbetet.”, ”Ofta återlämnas materialet till eleverna efter det att en bedömning av resultatet har gjorts, men under den tid det är i lärarens vård [...] måste materialet anses förvarat av skolan i den mening som avses i 2 kap. 3 § TF. Handlingar som förvaras av en skola är allmänna där, om de kan anses upprättade av eller inkomna till myndigheten.” Translation by the author. As indicated by the authors, returning official documents is regarded as disposing of them, an action which is permitted if granted by legislation (p. 111).

⁸⁹ SOU 2003:103 p. 111 ”lämnas ut till den som begär det”. Translation by the author.

⁹⁰ SOU 2003:103 p. 111 ”lämnas tillbaka till eleverna”. Translation by the author.

⁹¹ SOU 2003:103 p. 111.

⁹² SOU 2003:103 p. 113.

⁹³ SOU 2003:103 p. 113 “nästan undantagslöst torde vara offentliga”. Translation by the author.

⁹⁴ SOU 2003:103 p. 113.

⁹⁵ See e.g. SOU 2003:103, pp. 103; 105; 113.

⁹⁶ SOU 2016:41 p. 60.

⁹⁷ SOU 2016:41 pp. 60-61: “I takt med digitaliseringen uppkommer nya konsekvenser för offentlighetsprincipen. Ju bättre och billigare de tekniska möjligheterna att sprida och sambearbeta olika uppgifter blir, desto större blir det kommersiella värdet av de personuppgifter som finns hos myndigheterna. Många företag vill därför få åtkomst till uppgifterna. En del myndigheter kan ta betalt för vissa utlämnanden. Uppgifterna får därmed en ekonomisk betydelse även för myndigheterna. När företag har fått ut uppgifter med stöd av offentlighetsprincipen, kan de sprida och hantera uppgifterna för helt andra ändamål än dem för vilka myndigheten ursprungligen samlade in uppgifterna. Ibland kan företagen även publicera integritetskänsliga uppgifter på nätet med grundlagsskydd genom s.k. frivilliga utgivningsbevis, med den följden att vissa delar av det integritetsskyddande regelverket inte längre gäller.” Translation by the author.

⁹⁸ SOU 2016:41 pp. 60-61.

⁹⁹ SOU 2016:41 p. 176.

¹⁰⁰ SOU 2016:41 p. 199-200. An important reason for the collection of large volumes of data on children is the fact that education is considered “of general interest”. In turn, this means that registration of information may be done without the consent of the child or the child’s parents, SOU 2016:41 p. 179, see also SOU 2003:103, p. 199.

¹⁰¹ SOU 2016:41 pp. 180; 199.

¹⁰² See also Boström & Lundmark 2016, p. 144.

¹⁰³ The school could have implemented a routine to the effect that digital copies were to be disposed of once the original had been shared with the child. With the implementation of digital tools, schools would nevertheless have to implement new routines if the amount of official documents were not to increase in comparison with the paper situation.

¹⁰⁴ SOU 2007:22 p. 374 (“löper normalt ingen risk att sådana uppgifter [kärleksrelationer eller familjeproblem] lämnas ut och har därför i det avseendet ett bättre skydd för sin personliga integritet än barn i offentliga skolor”). Translation by the author.

¹⁰⁵ SOU 2007:22 p. 374.

¹⁰⁶ A new EU regulation on the protection of personal data stipulates that “[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned [...]”. It would seem as if the Swedish principle of public access to official documents makes it difficult to protect the children in accordance with the EU regulation. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), point (38) p. 7.

¹⁰⁷ SOU 2003:103 p. 12; SOU 2007:22 p. 373.

¹⁰⁸ SOU 2007:22 p. 373 (“samla in, sammanställa och sprida uppgifter om enskilda”). Translation by the author.

¹⁰⁹ Tamanaha, Brian Z.A. The Rule of Law for Everyone? *Current Legal Problems*, 55.1 (2002), p. 112. Tamanaha refers to the Austrian philosopher Friedrich Hayek in this section. *Rule of law* is a concept with varying interpretations. For the purposes of this study, what is often referred to as the “formal” view, closely linked to predictability, is used. For information on the formal view, see e.g. Young, Alison L. The Rule of Law in the United Kingdom: Formal or Substantive?, *Vienna Journal on International Constitutional Law*, 01/1/2012, Vol.6(2), p. 261.

¹¹⁰ Tamanaha, Brian Z.A. The Rule of Law for Everyone? *Current Legal Problems*, 55.1 (2002), p. 104; 112-113.

¹¹¹ See e.g. Magen, Amichai & McFaul, Michael A. Introduction: American and European Strategies to Promote Democracy – Shared Values, Common Challenges, Divergent Tools? *Promoting Democracy and the Rule of Law – American and European Strategies*. Magen, Amichai, Risse, Thomas & McFaul, Michael A. eds, Basingstoke, Palgrave Macmillan, 2009, pp. 1-33.

References

- Ashby, W. Ross. *An introduction to cybernetics*. London: Chapman & Hall, 1956.
- Atherton, Jay. From Life Cycle to Continuum: Some Thoughts on the Records Management–Archives Relationship. *Archivaria* 21, Winter 1985–86, pp. 43–51.
- Björkstrand, Gustav & Mustonen, Juha. Introduction: Anders Chydenius' Legacy Today. *The world's first Freedom of Information Act: Anders Chydenius' legacy today*, Mustonen, Juha (ed.), Kokkola: Anders Chydenius Foundation, 2006, pp. 4–6.
- Bohlin, Alf. *Offentlighetsprincipen*. Stockholm: Norstedts Juridik, 2010.
- Borglund, Erik. En introduktion till EDM och EDM ur ett arkivvetenskapligt perspektiv. *Arkiv, samhälle och forskning* 2007:1, pp. 44–58.
- Borglund, Erik & Engvall, Tove. Open data? Data, information, document or record? *Records Management Journal*, 24(2), 2014, pp. 163–180.
- Boström, Viola & Lundmark, Kjell. *Skoljuridik*. Malmö: Liber, 2016.
- Bunge, Mario. A General Black Box Theory. *Philosophy of Science*, Vol. 30, No. 4 (Oct., 1963), pp. 346–358.
- Council of Europe, *Recommendation 854 (1979), on access by the public to government records and freedom of information*, 1979.
- Cumming, Kate. Ways of seeing: contextualising the continuum. *Records Management Journal*, 20(1), 2010, pp. 41–52.
- Dingwall, Glenn. Life cycle and continuum: a view on recordkeeping models from the postwar era. *Currents of archival thinking*, Eastwood, Terry & MacNeil, Heather, eds. Santa Barbara: Libraries Unlimited, 2010, pp. 139–161.
- Edquist, Samuel. *Arkiven, bevarandet och kulturarvet*. Stockholm: Riksarkivet, 2014.
- Fredrikzon, Johan. *Särskilt betydelselösa. Informationsöverflöd och arkivgallring i Sverige vid mitten av 1900-talet*. Stockholms universitet, Institutionen för litteraturvetenskap och idéhistoria, magisteruppsats, 2014.
- Friberg, Anna. Experterna och språket. Begreppshistoriska perspektiv på statens offentliga utredningar. *Dolt i offentligheten: nya perspektiv på traditionellt källmaterial*, Förhammar, Staffan, Harvard, Jonas & Lindström, Dag (eds.). Lund: Sekel, 2011, pp. 47–59.
- Geijer, Ulrika, Lenberg, Eva, Lövblad, Håkan. *Arkivlagen. En kommentar*. Stockholm: Norstedts juridik, 2013.
- Gränström, Claes. Arkivteori. *Arkivvetenskap*, Ulfspärre, Anna Christina ed. 1:12 ed. Lund: Studentlitteratur, 1995, pp. 3–29.
- Gränström, Claes, Lundquist, Lennart & Fredriksson, Kerstin. *Arkivlagen. Bakgrund och kommentarer*. 2 ed. Stockholm: Norstedts Juridik, 2000.
- Holmgren, Martin. The Swedish Principle of Public Access to Official Documents – in Relation to Archival Theory and Electronic Data Processing. *The*

- Principle of Provenance*, Abukhanfusa, Kerstin & Sydbeck, Jan eds. Stockholm: Swedish National Archives, 1994, pp. 65–73.
- Huvila, Isto, Eriksen, Jon, Hausner, Eva-Maria & Jansson, Ina-Maria. Continuum thinking and the context of personal information management. *Information Research*, Vol. 19, No. 1, 2014, pp. 1–19.
- Jonason, Patricia. The transposition of the PSI Directive into the Swedish legal system. *Public Sector Information – Open Data: What is fair: Free Access or Fees?*, Balthasar, Alexander & Sully, Melanie (eds.). Facultas, Wien, 2014, pp. 53–63.
- Kallberg, Maria. *'The Emperor's New Clothes'.* *Recordkeeping in a new context*. Mid Sweden University, Faculty of Science, Technology and Media (diss.), 2013.
- Knudsen, Tim. *Offentlighed i det offentlige: om historiens magt*. Aarhus: Aarhus Universitetsforlag, 2003.
- Landqvist, Hans. *Författningssvenska: strukturer i nutida svensk lagtext i Sverige och Finland*. Göteborg: Acta Universitatis Gothoburgensis, 2000.
- Larsson, Torbjörn. How open can a government be? The Swedish experience. *Openness and Transparency in the European Union*. Deckmyn, Veerle & Thomson, Ian eds. Maastricht: European Institute of Public Administration, 1998, pp. 39–51.
- Magen, Amichai & McFaul, Michael A. Introduction: American and European Strategies to Promote Democracy – Shared Values, Common Challenges, Divergent Tools? *Promoting Democracy and the Rule of Law – American and European Strategies*. Magen, Amichai, Risse, Thomas & McFaul, Michael A. eds., Basingstoke, Palgrave Macmillan, 2009, pp. 1–33.
- McKemmish, Sue. Placing records continuum theory and practice. *Archival Science* 1(4), 2001, pp. 333–359.
- Livre III: Accès aux documents administratifs et la réutilisation des informations publiques*.
- Magnusson Sjöberg, Cecilia. *Rättsinformatik: inblickar i e-samhället, e-handel och e-förvaltning*. Lund: Studentlitteratur, 2011.
- Nilsson, Marco. *Juridik i professionellt lärarskap. Lagar och värdegrund i en svenska skolan*. Malmö: Gleerups Utbildning 2016.
- Personal data protection: information on the Personal Data Act*. Stockholm: Ministry of Justice, 4th revised edition, 2006.
- Rapaport, Edmund & Samuelson, Per. Storing of Public Data for Research – The Swedish Case. *Government Publications Review*, 1991, Vol.18(1), pp.65–69.
- Reed, Barbara. Reading the records continuum: interpretations and explorations. *Archives and Manuscripts*, Vol. 33 (1), 2005, 18–43.
- Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents*.

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Rosengren, Anna. *Åldrandet och språket. En språkhistorisk analys av hög ålder och åldrande i Sverige cirka 1875–1975*. Huddinge: Södertörns högskola, 2011.
- Rosengren, Anna. *Openness, Privacy and the Archive: Arguments on openness and privacy in Swedish national archival regulation 1987–2004*. Huddinge: Södertörns högskola, 2016, Working paper 2016:4.
- Rosengren, Anna. Offentlighetsprincipen i teori och praktik. *Arkiv, samhälle och forskning* 2017:1, pp. 26–57.
- Rydén, Reine. Hur ska nutiden bevaras? *Arkiv, samhälle och forskning* 2011:2, pp. 6–21.
- Saarenpää, Ahti. Data protection: In pursuit of information. Some Background to, and Implementations of, Data Protection in Finland. *International Review of Law, Computers & Technology* no. 1 (1997), pp. 47–64.
- Sandén, Ulrika. *Sekretess och tystnadsplikt inom offentlig och privat hälso- och sjukvård: ett skydd för patientens personliga integritet*. Umeå: Umeå universitet, 2012.
- Schellenberg, Theodor. *Modern archives: principles and techniques*. Melbourne: Chesire, 1956.
- SFS 1949:105 Tryckfrihetsförordning.
- SFS 1998:204 Personuppgiftslag.
- SFS 1990:782 Arkivlag.
- SFS 2009:400 Offentlighets- och sekretesslag.
- SOU 2003:103 *Sekretess i elevernas intresse. Dokumentation, samverkan och integritet i skolan*.
- SOU 2007:22 *Skyddet för den personliga integriteten kartläggning och analys*.
- SOU 2011:58 *Skolans dokument – insyn och sekretess*.
- SOU 2016:41 *Hur står det till med den personliga integriteten. En kartläggning av Integritetskommittén*.
- Swärd, Proscovia. Enterprise Content Management and the Records Continuum Model as strategies for long-term preservation of digital information. *Records Management Journal*, Vol. 23, No 3, 2013, pp. 159–176.
- Tamanaha, Brian Z.A. The Rule of Law for Everyone? Current Legal Problems, 55.1 (2002), pp. 97–122.
- Upward, Frank. Structuring the records continuum – Part two. Structuration theory and recordkeeping. *Archives and Manuscript*, Vol. 25, No. 1, 1997, pp. 10–35.
- Upward, Frank. Modelling the continuum as paradigm shift in recordkeeping and archiving processes, and beyond – a personal reflection. *Records Management Journal*, 2000, Vol.10(3), p. 115–139.

- Upward, Frank & McKemmish, Sue. Teaching recordkeeping and archiving continuum style. *Archival Science*, 6, 2006, pp. 219–230.
- von Bertalanffy, Ludwig. *General system theory: foundations, development, applications*. New York: Braziller, 1969.
- Young, Alison L. The Rule of Law in the United Kingdom: Formal or Substantive?, *Vienna Journal on International Constitutional Law*, 01/1/2012, Vol.6(2), pp. 259–280.
- Österdahl, Inger. Between 250 Years of Free Information and 20 Years of EU and Internet. *Etikk i praksis*, 2016, Vol.10(1), pp.27–44.

Unpublished material

- Barkå, Mira. *Legal framework for records management and archives. Public authorities and private financial institutions in Sweden*. 3rd Workshop on Archival Legislation for Finance (ALFF) in Europe, year unknown.

Online Proactive Disclosure of Personal Data by Public Authorities. A balance between transparency and protection of privacy

PATRICIA JONASON

Sweden is well known for having a generous and well-functioning right of access to information. However, the legal framework, the 250th anniversary of which we have recently celebrated, only provides for reactive disclosure. This is because the Freedom of the Press Act, which regulates the right of access to official documents, only endorses the citizens with the right to access documents after a request been made, and not with the right to access documents that are proactively "pushed out" by public authorities. This means in turn that the Swedish law only obliges the public authorities to disclose information after the submission of a request, and does not oblige these authorities to disclose information proactively. In practice Swedish public authorities, and not least local authorities, extensively publish information and documents on their websites. The procedure of publishing documents online certainly may constitute a useful tool for increasing transparency of the administration and improving public participation in public life¹, but the method may also have negative consequences. Indeed, when the information the public authorities make accessible on their websites contains elements of personal character, online disclosure may cause infringements of privacy. These risks of infringements that disclosure of personal information on the websites of public authorities can lead to, are exacerbated by the characteristics of the Internet and the possibilities of processing data offered by Cyberspace technology. The disclosure of data on the Internet doesn't know, in principle, any geographical limits. It does not know either any temporal limits: the information

¹ See Helen Darbishire, *Proactive Transparency: The future of the right to information*, *World Bank Institute; Governance Working Paper Serie*.

will never be deleted from the Internet² and will continue to define one's personal identity and personal history a long time after the information has lost its accuracy. Moreover, easy to gather together which other personal data by the help of search engines, the proactively disclosed information may be a supplementary piece in the mapping of an individual's personal circumstances, when it is not the first "link in the chain", from which other data are gathered. Additionally, if the degree of sensitivity of the disclosed data may increase the risks of privacy infringement, the dangers even exist if the personal data are quite insignificant by themselves, all the more since what constitutes an infringement is individual, it varies from person to person.³

The risks of privacy breaches are not only theoretical: the Swedish Data Protection Authority, has, as we will see further, handled several complaints stemming from citizens raising objections against the publication of personal data on the website of public authorities⁴ as well as has on some occasions *ex officio* investigated cases where personal data were published on public websites.

So, if the method for giving access to information consisting of online proactive disclosure may be a useful complement to the right of access in its reactive form, it might in the meanwhile lead to privacy infringements. This

² See thus the Google case C-131/12 in which the Court of Justice of the European Union acknowledges a right to be delisted. See Jonason, P. (2017), *Le droit à l'oubli numérique en Suède*, Blog droit européen, [https://blog\\$droiteuropeen.com/2017/05/19/le-droit-a-loubli-numerique-en-suede-par-patricia-jonason/](https://blog$droiteuropeen.com/2017/05/19/le-droit-a-loubli-numerique-en-suede-par-patricia-jonason/)

³ An example of privacy violations due to online publication of information that could at first glance appear as non sensitive concerns the posting on the website of the municipality of Borlänge of the names of all the inhabitants of the municipality. This publication, which, according to the municipality itself had the artistic purpose to "represent what an amount (mängd) is, the soul of the city and its human capital", has nevertheless been experienced by some of the inhabitants as constituting an infringement of their private life. Among the plaintiffs, some were women who, afraid of harassment, didn't wanted to disclose where they lived, other were refugees who wanted to be anonymous in Sweden. Other persons were outraged by the simple fact that information about them was accessible from all over the world. See in decision of the Data Protection Authority, Case n° 1062-99 Tillsyn enligt personuppgiftslagen (1998:204) – (Invånare i Borlänge kommun på webbplats).

⁴ In the meanwhile, its is difficult to estimate the number of complaints lodged to the Swedish Data Protection Authority against online publication of personal data. Indeed, it has not been possible to get precise information from the authority itself on the number of complaints. Moreover, due to the fact that the Data Protection Authority has no obligation to investigate a case after it has received a complaint, the number of complaints investigated does not necessary correspond to the number of complaints lodged in practice.

in turn poses the question of the existence of a protecting legal framework. What do the legal rules in place look like? How are they applied? These are the two questions we aim to answer in this paper with a special emphasis on the balancing between the need for transparency and the need for protection of privacy.

In the following we will examine the applicable legal provisions and their application in concrete cases (1) before summarising our findings (2).

1. The legal framework applicable to online proactive disclosure and its application

As mentioned earlier the Swedish legal framework on the right of access to information does not provide for rules on proactive disclosure.⁵ Public authorities, however, make use of this proceeding, not least in publishing diverse kind of documents and information on their websites, sometimes with an underlying aim of achieving more openness.⁶ Is it lawful when public authorities publish information of a personal character in this way?

⁵ On the contrary to many legislations on access to information around the world. See Manuela Garcia-Tabuyo, Alejandro Saez-Martin, Carmen Caba-Perez, (2017), "Proactive disclosure of public information: legislative choice worldwide", *Online Information Review*, Vol. 41 Issue:3, pp. 354-377. Some special Swedish legal instruments nevertheless regulate proactive disclosure, as for instance the Regulation on legal information, Rättsinformatiönsförordningen (1999:175).

⁶ Civil servants sometimes erroneously conceive that proactive disclosure is encompassed by the principle of access to information guaranteed by the Freedom of the Press Act. The statement, reproduced below, stemming from a County Council, criticised for having published meeting documents containing personal data on its website, witnesses this attitude. In order to justify the online publication the County Council argued that "*all meeting are open, in a democratic way and all the material including minutes are accessible for the public which has the right to insight and control in the decision-making*". See Decision of the Parliamentary Ombudsman of 4th March 2011, case n° 3684-2009, p. 2. Moreover, the fact that the Swedish Data Protection Authority underlines, in the introductory part of a checklist specifically drafted for municipalities and County Councils posting minutes and registers on their websites, that the principle of access to official documents doesn't pose any obligation to publish these kinds of documents on the Internet, could be seen as a confirmation that there is a certain faith among public authorities that the legal framework on the right of access to information encompasses the duty to disclose information on their own accord. *Checklista för kommuner och landsting – Webbpublicering av protokoll och diarier*. See also when it concerns the state's public authorities the Guidelines published by the Data Protection Authority *E-förvaltning och personuppgiftslagen – Statliga myndigheters behandling av personuppgifter*.

In order to answer the question and to determine how to carry out the balancing between transparency and protection for privacy that is raised in this kind of situations, one needs to legally qualify such a publication and determine the legal framework applicable.

Concerning the *qualification*, proactive disclosure of data of personal character constitutes data processing of personal data in the sense of data protection legislation. Indeed, it corresponds to the definition contained in Section 3 of the Personal Data Act (1998:204), which describes processing of personal data as “*Any operation or set of operations which is taken as regards personal data, whether or not it occurs by automatic means, for example [...] disclosure by transmission, dissemination or otherwise making information available [...]*”.⁷

As to the *applicable legal regime*, as proactive disclosure – as opposed to reactive disclosure – is not encompassed by the constitutional obligations to give access to information, the *lex superior* principle⁸, playing in favor of access to the detriment of protection for privacy when the right of access is guaranteed by the Freedom of the Press Act (1949:105), is not applicable here.⁹ Instead, the data protection legislation, including the Personal Data Act, is applicable.¹⁰

⁷ Which corresponds to Article 2 (b) of the Data Protection Directive 1995/46/EC, on which the Swedish Act relies. Article 2 (b) states: “*processing of personal data*’ (‘processing’) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as [...], disclosure by transmission, dissemination or otherwise making available, [...]”.

⁸ It means the principle aiming at solving law conflicts and according to which the law which constitutes the highest norm takes precedence before the law which has a lower status.

⁹ See also Section 8 of the Personal Data Act which states that “*The provisions of this Act are not applied to the extent that they would limit an authority’s obligation under Chapter 2 of the Freedom of the Press Act to provide personal data.*” See also *Checklista för kommuner och landsting – Webbpublicering av protokoll och diarier*.

¹⁰ Also to be noticed is that online publishing of information and documents doesn’t fall into the scope of protection of the Fundamental Law on Freedom of Expression (1991:1469). Public authorities which have invoked been in possession of a so called *certificate of publication* and therefore benefiting, thanks to the database rule, of the constitutional protection of the Fundamental Law on Freedom of Expression, have been denied this protection by the Swedish Data Protection Authority. For example, in a decision regarding the publication by the municipality of Trelleborg of personal data related to students expelled from a upper secondary school, the supervisory authority explicitly mentioned that a certificate of publication for a website “*does not constitute an obstacle for the application of the Personal Data Act (in the present case)*”. In a com-

The legal framework applicable to online proactive disclosure, i.e. the pertinent data protection rules, has evolved over time. All online proactive disclosure that took place between 1998, the year of the entering into force of the Personal Data Act, and 2001 fell into the scope of the entire and rather burdensome Personal Data Act shaped according to the regulatory model.¹¹ However, two consecutives, but not directly correlated, changes in the data protection legislation have successively added lightened regimes.¹² First, the introduction, by the Government, in 2001 of a new provision in the Personal Data Ordinance has impacted proactive disclosure of certain kinds of documents carried out by local authorities. Indeed, publication of personal data in minutes and registers stemming from municipalities and County Councils have been exempted from the prohibition laid down in the Personal Data Act to transfer personal data to third countries. Second, in 2007, an amendment of the Personal Data Act, introducing the concept of *processing of personal data in unstructured material*, has potentially had an impact on all kinds of data processing, including online proactive disclosure, exempting data processings that are to be regarded as such processings, from the majority of the provisions of the Personal Data Act, and submitted these processings to a lightened set of rules with focus on preventive abuse of personal data, the so called abuse centred model.

The three applicable regimes will be presented further and be illustrated by cases handled by the Swedish instance in charge of monitoring the compliance with data protection legislation, the Datainspektion.¹³ The deci-

prehensive reasoning the Datainspektion explains its position in arguing that "*the municipality [which published on its website minutes containing decisions in a case where exercise of power is involved] should, under these circumstances be considered to represent the State (det allmänna). The Data Protection Authority assesses therefore that the provisions of the Fundamental Law, aiming at protecting the freedom of expression of the individuals, can not be invoked by the municipality in the present case in order to escape legal obligations, in particular when the obligations – as in the present case – exist in favor of individuals*". Decision 2010-01-29, Case n° 987-2009 Tillsyn enligt personuppgiftslagen (1998:204) – angående publicering av personuppgifter på Internet.). For further information on the system of certificate of publication see Inger Österdahl *Between 250 years of free information and 20 years of EU and Internet, Etik i praksis*, 2016, Vol.10(1), pp.27–44.

¹¹ *Hanteringsmodell* in Swedish.

¹² In the second section of this paper, dedicated to the findings, we describe the successive "shapes" of the legal framework as some kind of "layers".

¹³ It happens that the Parliamentary Ombudsman is involved in this type of cases. It seems then it then relies for its appreciation of the lawfulness or not of the online publication subject to a complaint, to the reasoning made by the Data Protection Authority. It has

sions of the Datainspektion that have been selected for analysis illustrate a large spectrum of decisions: besides illustrating the different stages/shapes of the applicable legislation, the decisions also mirror the diversity of the public actors involved in proactive disclosure, i.e. national agencies/institutions, municipalities and County Councils. The focus of the analysis is for each of the selected decisions how the Swedish monitoring authority, the Datainspektion, deals with the balance to be drawn between the need to protect privacy and the need for openness.

1.1. The regulatory model and its application

Being a processing according to the definition contained in the data protection legislation, the online publication of personal data in documents published on public authorities' websites is subject to the rules of the data protection legislation, i.e. a set of rules aimed at protecting the privacy of the data subject. Indeed, the Personal Data Act (1998:204), issued 29 April 1998, aims to "*protect people against the violation of their personal integrity by processing of personal data*" (Section 1).

As the Data Protection Directive 95/46/EC on which it is based, the Swedish Act contains for that purpose a number of requirements the controller of the processing of personal data must fulfil as well as prohibitions that he/she has to comply with.

They are for instance the *fundamental requirements for processing of personal data* laid down in Section 9 regarding the quality of the data: the data have *inter alia* to be processed lawfully; be collected for specific, explicitly stated and justified purposes, and not have been processed in a way incompatible with those purposes.¹⁴ The prohibitions relate to the proces-

been the case in the decision 2011-03-04, case n°3684-2009, where a County Council had been criticised for having published on its website, before a meeting, reasoned opinions containing personal data. In the current case the Ombudsman, after having examined the incriminated publication of personal data - related to a person been in a psychiatric clinic - in the light of the secrecy legislation, assessed that the publication also had to be appreciated in relation to the Personal Data Act. The Ombudsman, referring to and reproducing a decision taken by the Data Protection Authority concerning a similar case, embraced the conclusion of the Datainspektion, i.e. that the County Council in the current case had, through the publication, processed personal data in breach of the Personal Data Act.

¹⁴ Additionnally, the data must be processed in accordance with the principle of accuracy, as they have to be adequate and relevant and not excessive in relation to the purpose of the processing. The data must furthermore be correct and, if necessary, up to date and not be

sing of sensitive personal data (Section 13), the processing of information concerning legal offences (Section 21) and to the transfer of personal data to a third country¹⁵ (Section 33).

More interesting for the current study are the requirements regarding the legitimization of the processing of personal data, since the Datainspektion has focused its reasoning on these requirements when it has handled cases of online proactive disclosure. These requirements are to be found under the heading “When processing of personal data is permitted” (Section 10). As a general rule, the processing is permitted when the data subject has *consented* to the processing. However, the Personal Data Act, just as the Directive does, also allows data processing for other grounds exhaustively listed in Section 10, one of them being “*when a purpose that concerns a legitimate interest of the controller or of a third party to whom personal data is provided should be able to be satisfied, if this interest is of greater weight than the interest of the registered person in protection against violation of privacy*” (Section 10 f).¹⁶

This ground, that is at the front when it concerns the determination on whether online publication of documents containing personal data is lawful or not, entails a balancing of interests: online publication of documents containing personal data may be considered as lawful if the legitimate interest of the public authority (the data controller) or third party (generally the public) to disclose or to have access to information, outweighs the interest of the persons whose personal data are contained in the published documents to have her/his privacy protected.

This provision, as the rest of the Swedish Personal Data Act, originates from the Data Protection Directive. A look to the Swedish preparatory works leading to the implementation of the Directive shows that they are not particularly enlightening on the question of the balancing of interests. The preparatory works mention however that the Datainspektion may have

kept for longer than necessary, having regard to the purpose of the processing.

¹⁵ With *third country* means country which is not a member of the EU or the EEA.

¹⁶ See the translate Personal data Act <http://www.wipo.int/edocs/lexdocs/laws/en/se/se097en.pdf>. The other legal grounds are the following: to enable a performance of a contract; when the controller should be able to comply with a legal obligation ; when the vital interests of the registered person should be protected ; when a work task of public interest should be performed or when the controller or a third party to whom the personal data is provided should be able to perform a work task in conjunction with the exercise of official authority.

a responsibility for providing data controllers with recommendations and guidelines about the balance of interests.¹⁷ This has been done by the Data Protection Authority which has for example published a handbook tackling the issue of balancing of interests in a general manner.¹⁸

How the Datainspektion carries out the balancing in practice within the application of the regulatory model can be illustrated by a decision from **September 8, 2004**.¹⁹ The decision concerns the planned publication on the website of a municipal committee in charge of environmental matters²⁰ of “project reports” that was meant to contain pictures and the names of pizzerias criticized for having an unsatisfactory level of hygiene.

The Datainspektion begins its analysis of the case noticing that the names of the pizzerias constitute indirect personal data when these pizzerias are individual firms/registered as sole proprietors, and assesses that the Personal Data Act is therefore applicable. The Data Protection Authority then reminds that the general rule for the legitimization of processing of personal data is, according to the data protection legislation, the consent, but points out that the processing might be lawful in other situations, *inter alia* when the interests of the data controller to publish personal data outweigh the interest of the persons concerned to be protected against privacy infringements that the publication may lead to.²¹

This was the case according to the Datainspektion which, in appreciating the interests involved and their balance, takes into account that the personal data processed are only indirect personal data (such as the name of the pizzerias) and that the interests that the data become publicly known is high. The monitoring authority concludes that the processing has to be seen as permitted. The interest of openness is, after a balancing of interests, in this case appreciated as outweighing the need of protection for privacy.

1.2 The specific rule regarding the transfer of personal data to third countries and its application

As mentioned above, the Swedish Government introduced in 2001 in the Personal Data Ordinance (1998:1191)²², a provision tailor-made to create a

¹⁷ See SOU 1997:39 *Integritet, Offentlighet, Informationsteknik*, p. 363.

¹⁸ ”*Interesseavvägning enligt personuppgiftslagen. Datainspektionen informerar*”.

¹⁹ Case n°54-2004.

²⁰ Miljökontoret in Jönköping.

²¹ Decision 2004-09-08, case n°54-2004., p.2.

²² The Ordinance contains supplementary rules to the Personal Data Act.

lighter regime for local public authorities publishing personal information on the Internet. Indeed Section 12 of the Ordinance, under the heading “Transfer of personal data to third country”²³ states that municipalities and County Councils are allowed to transfer personal data when these data are included in “*registers (diarier), a notice to a meeting with the members of the council or with a [municipal] committee, a notification about meetings with members of the council or agreed minutes of the meeting with members of the council or a committee*”.

According to Section 12.2, personal data which in a direct manner point out the person registered shall not be subject to a transfer. There are exceptions when personal data concern elected representatives carrying out their mandates. The prohibition to transfer personal data to third countries also does not apply if the cumulative conditions set out in Section 12.2 are met, i.e. (1) “*other personal data related to the persons registered are not the ones encompassed by Section 13 (sensitive data) nor by Section 21 (data about criminal offences) of the Personal Data Act*” and (2) “*there is no ground for considering that there are risks that privacy of the persons registered been infringed through the transfer*”. In any case, the unfailing identifiers constituted by the personal number (*personnummer*) and by the co-ordination number (*samordningsnummer*²⁴) may never be subject to a transfer (Section 12.3).

Section 12 which, according to the Datainspektion²⁵, “*makes it easier*” for the local authorities to publish personal data on the Internet, could correspond to an endeavour to take into account the attitude of openness of the local politicians and civil servants and their wish to, by means of giving access to information regarding the issues of importance for the local community, promote the participation of the public.

One may say that by means of Section 12 of the Personal Data Ordinance and in determining the conditions for the legal publication of personal data,

²³ From the very beginning the provision was introduced in Section 11 (SFS 2000:1055; entered into force January 1st, 2001). The number of the Section changed to 12 from October 1st 2001 (SFS 2001:582).

²⁴ Which is an identification number for people who are not or have not been registered in Sweden. The purpose of the co-ordination number is to allow *inter alia* public authorities to identify people even when they are not registered.

²⁵ The provision “*underlättar för kommuner att publicera personuppgifter på Internet*” states the Datainspektion in a report dedicated to processing of personal data by municipal committees of social affairs and Environmental affairs, *Behandling av personuppgifter hos social- och miljöförvaltningen. Datainspektionens rapport 2004:1*, p. 22.

the Government itself has carried out the balancing between the interest of the public to access information and the need to protect privacy. The position statement of the Government – author of the reform – is reflected in the kinds of documents selected to benefit from the lightened regime. Indeed, the categories of documents selected for falling into the scope of the specific regime are the very ones which may inform the citizens on what is going on in the local communities (municipalities and County Councils). They are the kinds of documents to which access may provide the citizens with the possibility to monitor the compliance of the actions of the local decisions makers with the law, and may improve public participation.

The position statement is furthermore illustrated by the distinction made by the government between processing of personal data regarding politicians (data concerning elected representatives carrying out their mandates) on one hand, and processing of personal data regarding the other persons, on the other hand. For the former, the interest in privacy actually disappears for the benefit of openness. The result of the balance of interests is already stated in the law. For the latter, the legislator lays down the criteria that makes it possible to decide if the transfer is allowed or not. One of them requires nonetheless the appreciation *in concreto* of the situation, the appreciation whether or not “*there are risks that the privacy of the person registered would be infringed through the transfer*”.²⁶ No mention is explicitly made of a balance of interests however.

A decision from July 2008 may give an idea as to the application of Section 12 of the Personal Data Ordinance and shed light on the balancing of interests the Datainspektion actually carries out when applying this provision. The decision, from **3 July 2008**²⁷, concerns the online publication of personal information by the County Council of Sörmland. The personal data, the publication of which was challenged, consist of the name, the title, the private e-mail address and the private cell phone number of a person who had lodged a complaint to the Parliamentary Ombudsman against the County Council. The complaint was in fact attached to minutes stemming from the committee for Health and Medical Care and published on the website of the County Council. The data subject was particularly worried about the online publication of his personal data as he was working at a psy-

²⁶ We will come back to this “appreciation” further on, under Section 2.

²⁷ Case n° 788-2008.

chiatric hospital in a department taking care of patients suffering from serious psychic disorders.

Like the County Council against which the complaint was lodged, the Datainspektion, although implicitly, considers that the documents at stake in the case fall into the scope of the special regime set out in Section 12 of the Personal Data Ordinance. The Datainspektion further assesses that the publication does not touch upon sensible data, nor upon data about legal offences, i.e. the kind of data that the Ordinance excludes from the field of application of the lightened legal regime. The Data Protection Authority nevertheless considered that the County Council had published data that point out an individual in a direct manner, because of the complaint the individual had lodged to the Ombudsman. The Supervisory authority and the County Council do not agree on the question of the existence of risks for privacy infringements potentially stemming from the transfer of data/the publication. The assumption of the County Council that it has been no risk for privacy infringement is primarily based on the fact that the personal data in the case were contained in a complaint to the Ombudsman, a document which was accessible to the public (*offentlig*). The Datainspektion emphasises, on the contrary, that the current publication on the Internet leads to risks of privacy infringements and concludes that the publication is therefore not allowed. The arguments related to the interests of having the current personal data published on the Internet are particularly interesting and show that both the County Council and the Datainspektion entered into the field of balancing, although the legislator has not expressly invited the concerned actors to it. Indeed, the County Council for its defense put forward the fact that the publication was aimed to inform the members of the County Council about the activities of the Health and Medical Care Committee, while the Datainspektion counterattacks stating that the interest in having the name and the private numbers of the person published on the Internet (the website of the County Council) is very low. The Datainspektion bases nevertheless its conclusion on the criteria posed by the Ordinance, the question of the risks of infringements of privacy due to the transfer/the publication, and concludes that the processing could not be allowed.

1.3 The introduction of a lightened regime, the abuse centred model and its application

Six years after the introduction in the Personal Data Ordinance of specific rules for the publication by local authorities of personal data in minutes and registers, the Personal Data Act has also been subject to a reform, due to the enactment of a new provision, Section 5a.²⁸ This general reform, aimed at simplifying compliance to the data protection legislation for all kinds of data controllers, actually entails “en passant” a lighter regime for public authorities publishing personal data on the Internet.

The reform consisted in supplementing the traditional regulatory model (*hanteringsmodell*²⁹), which lays down every step in the processing of personal data, by an abuse centred model (*missbruksmodell*) which focuses on the use of personal data being considered as an abuse.³⁰ So, when processing of personal data may be considered being a processing in *unstructured material*, the majority of the provisions of the Personal Data Act, including *inter alia* Section 10 on the conditions of legitimation of the processing³¹, Section 13 on sensitive data, Section 21 on legal offences and Section 33 on transfer to third countries, do not need to be applied. Nevertheless, the processing of personal data in unstructured material shall not occur “if it entails an infringement of the privacy of the person concerned” (Section 5a *in fine*).

What is a processing of personal data in unstructured material? According to the definition contained in Section 5a of the Personal Data Act, it consists of “processing of personal data which is not included nor intended to be included in a collection of personal data which has been structured in order of facilitating the search or the compilation of personal data”. This encompasses *inter alia* running text published on the Internet, which for instance, the minutes of local authorities generally are.³²

²⁸ SFS 2006:398, entered into force on January 1st, 2007.

²⁹ See SOU 1997:39, *Integritet, Offentlighet, Informationsteknik* p.p. 179 and Prop. 1997/98: 44 *Personuppgiftslag*, p.p. 36.

³⁰ Prop. 2005/06:173 *Översyn av personuppgiftslagen*, p. 12.

³¹ “When processing of personal data is permitted”.

³² See the examples given in the next section. Nevertheless, “If material, for instance the running text, be included in a database with a structure based on personal data, as for instance a case management system, the rules from the regulatory model then apply”. Prop. 2005/06, *Översyn av personuppgiftslagen*, p.59.

The fact that personal data can be searched by means of search engine (such as Google) and linked with other personal data does not entail the character of processing of personal data in *unstructured material* on postings made on the Internet.³³

The preparatory works give some elements for appreciating whether or not the processing in unstructured material entails a privacy infringement. According to these preparatory works the appreciation “*shall not be made on a flat rate basis (schablonartat) but has to also have its point of departure in for instance the context in which the personal data appear, the purpose they are processed for, the dissemination that has occurred or the risk for dissemination and what the processing may lead to*”.³⁴ The preparatory works mention furthermore that should also be taken into consideration the fact that what can be experienced as a violation for a certain person or in a certain context does not need to be experienced the same by another person or in another context.³⁵

The legislator touches moreover upon the question of the balancing of interests, pointing out that “*by its very nature the application of a provision such as the one proposed may (får) build on the balance of interests in which the interest of the person concerned to have a private sphere is balanced against contrary interests in the concrete case*”.³⁶

Three decisions taken by the Datainspektion after the introduction of the abuse centred model in the Personal Data Act will be analysed here. The two first decisions illustrate cases where online publication of personal data by *local authorities* was in focus, while the third and last decision concerns

³³ See the judgment of the Swedish Supreme Court (NJA 2013 s. 1046). The case concerned the publication of a judgment containing the name of the defendant on the website of a debt collection agency (incasso). While the first court (tingsrätten) considered that as the personal data of the defendant that were contained in the published judgment were searchable on the Internet with the search engine Google which links to the website of the agency where the judgment was published, the personal data were to be considered as related to an identified person. The personal data were therefore to *be considered as included in a structure based on personal data*. This interpretation of Section 5a of the Personal Data Act was not accepted by the Court of Appeal (Hovrätten) nor by the Supreme Court (Högsta domstolen) who both perceived the processing in question as a processing falling into the scope of the abuse centred model.

³⁴ Prop. 2005/06:173, p. 59.

³⁵ *Idid.*

³⁶ Prop. 2005/06:173, p. 27. We will come back to this point further on under the second section of this paper.

online disclosure of information by a *national institution*, in the current case the Parliamentary Ombudsman.

In the first decision of the Datainspektion from **January 29, 2010**³⁷, the issue at stake is the publication on the website of the municipality of Trelleborg of minutes containing a decision of the committee for high school and adult education to expulse two students from an upper secondary school. The Datainspektion, which considers that the publication is deemed to be a processing falling into the scope of Section 5a of the Personal Data Act, concludes, after having carried out a balancing of the interests at stake, that a violation of Section 5a of the Personal Data Act has taken place. The supervisory authority, which refers to the fact that the appreciation of privacy infringement shall not be made on a flat rate basis³⁸, takes especially into account that information about expulsion may be particularly sensible for the students concerned and for their relatives. The Data Protection Authority mentions that the information may have negative consequences when the students will search for employment or education, and it also emphasises the fact that the risk for dissemination of the data has been high since the data have been searchable by means of search engines. The Datainspektion also assesses that personal data “*in this context may be considered to have a limited interest for the municipality and the public*”, and further considers that the interests for the municipality and for the public “*may be satisfied without naming the students with name and dates of birth*”.³⁹

In the second decision, from **April 7, 2010**⁴⁰, the criticised proactive disclosure consisted of two cases of publication of personal information in minutes posted on the website of the County Council of Sörmland.⁴¹

The first case concerns the online publication of a reasoned opinion of the County Council in a court case regarding co-payments for heavy medi-

³⁷ Case n° 987-2009 Tillsyn enligt personuppgiftslagen (1998:204) – angående publicering av personuppgifter på Internet. It is the decision mentioned earlier (footnote 10) in which the Datainspektion rejected the argument of the public authority from having the publication on its website protected by a certificate of publication.

³⁸ Case n° 987-2009, p. 6.

³⁹ Id., p. 7.

⁴⁰ Case n° 119-2010 Tillsyn enligt personuppgiftslagen (1998:204).

⁴¹ There is a connection between this case and the case we analysed previously (2008-07-03, case n°788-2008) on the basis of Section 12 of the Personal Data Ordinance. In fact the County Council of Sörmland did published again the personal data it was supposed to take away from its website. See footnote 27.

cal treatments. The reasoned opinion contains the name of the spouse of a patient suffering from a serious disease. Her surname is quite unusual and the information constitutes, according to the Data Protection Authority, sensitive personal data related to health in the sense of Section 13 of the Personal Data Act,

The second case concerns the online publication of a reasoned opinion from the County Council addressed to the Parliamentary Ombudsman after a complaint against the County Council made by an individual. It appears from the incriminated minutes that the individual named in the reasoned opinion had requested access to its journal from a center for addicted persons of a psychiatric clinic. Again, the information that a person has been the patient of a health institution constitutes, according to the Data Protection Authority, sensitive data related to health.

After having established that these publications constitute a processing of personal data in unstructured material regulated by the abuse centred model and that the prohibition to process sensitive data as laid down in Section 13 of the Personal data Act is therefore not applicable in the current cases, the Datainspektion nevertheless assesses that the publication of such sensitive personal information on the Internet may lead to an infringement of privacy as prohibited by Section 5a of the Personal Data Act. The Datainspektion refers to the fact that the appreciation has not to be made on a flat rate basis.⁴² The Data Protection Authority also emphasises that the attitude of the person concerned vis a vis the processing may be of importance for the determination of the privacy infringement, and uses the wordings of the preparatory works to explain that what constitutes a privacy infringement may differ between persons as well as between contexts. When carrying out the balancing between the interest of the County Council to render its activities transparent, and the interest of the protection of privacy, the Data Protection Authority considers that the interest of the person concerned “*significantly outweighs*” the interest of the County Council in both cases.⁴³

The third and last decision analysed here illustrates online publication of personal data performed by a *state authority*. The decision from **October 5, 2010**⁴⁴ concerns a plaintiff who had brought a complaint to the Parlia-

⁴² Case n° 119-2010, p. 4.

⁴³ Id., p. 5.

⁴⁴ Case n° 663-2010.

mentary Ombudsman and whose name has subsequently been published in the case law database located on the website of the Parliamentary Ombudsman. After concluding, with some reluctance⁴⁵, that the abuse centred regime was applicable in the current case, the Datainspektion carries out a balancing of the concrete interests at stake, referring to the non-flat-rate rule set out in the preparatory works. In fact, the Datainspektion does not only examine the balance of interests in the current case but also investigates more generally the balance of interests concerned by the publication of the name of the plaintiffs in the online database as well as the lawfulness of the publication in the online database of the name of the civil servants involved in cases handled by the Parliamentary Ombudsman. Interestingly, the Datainspektion refers to the fact that the applicable provisions (from the Personal Data Act) have their origin in the European Data Protection Directive, and emphasises that the balance of interests to be made cannot be based on an interpretation that contradicts the fundamental rights protected by the European Union such as the right to private life guaranteed by Article 8 of the European Convention of Human Rights (ECHR).⁴⁶ Additionally, as if to give more weight to its arguments, the Data Protection Authority mentions the need to respect the principle of proportionality contained both in the Data Protection Directive and in the ECHR, and concludes that the balance of interests laid down by the Swedish legislator contains a similar proportionality assessment.⁴⁷ Within the balancing, the Datainspektion takes into account the increasing risks for privacy infringements stemming, in particular, from the publication of personal data on the Internet.⁴⁸ Moreover, the Data Protection Authority assesses that the very fact that a person has made a complaint to the Ombudsman may lead to complications for the plaintiff (when searching employment for instance) and that the publication of such information may in turn lead to the unwillingness to make complaints. Against the arguments raised by the Parliamentary Ombudsman, i.e. that the online publication of the names of the civil servants involved in the cases was a transparency measure, the Data-

⁴⁵ According to the Datainspektion "it may be questioned if the legislator had in mind to make the abuse centred regime applicable to the kind of processing at stake when the Parliamentary Ombudsman make its case law database accessible on Internet", case n° 663-2010, p. 3.

⁴⁶ Case n°663-2010, p. 4.

⁴⁷ Id., p. 5.

⁴⁸ Id., p. 6.

inspektion⁴⁹ uses the arguments that the transparency goals the Ombudsman aims to achieve may be satisfied also if the name of the civil servant is taken away from the decision.

The Datainspektion concludes that in a general manner, as well as in the current case (regarding the issue of the plaintiff), the publication of names in the case law database accessible on the website of the Ombudsman should not be seen as permitted on the basis of the abuse centred model. The Datainspektion is, moreover, of the opinion that a legal instrument is needed for permitting this kind of online proactive disclosure.⁵⁰

2. Summary and findings

From the analysis above we may now make some reflections on three questions: the relationship between the different legal regimes regulating online publication by public authorities (2.1), the basis for the balancing of interests (2.2) and the balancing of interests itself (2.3).

2.1 The relationship between the legal regimes regulating online publication

As we could notice above, the legal framework has changed over time, or, more correctly, it has got more layers over time. The regulatory model that has been applicable since the entering into force of the Personal Data Act in 1998, has been applicable to online publication of personal data also after the introduction of the abuse centred regime in 2007. Indeed, when the disclosure of data takes the shape of processing of personal data in *structured material*, the whole set of rules laid down in the Personal Data Act are applicable on the processing. As an example, the set-up on the website of a municipality of a search function enabling the citizens to get information about food establishments having been subject to public monitoring, is subject to the all obligations laid down by the Personal Data Act. Indeed, according to a statement of the Datainspektion dated 2015 this kind of processing has to be considered as a processing in structured material.⁵¹ In this case, Section 10 f) of the Personal Data Act should be the legal basis

⁴⁹ Id., p. 6.

⁵⁰ Id., p. 10.

⁵¹ The search function been deemed to obtain specific information from a cases management system (ärendesystem).

permitting the processing of the data – as it was the case in the Datainspektion's decision from 2004 illustrating the regulatory regime, where the names of pizzerias were involved.⁵² For the processing to be lawful, it is also required that the other conditions posed by the Act are fulfilled, not least the conditions regarding the quality of the data processing. In the case mentioned here concerning the search function for accessing information on food establishments, the Datainspektion expresses nevertheless doubts on the compliance of the processing with the *fundamental requirements for processing of personal data* laid down in Section 9. Indeed, according to the Data Protection Authority *"taking into consideration the purpose of the processing, i.e. to satisfy the need of the public to have access to the results of the controls, it is high doubtful if the accessibility of the data related to controls that occurs for many years ago may be considered as motivated"*. The Datainspektion also concludes that it can be highly doubtful too if the balancing of interests may give support for such a long reaching processing of personal data.

The regulatory regime is thus still applicable for online proactive disclosure on the basis of Section 10 f), but in practice it is not used that much as online publication of documents and data are often qualified as unstructured material and falls into the scope of Section 5a of the Personal Data Act and its abuse centred regime.

The relationship between Section 12 of the Data Personal Ordinance (as introduced 2001) and the other regimes, not least to the abuse centred regime, is less clear, however.

First the introduction of the new Section 12 in the Personal Data Ordinance is quite perplexing. Indeed, the provision that seems to have been introduced – as the heading of the new provision ("Transfer of personal data to third country") and its wordings reflect – as a means for circumventing the prohibition to transfer data to third countries, was actually introduced before the clarification made by the European Court of Justice in the case Bodil Lindqvist. In its judgement from November 6, 2003, the European Court gave an interpretation of Article 25 of the Data Protection Directive on the prohibition to transfer personal data to third countries, being of the opinion that there is no transfer of data to third countries when personal data are published on a website which is stored with a hosting provider established within the EU. Nevertheless the Datainspektion has

⁵² See above under 1.2., the case n° 788-2008.

claimed that “*although this provision is, according to its wording, about exemptions from the prohibition to transfer personal data as laid down in the Personal Data Act Section 33, the very purpose of the provision was to regulate under what conditions the municipalities and County Councils may (får) publish registers, minutes etc. on the Internet*”.⁵³

When we turn to the application of Section 12 of the Ordinance, we can conclude from the decisions of the Datainspektion we have analysed that this provision is rarely applied as a self-standing and self-sufficient legal basis. It was the case in the decision from September 3, 2008, that we used to illustrate the application of Section 12. In this decision Section 12 of the Personal data Ordinance was the only provision discussed by the Datainspektion as the legal basis permitting the publication on the Internet.⁵⁴ In the decisions we analysed and that were taken later, the Datainspektion uses Section 12 of the Ordinance only as a benchmark for appreciating the case and not as a self-standing legal basis. Indeed, the Datainspektion assesses that the provision “*may give guidelines for what has to be considered as an infringement according to the abuse centred rule*”.⁵⁵

Instead of being a self-sufficient basis for allowing publication, Section 12 of the Ordinance is thus primarily to be regarded as an interpretation tool for the application of another provision, namely Section 5a of the Personal Data Act.

We can also notice that the guidelines drafted by the Datainspektion with the purpose to help the local authorities to comply with the data protection legislation when they publish minutes and registers on their websites⁵⁶, have integrated the requirements posed by its 12th Section, however without explicitly referring to the Personal Data Ordinance itself.⁵⁷

⁵³ Decision 2010-04-07 case n°119-2010 Tillsyn enligt personuppgiftslagen (1998:204) – angående publicering av personuppgifter på Internet, p. 4.

⁵⁴ We may also notice that the Datainspektion never uses the expression *transfer to third country* but employs the term *publication*.

⁵⁵ See case n°119-2010, p. 4 and case n°987-2009 p. 7.

⁵⁶ The Datainspektion has indeed drafted Guidelines/a checklist after having 2011 monitored about 50 municipalities (*kommunstyrelsen* – Municipal executive boards), which represent about 1/6 of the total of the Swedish municipalities. Through the survey the Swedish Data Protection Authority could assess that all the municipalities published minutes on their website, that about 15 of them also published registers (*diarier*) and that all the municipalities published personal data. Moreover through verifications at random the Datainspektion discovered that personal data were processed in breach of the Personal Data Act. These observations have led the Datainspektion to draw up a checklist addressed

As we can see, the legal framework that may apply to online publication of personal data – especially when proactive disclosure is performed by local authorities – is not easy to comprehend.

2.2 The basis for the balance of interests

When personal data is subject to online proactive disclosure by public authorities, the question of the balancing of the interests of transparency and the interests for protecting privacy is always raised, whatever the legal regime applicable for determining the lawfulness of the processing. The ground or basis for the balancing varies however depending on the regime.

As for the regulatory model, the requirement to carry out a balancing is contained in the law itself. Indeed, Section 10 f) of the Personal Data Act states that a processing is lawful *“when a purpose that concerns a legitimate interest of the controller or of a third party to whom personal data is provided should be able to be satisfied, if this interest is of greater weight than the interest of the registered person in protection against violation of privacy”*.

The balance of interests is thus constitutive of the legal ground that has to be in place in order for the processing to be permitted. This provision derives from the Data Protection Directive. The Swedish preparatory works, which focused on how the Data Protection Directive had to be transposed in the Swedish legal system, do not, as we mentioned before, contain information of proper interests for carrying out the balancing.⁵⁸

As for the balancing that has to be made in the frame of the application of Section 5a of the Personal Data Act in the context of the abuse centred model, the requirement to carry out a balance of interests is not laid down in the law but in the preparatory works as we mentioned above. And these are generous in giving information for the carrying out of the balance, at least when giving guidelines and examples of how to determine if a privacy infringement occurs.⁵⁹ In any case, the legislator states that *“it is in the last instance a question for the application of the law to, in each case, take into*

to the municipalities and the County Councils - *Checklista för kommuner och landsting – Webbpublicering av protokoll och diaries*.

⁵⁷ See p. 2 and 3 of these guidelines *Checklista för kommuner och landsting – Webbpublicering av protokoll och diaries*

⁵⁸ Furthermore, it seems that the majority, if not all of the examples used in order to illustrate how to understand and implement the rules concern the private sector. See SOU 1997:39, p. 363.

⁵⁹ See Prop. 2005/06:173, p.p.26-29.

*account all circumstances, to balance the privacy infringement of the data subject against potential contrary interests”.*⁶⁰

Regarding the special regime provided by Section 12 of the Personal Data Ordinance governing online proactive disclosure of minutes and registers performed by local authorities, the legislator (the government in this case) has itself made a statement on the balance of the interest to promote transparency of the local public authorities carrying out proactive disclosure on the one hand, and the interest to protect privacy of the data subject on the other hand.⁶¹ When it comes to the *application* of this regime, i.e. the application of Section 12 of the Personal Data Ordinance, if we consider that there is a balancing of interests to be carried out in the concrete cases, this should appear when it comes to appreciate that *“there is no ground for considering that there are risks that the privacy of the data subject been infringed through the transfer”*. In fact, we have no knowledge about how the legislator has reasoned when it concerns the application of Section 12 of the Personal Data Ordinance and if the appreciation has to be based on a balancing of interests. At the same time, Section 12.2 of the Personal Data Ordinance has large similarities with Section 5a of the Personal Data Act whose application, as we saw before, is built *“by nature”* on the carrying out of a balance of interests. In the decision taken for illustrating the application of Section 12 of the Personal Data Ordinance, we noticed that such a balance was carried out in practice.⁶²

The Guidelines of the Datainspektion addressed to municipalities and County Councils are not so explicit concerning the balancing. They only state that *“For the publication of other personal data [i.e. other than data that directly point out an individual] a so called balance of interests has to be carried out in the concrete case”*.⁶³

In fact, the function of the balance of interests varies: in the context of the regulatory regime (Section 10 f) of the Personal Data Act) the outcome of the balance of interests is aimed to give an answer to the question of whether or not there is a ground for the processing.

⁶⁰ [D]et är i slutändan en fråga för rättstillämpningen att i varje enskilt fall, med beaktande av samtliga omständigheter, väga det intrång som kan ha skett i den personliga integriteten mot eventuella motstående intressen, Prop. 2005/06:173, s. 29.

⁶¹ See above under 1.2.

⁶² I.e. case n° 788-2008, see under 1.2 above.

⁶³ *Checklista för kommuner och landsting– Webbpublicering av protokoll och diarier*, p. 3.

In the context of the abuse centred model (Section 5a of the Personal Data Act) as well as when it comes to the special regime put in place for proactive disclosure of minutes and registers by local authorities (Section 12 of the Personal Data Ordinance), the balance of interests gives an answer to the question if there is a privacy infringement/a risk for privacy infringement or not which, in turn, gives an answer to whether or not the processing is permitted.

2.3 The balance of interests itself

The lawfulness of online publication of personal data is dependent on the outcome of the balance between the interest of privacy of the data subject and other interests. Two questions related to the issue of the balance of interests caught our particular attention: the question of whose interests are balanced against the interest of the data subject, and the question of taking into account the specific dangers for privacy that publication on the Internet generate.

Whose interests have been taken into account in the balance of interests?

The way the interests to be taken into account in the balance is formulated appears to differ between the regimes. However, it seems that the interests encompassed in practice when it is about online publication by public authorities are the same, at least in the context of the application of Section 10f) and Section 5a of the Personal Data Act.

Concerning Section 10 f) of the Personal Data Act, the wordings refer to the legitimate interest of *the controller or of a third party to whom personal data is provided*. In the context of online publication of documents, it means principally the interest of the public authorities publishing the data and the interest of the public to receive information.

In the preparatory works explaining the balancing to be made when Section 5a of the Personal Data Act is applicable, the legislator mentions the balancing of the interest of the data subject against “*contrary interests in the concrete case*”.⁶⁴ The range of interests is wider in this case. In the meantime, when it is about online publication of personal data, the “contrary interests” at stake should reasonably be the interests of the public authority to

⁶⁴ Prop. 2005/06:173, p. 27.

perform the publication as well as the interests of the public to receive the information.

In summary, the interests that may be put in the balance are all related to the need for transparency: the need of the public authorities to be transparent and inform the citizens on what's is going on; the need for the public to have access to information, in order to control public actions and/or to participate in the decision making process.

There is no mentioning of a balancing of interests in Section 12 of the Personal Data Ordinance, and we do not know if the question has been tackled in the "preparatory works". However, when applied in the decision of 2008, the public interests to have access to the published information was brought to the fore.⁶⁵

We may say some words on the need of *transparency for the sake of the persons having a political mandate* - i.e. the need for them who participate in the formal decision making process to have access to information by on-line publication - argument sometimes used by the public authorities having published personal data online⁶⁶, is an interest worth to be taken into consideration. It seems to us that publishing information with the purpose to inform the political representatives by means of the website is of more practical character than "ideological" if we may say so. The website is used in this case as an electronic notice board. It can be questioned if there is a need to publish the information world-wide then, and if it not sufficient to publish the information on the intranet of the public authority. It seems to us that this interest has therefore less dignity than the other two above-mentioned interests. We may further notice that this kind of interest has not been paid any particular attention by the Datainspektion.

For their part the two interests more directly connected to the ideal of transparency, the interest of the public authorities to inform (an active kind of transparency, we could say) and the interest for the public to be informed (a passive kind of transparency) are abundantly referred to by the Data-

⁶⁵ Case 788-2008, p. 2.

⁶⁶ See for example in a decision of the Datainspektion from March 9, 2010, Case n°1857-2009, where the County Council of Dalarna justified the online publishing of the meeting documents (*möteshandlingar*) containing the criticised personal data by the wish to ensure the general public's insight as well as for facilitating the dissemination of the documents to the members of the County Council.

inspektion. Sometimes separately, sometimes together, and sometimes with other elements more or less related to transparency.

In the decision of April 7, 2010, concerning information related to an individual's health status and information related to the contacts taken by an individual with a centre for addicted persons, information that were contained in complaints lodged to the court and to the Parliamentary Ombudsman respectively, the Datainspektion only refers to the *interest of the County Council* – the public authority criticised for having published personal data online – to give the public insight into its activities. This corresponds to what is set out in the Guidelines of the Datainspektion addressed to local authorities: the Data Protection Authority only mentions the “*interest of the municipality or of the County Council to publish personal data*”.⁶⁷

In one of the decisions analysed, only *the interest of the public* has been mentioned. The decision in question is the one dated July 3, 2008, in which the Datainspektion made an application of Section 12 of the Personal Data Ordinance. The Data Protection authority did not expressly mention a balance of interests but assessed that “*the interest that the name and the private cell phone number will be accessible to the public knowledge through the publication on the Internet has to be considered as relatively low*”.⁶⁸

In two of the decisions analysed, both *the interest of the public authority* and *the interest of the public* have been taken into account by the Datainspektion. In the decision of January 29, 2010 concerning personal data on expelled students, the Data Protection Authority referred to the “*interests of the municipality and the public*” for being informed of the case.⁶⁹ In the decision of September 8, 2004 concerning data related to pizzerias, the Data Protection Authority stated that for the processing being permitted “*the interest of the data controller for the publication has to outweigh the interest of the data subject to be protected against the privacy infringement the publication may lead to*”⁷⁰ adding that “*moreover it should be taken into account that the interest that the current data are accessible to the public (kommer till allmän kännedom) may be considered as high*”.⁷¹

⁶⁷ Checklista för kommuner och landsting– Webbpublicering av protokoll och diaries, p. 3.

⁶⁸ Case 788-2008, p. 2.

⁶⁹ Case 987-2009, p. 8.

⁷⁰ Id. p. 2.

⁷¹ Id., p. 2.

In the decision of October 5, 2010 in which the Datainspektion criticised the Parliamentary Ombudsman for publishing the names of the plaintiffs and of civil servants in the case law database located on its website, the Data Protection Authority mentions, without validating the privacy infringements, the purposes presented by the Ombudsman. They consist in providing the public insight into the activities of the Ombudsman, but also in disseminating knowledge about the legal appreciations contained in the decisions of the Parliamentary Ombudsman with the aim to give public authorities and civil servants guidelines for how to act in a correct way”.⁷²

The specific threats due to the publication of personal data on the Internet

The disclosure of personal data by means of the publication on the websites of the public authorities is surrounded by specific threats due especially to the wide dissemination of the data posted on the Internet as well as to the efficient searching possibilities and the easiness to make compilations of data that search engines offer.⁷³ The threats for privacy having to be taken into account in order to carry out the balancing of interests, the Datainspektion does refer in its decisions to the specific threats stemming from the Internet, although elaborating more or less on them.

Indeed, except for the decision of September 8, 2004 regarding the pizzerias in which the Internet was not mentioned at all, and for the decision of July 3, 2008 concerning the publication of a complaint lodged to the Parliamentary Ombudsman by a person working at a psychiatric hospital were the specific risks with Internet were only referred to *implicitly*, the Datainspektion does in its decisions *explicitly* mentions the risks due to the publication of personal data on Internet.

In the decision of April 7, 2010 in which *inter alia* data related to the health status of a data subject were at stake, the Datainspektion stated that “*through the publication on the Internet there is a high risk for a large dissemination*”.⁷⁴ In the decision of January, 29, 2010 concerning the students expelled from an upper secondary school, the Supervisory authority emphasises that the risk for dissemination of the data – which may be very sensitive for the students and their relatives – has been high due to the fact

⁷² Case n° 663-2010, p. 6.

⁷³ More on that issue in the introductory part of this paper.

⁷⁴ Case 119-2010, p. 5.

that the data have been searchable with means of search engines.⁷⁵ The Data Protection Authority was even more precise about the risks that emanated from the Internet in its decision of October 5, 2010, in which it criticised the Parliamentary Ombudsman for publishing the names of the plaintiffs and of civil servants in its online database. The Datainspektion mentions explicitly the increase of the risks for privacy due to online publication “*What makes the publication so sensible [...] is the way of publishing*” the Datainspektion states. The Data Protection Authority refers *inter alia* to the relative easiness to make comprehensive compilations, emphasises that the data are easily accessible especially by means of search engines, and mentions the possibilities to make compilations and to reuse the material that is accessible on the Internet.⁷⁶

Surprisingly and regrettably, the guidelines of the Datainspektion do not mention the necessity to take into the account the specificity on the Internet and the particular risks that online disclosure of personal data generate for privacy.

The question may be raised on what the legal framework will look like after the entering into force of the General Regulation on Data Protection (EU) 2016/679, and how this will affect proactive disclosure. It seems clear that the abuse centred model, which, in an indirect manner has lightened the conditions for online publication carried out by public authorities, will disappear.⁷⁷ Will we then go back to a system similar to the one that applied before the reform of 2007 of the Personal Data Act, i.e. a system where online proactive disclosure of personal data is permitted if the interest of the data controller or of third party outweighs the privacy rights of the data subject?⁷⁸ The formal answer seems to be uncertain due to different interpretations of the Regulation. According to one of the interpretations none processing carried out by public authorities will be encompassed by this legal ground, which could mean in turn that online proactive disclosure car-

⁷⁵ The Datainspektion states “Google, for instance”. Case 987-2009, p. 7.

⁷⁶ Case n° 663-2010, p. 6.

⁷⁷ See the statement of the Datainspektion on <http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-upphor/>

⁷⁸ Legal ground laid down in the Regulation (Article 6 1.f) as it was in the Data Protection Directive (Article 7).

ried out by public authorities would be considered as “*processing necessary for a performance or a task carried out in the public interest*” and will consequently be submitted to the requirement of having a legal basis (Article 6.3⁷⁹). If the other interpretation takes precedence however, the one according to which not all processing from public authorities will be excluded from this legal ground, the balance of interests might be theoretically still applicable to online proactive disclosure performed by public authorities.⁸⁰ Whatever the interpretation adopted, we think that the legislator should, in order to give some space for the public sector to publish information while ensuring the protection of the privacy of the persons concerned, adopt specific legal instrument(s), in the way it did partially in 2001⁸¹ and set out the overarching frame for the balance between the interests of transparency and privacy.⁸²

In legal terms, online proactive disclosure of personal data by public authorities should, with the new European Data Protection framework, enter a new phase. This shift could give the Swedish legislator the opportunity to re-think and rationalise the legal framework for online proactive disclosure of public documents and information containing personal data. The enactment of a new framework could be advantageously accompanied by guidelines and other recommendations drafted by the Datainspektion, addressed to all public authorities and with a special emphasis on the threats for privacy generated by publication on the Internet. The aim of this kind of guidelines should not only be to inform about the applicable data protection rules, but also to spread awareness among the public sector on the specific and serious threats online publication of personal data may have for privacy, and in turn for democracy.

⁷⁹ This legal basis “*should*”, according to Recital 41 of the Regulation “*be clear and precise and its application should be foreseeable to persons subject to it*”.

⁸⁰ See *Remittering av betänkandet SOU 2017:39 Ny Dataskyddslag*, 2017-09-04, n° 1210-2017, p.8.

⁸¹ By means of the Personal Data Ordinance, Section 12. The legal framework concerned the publication of the minutes and registers of the local authorities.

⁸² This corresponds also to recommendation of the Datainspektion to enact specific legal instruments, expressed in the 2010 decision in which the Data Protection Authority criticised the Parliamentary Ombudsman for publishing names in the decisions published in the case law database accessible on its website,

Data Protection Authorities in Central and Eastern Europe: Setting the Research Agenda

EKATERINA TARASOVA

Data Protection Authorities (DPAs), sometimes also referred to as Privacy Commissioners or Privacy Commissions, are authorities established for protecting privacy and monitoring personal data processing. DPAs are crucial actors in data protection. Flaherty argues that “under the broad rubric of ensuring privacy, the primary purpose of data protection is the control of surveillance of the public, whether this monitoring uses the data bases of governments or of the private sector” (1989:11). There are a number of different models for regulating surveillance “including regulation by national governments (executive, legislative, and judicial); extra-governmental organizations (watchdogs, ombudspersons and commissions); international agreements; and self-regulation by industry” (Regan 2012: 397). Data protection regime with establishment of DPAs as regulatory authorities is one of such models, characteristic for the member-states of the European Union and the neighboring countries. In the European Union, this regime is based on the Directive 95/46/EC that is the “most significant privacy protection legislation since the 1970s”, according to Rule (2009:31). Together with the Council of Europe’s Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data from 1981, it provides grounds for enacting Data Protection Acts and establishing DPAs. The Directive 95/46/EC obliged the EU member-states to set Data Protection Authorities and also gave rise to the Article 29 Data Protection Working Group which provided the platform for cooperation and communication between DPAs at the EU level.

Since DPAs have been set up in the Western Europe and the North America since 1970s, the research has focused to a large extent on DPAs in these contexts. DPAs in other regions have been established relatively recently. In Central and Eastern Europe, DPAs were established in the 1990s and later, after the change of socialist regimes. DPAs in Central and Eastern Europe region, including both EU member-states and non-mem-

ber-states, provide an excellent case for examining workings of DPAs in contexts other than West European and North American ones. Specific features of the region discussed further may contribute more nuanced understanding of DPAs workings.

This paper aims to set the agenda for future research on data protection authorities. It summarizes briefly the previous research on DPAs highlighting what is already known about DPAs and articulating gaps in knowledge, proposes to focus on DPAs in Central and Eastern Europe and suggests research agenda for further exploration.

Previous research on Data Protection Authorities

The research on Data Protection Authorities has mainly dealt with the following areas of inquiry. First, there are studies analyzing functions, responsibilities and roles of DPAs. Networks of privacy advocates, including DPAs, and their engagement in international privacy protection regimes are the second area of concern. Third area are issues connected to independence of DPAs. This subsection summarizes briefly the research on these three areas.

What DPAs are supposed to do and what they indeed do

The research on DPAs has focused on the history of data protection, as well as functions and responsibilities of DPAs (e.g. Banisar & Davies 1999, Bennett 1992, Burkert 1981, Flaherty 1986, 1989, Greenleaf 2015). Bennet summarizes the research on DPAs as focusing on “the content of law and the powers and responsibilities of privacy and data protection authorities” and on “what works and what does not” for effective data protection (Bennett 2012:412). While functions and responsibilities of DPAs have been analyzed to a large extent, the research on what DPAs indeed do is not extensive. How DPAs find their ways around their responsibilities and functions that are outlined in Data Protection Acts and what kind of roles they take on when they implement their function is less known.

Two factors have been said to shape work of DPAs. The first factor is personalities involved in DPAs work, in particular DPAs head and management. Heads of DPAs may perceive their roles differently. That may influence how they set priorities in implementing tasks of DPAs. Bennett notes that Flaherty in his seminal work from 1989 put forward the role of “a single privacy advocate at the head of the agency who knows exactly when to use the carrot and when to use the stick, and who is not concerned with

balancing data protection with other administrative and political values” as a “recipe” for effective data protection (Bennett 1992:239). Righettini examines the role of leadership in evolution of the data protection regulative policy style (2011). The second factor that shape work of DPAs are structural challenges and opportunities. Hustinx argues that for DPAs to make a difference there is a need for legal framework that would make it possible, thus highlighting importance of structural environment of DPAs (2009). In a similar line, Bosco et al investigate DPAs perspectives on legal framework and regulatory challenges regarding profiling techniques (2014). Apart from legal framework, organization of business and politics matters for outlook of data protection in a specific country (Newman 2008). Although these two factors have been argued to be important for shaping work of DPAs, the research has mainly focused on DPAs from structural, or in other words institutional, perspective – the second factor (e.g. in the works by Flaherty, Bennett, Raab, Jóri and Schütz).

As institutions, DPAs are primarily engaged in shaping and applying data protection law, “they are advocates, ombudspersons, and administrative authorities” (Jóri 2015). Schütz defines the roles of DPAs even broader stating that DPAs implement privacy policies, raise awareness, and provide consultancy services and network (2012a). The works of both Jóri and Schütz demonstrate that DPAs could deal with an immense number of issues. DPAs have to set priorities. Priorities are set according to perceptions of what is considered most important or most efficient to do. That implies that activities of DPAs are not only regulated by the Data Protection Acts and other documents, but they are shaped in the course of DPAs work and interaction with various actors in society.

If DPAs and specifically commissioners go beyond the defined set of responsibilities and take on an active position and advocate for privacy protection, there is a better chance to set privacy protection on the agenda, according to Flaherty (1989). “In order to be effective watchdogs over public administrations, data protectors have to adopt a functional, expansive, and empirical, rather than a formal and legalistic, approach to their statutory tasks” (Flaherty 1989:385). In line with that, Bennett argues that: “We perhaps need more data protection and privacy commissioners who take less of a “strict constructionist” approach to data protection law, and who are willing to push the boundaries of their statutory responsibilities and jurisdictions” (2015:6). However, taking on the role of privacy advocates may come with consequences. “Although many commissioners might see themselves as advocates, they cannot easily imitate these activists lest

they risk being ignored – or perhaps not being renewed in office – by hostile governments or parliaments, or written off by powerful groups which they must often cajole, rather than hector, into more privacy-protective practices” (Raab 2011:196). Jóri argues that the focus on one or another role is related to the state of data protection in a country (2015).

To sum up, the research on how DPAs are set up and what kind of functions and responsibilities they have is vast. Grounds for the analysis of how DPAs work is shaped by personalities of DPAs head and management and institutional structures have been established. At the same time, DPA’s implementation of their functions requires further exploration.

International networks of privacy advocates

Apart from the domestic level, DPAs have been active at the international level. They have united their efforts together with each other and other actors advocating for privacy protection in order to bring concerns about privacy higher on the agenda. International cooperation of privacy advocates has received much scholarly attention (Bennett 2008, Galetta et al. 2016, Greenleaf 2015, Kohnstamm 2016, Newman 2008, Rauhofer 2015, Yesilkagit 2011, Zalnieriute 2015) because collective actions of transnational networks raising privacy higher on the international agenda.

Mechanism that makes the cooperation of DPAs at the EU level possible –the Directive 95/46/EC, has been a theme of the previous research on DPAs. Newman focuses on the role of the Directive 95/46/EC in shaping international privacy regulation regime (2008). Greenleaf agrees that the EU Article 29 Working Party, under which DPAs develop policy jointly and set up by this Directive, is one of the most important institution where cooperation of DPAs take place (2015). On a similar note, Raab distinguishes the role of the Article 29 Working Party in bringing “national DPAs together to adopt positions and opinions on prominent issues on policy agendas in Europe and between the EU and elsewhere” (2011:201). The work of Raab, among others, demonstrates that the influence of the Directive extends beyond the EU member-states. Although it has been studied to some extent, the study of this influence in new contexts may bring new perspectives to it.

Another theme about transnational privacy networks is the interaction between domestic and international levels. Zalnieriute considers it striking that international privacy governance takes place through cooperation of privacy commissioners placed at the domestic level (2016). Developing on that, Zalnieriute questions deliberative capacity of transnational networks of

DPA that, if present, could bring new quality to international privacy governance (2015). Bennett argues that trust is an important factor in cooperation between DPAs (2015). Cranor adds another dimension pointing at formal and informal channels for cooperation. She emphasizes that interaction through formal and informal channels of cooperation could be beneficial for timely solution of rising issues (2002). The other theme includes cooperation between DPAs on the matters of enforcement. While Bennett argues that there are legal, economic, organizational and cultural barriers for enforcement cooperation between DPAs (2015:5), Kloza and Mościbroda propose some conditions and means for effective international enforcement cooperation (2014).

To sum up, transnational cooperation between DPAs and also other actors advocating for privacy protection has been much in focus. The rise of DPAs worldwide brings a new light to transnational cooperation of DPAs. More actors in transnational networks of privacy advocates could increase ability of these networks to bring change in data protection. Therefore, transnational networks and cooperation remains on the research agenda due to new circumstances.

Independence of DPAs

Independence is the third area of inquiry regarding DPAs (e.g. Greenleaf 2012, Schütz 2012b). To what extent authorities dealing with data protection are independent has been an important research question because independence is crucial for DPAs for doing their job properly. DPAs are taken as an example of regulatory agencies, although the one with potentially higher pressure from state, business and society than other regulatory agencies (Schütz 2012b). Schütz demonstrates that independence is a multifaceted concept where formal independence does not necessarily mean that DPAs are independent in practice (2012b). Moreover, meanings of independence could vary between different stakeholders, DPAs, politicians and non-state actors (Jackson 2014).

Schütz makes an attempt to separate formal independence from independence in practice on the example of DPAs in four EU member-states (2012b). In order to do so he assesses how independence is defined in the law, how DPAs are connected to ministries and other governmental agencies, who has the right to appoint and dismiss the head of the DPAs, how funding of DPAs is organized. Jackson distinguishes two dimensions of independence: structural mechanisms and behavioural quality that are characterized as processes outside and inside of DPAs respectively (2014).

Therefore, the question of independence is crucial not only from the perspective that DPAs need independence for making a difference in protecting privacy but also from the perspective of what is understood by independence. The research of Schütz is particularly spectacular in this respect as his findings reveal that the DPA in Poland is more formally independent than others while that is not the case when independence in practice is assessed. The question of independence could be even more substantial in the countries that have recently gone through the change of political regime.

To sum up, independence of DPAs is a highly relevant issue in privacy governance and data protection. The study of DPAs in the countries other than established democracies may bring new perspectives to issues concerning independence of DPAs. The region of Central and Eastern Europe provides an interesting case in this respect with relatively recent transformations of political regimes, including processes of democratic transition and Europeanisation.

Specificity of Data Protection in Central and Eastern Europe

Historically, data protection institutions have developed in the Western European and North American countries and from there spread to other contexts. These countries as pioneers of data protection have received considerable scholarly attention. Most of the findings in the field are made on the case of Western European and North American countries. While Western European and North American countries have shared similar conditions of being established democracies and developed economies, other regions may have different conditions and challenges of data protection. The findings of the previous research on data protection authorities need to be verified in other contexts. The context of Central and Eastern Europe is chosen here because the research on DPAs in Central and Eastern Europe is generally scarce and the region has several specific features that may be of interest for understanding the development of data protection in Europe within and beyond the European Union. Central and Eastern Europe is understood here as constituted by the countries to the east of Germany, to the south of the Baltic sea, to the west from Russia and to the north of Greece.

After the fall of the Soviet Union and the collapse of the socialist and communist political regimes, the countries in Central and Eastern Europe have gone through the processes of political transformation. While in case

of some countries the democratic transitions have been relatively successful, other transitions are still unfinished. The scientific discussions have begun to question whether political processes in these countries should be at all called democratic transition or they should be discussed in some other analytical terms. Political turbulence in the region may matter for governing data protection and work of data protection authorities, for instance, in questions concerning interaction of DPAs with other governmental bodies, their independence and general “fitting into” political systems.

Central and East European countries have been influenced by Europeanisation processes, understood as “penetration of the European dimension in national arenas of politics and policy” (Börzel 1999 in Featherstone & Radaelli 2003). Newman argues that “[a]s a result of the EU enlargement process, countries [in the CEE] have adopted data privacy legislation far in advance of any domestic economic need for personal information rules” (2008:115). Newman means that the establishment of data privacy legislation may be more externally driven by Europeanisation processes of the region and less driven by internal challenges, in particular through adaptation of the EU model of data protection which he calls comprehensive model of data protection (he distinguishes comprehensive and limited data protection regime (2008:32). Moreover, Newman continues saying that “[b]ecause of the relative immaturity of information-intensive industries in these countries, opposition from the private sector has been minimal” (2008:115). Conditions for establishing data protection institutions thus differ in the context of Central and Eastern Europe from the context of the Western Europe. That yields for the question to what extent and in what ways processes of Europeanisation (building relations with the European Union) have influenced the development and practices of DPA in the Central and Eastern Europe, including countries that are not EU members.

The specificity of the region is expressed as well in low levels of trust in society (Boda & Medve-Bálint 2012, Sztompka 1996). That is an important contrasting feature of the countries in Central and Eastern Europe contrasting to the context of Western Europe. As Bennet notes that trust is important for cooperation between DPAs (2015), low levels of trust may lead to different configuration of relations between DPAs and with other actors in society in Central and Eastern Europe. The argument of Bennet about importance of trust for cooperation between DPAs (2015) can be taken further. Trust is not only needed for establishing cooperation between privacy advocates but it is also needed for success of domestic activities of DPAs. For the adequate implementation of their functions, DPAs need to

be trusted by society. While questions about trust seems to be less of an issue in the Western European countries with the established institutions of data protection and higher levels of general trust in societies, it is certainly more relevant in the Central and East European context. Research inquiries may include questions about connections between general levels of trust and society and activities that DPAs carry out and whether they take on the role of privacy advocates.

Further research

The examination of the previous research on DPAs has revealed that there are a number of issues that could be investigated further, including how DPAs implement their functions and what kind of roles they take and under what conditions, how DPAs interact within transnational networks and cooperate with other actors engaged in advocating for privacy protection, to what extent DPAs are independent and how independence of DPAs could be understood. The analysis of these issues, while investigated to some extent in the context of Western European and North American countries, in other regions is limited. The further exploration of these issues on the example of Central and Eastern Europe may provide a more nuanced understanding of responsibilities, functions and roles of DPAs, their engagement in international privacy networks and various aspects of their independence. The specific contribution of the case of Central and Eastern Europe would lay in scrutinizing DPAs in the contexts characterized by recent political transformations, Europeanisation processes and lower levels of trust. These factors investigated all together or in separate studies can contribute new perspectives to understanding working of DPAs and data protection in general.

References

- Banisar, D. and Davies, D. (1999). *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*. John Marshall Journal of Computer & Information Law, Vol. 18 (1)
- Bennett, C. J. (1992). *Regulating privacy: data protection and public policy in Europe and the United States*. Ithaca, N.Y.: Cornell University Press
- Bennett, C. J. (2008). *Privacy Advocates: Resisting the Spread of Surveillance* [electronic resource] [Elektronisk resurs].
- Bennett, C.J. (2012). Privacy advocates, privacy advocacy and the surveillance society. In Ball, K., Haggerty, K.D. & Lyon, D. (ed.) (2012). *Routledge handbook of surveillance studies*. London: Routledge pp. 412–419
- Bennett, C. J. (2015). *The Global Enforcement Privacy Network: A Growing Network But How Much Enforcement?* Available at SSRN: <https://ssrn.com/abstract=2640331> accessed 27.08.2017
- Boda, Z. and Medve-Bálint, G. (2012). The politicized nature of many East European institutions means that they are trusted less than those in Western Europe. *EUROPP European Politics and Policy*. Available at <http://blogs.lse.ac.uk/europpblog/2012/08/21/institutional-trust-zsolt-boda/> accessed 27.08.2017
- Bosco, F., Creemers, N., Ferraris, V., Guagnin, D., Koops, B-J. (2014). *Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities*. In Gutwirth, S., Leenes, R. & de Hert, P. (2015). *Reforming European Data Protection Law* [Electronic Resource]. Dordrecht: Springer Netherlands, pp. 3–33
- Burkert, H. (1981). *Institutions of Data Protection – An Attempt at a Functional Explanation of European National Data Protection Laws*. *Computer Law Journal*, Vol. 3, pp.167–188
- Cranor, L. F. (2002). *The Role of Privacy Advocates and Data Protection Authorities in the Design and Deployment of the Platform for Privacy Preferences*. *Proceeding of the 12th Conference on Computers, Freedom & Privacy*, pp.1–8. Available at <http://dl.acm.org/citation.cfm?id=543506> accessed 27.08.2017
- Featherstone, K. and Radaelli, C.M. (ed.) (2003). *The politics of Europeanization*. Oxford: Oxford University Press
- Flaherty, D. H. (1986). *Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies*. *Science, Technology, & Human Values*, Vol. 11(1), pp. 7–18
- Flaherty, D. H. (1989). *Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill, N.C.: Univ. of North Carolina press

- Galetta, A., Kloza, D., & De Hert, P. (2016). Cooperation among data privacy supervisory authorities by analogy: lessons from parallel European mechanisms. Brussels: PHAEDRA.
- Greenleaf, G. (2015). Global data privacy laws 2015: Data privacy authorities and their organisations. *Privacy Laws & Business International Report* 134, 16–19. UNSW Law Research Paper No. 2015–53
- Greenleaf, G. (2012). Independence of Data Privacy Authorities: International Standards and Asia-Pacific Experience. *Computer Law & Security Review*, Vol. 28 (1 & 2), pp. 1–47
- Hustinx, P. (2009). The Role of Data Protection Authorities. In Gutwirth, S. (ed.) (2009). *Reinventing data protection?* 1st ed. New York: Springer
- Jackson, C. (2014). Structural and behavioural independence: mapping the meaning of agency independence at the field level. *International Review of Administrative Sciences*, Vol. 80(2), pp. 257–275
- Jóri, A. (2015). Shaping vs applying data protection law: two core functions of data protection authorities. *International Data Privacy Law*, Vol. 5(2), pp. 133–143
- Kloza, D. and Mościbroda, A. (2014). Making the case for enhanced enforcement cooperation between data protection authorities: insights from competition law. *International Data Privacy Law*, Vol. 4 (2), pp. 120–138
- Kohnstamm, J. (2016). Getting Our Act Together: European Data Protection Authorities Face Up to Silicon Valley. In Wright, D. & De Hert, P. (ed.) (2016). *Enforcing Privacy Regulatory, Legal and Technological Approaches*. Cham: Springer International Publishing, pp. 455–472
- Newman, A.B. (2008). *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Cornell University Press: Ithaca and London
- Raab, C.D. (2011) Networks for Regulation: Privacy Commissioners in a Changing World, *Journal of Comparative Policy Analysis: Research and Practice*, Vol. 13(2), pp. 195–213
- Regan, P.M. (2012). Regulating surveillance technologies. Institutional arrangements. In Ball, K., Haggerty, K.D. & Lyon, D. (ed.) (2012). *Routledge handbook of surveillance studies*. London: Routledge, pp. 397–404
- Rauhofer, J. (2015). Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?. *Data Protection Law Review*, Vol. 1, pp.5–15
- Righettini, M.S. (2011). Institutionalization, Leadership, and Regulatory Policy Style: A France/Italy Comparison of Data Protection Authorities. *Journal of Comparative Policy Analysis: Research and Practice*, Vol. 13(2), pp.143–164
- Rule, J. B. (2009). The limits of privacy protection. In Goold, B. J (ed.) (2009). *New Directions in Surveillance and Privacy*. Willian Publishing
- Schütz, P. (2012a): The Set Up of Data Protection Authorities as a New Regulatory Approach. In: Gutwirth, S.; Leenes, R.; De Hert, P.; Pouillet, Y.

- (eds.): *European Data Protection: In Good Health?* Dordrecht: Springer, pp. 125–142
- Schütz, P. (2012b). Comparing formal independence of data protection authorities in selected EU member states. Conference Paper for the 4th ECPR Standing Group for Regulatory Governance Conference. Available at <http://regulation.upf.edu/exeter-12-papers/Paper%20265%20-%20Schuetz%202012%20-%20Comparing%20formal%20independence%20of%20data%20protection%20authorities%20in%20selected%20EU%20Member%20States.pdf> accessed 27.08.2017
- Sztompka P. (1996). Trust and Emerging Democracy: Lessons from Poland. *International Sociology*, Vol. 11, pp. 37–62
- Yesilkagit, K. (2011) Institutional compliance, European networks of regulation and the bureaucratic autonomy of national regulatory authorities. *Journal of European Public Policy*, Vol. 18 (7), pp. 962–979
- Zalnieriute, M. (2016). The promise and potential of transgovernmental cooperation on the international data privacy agenda: Communicative action, deliberative capacity and their limits. *Computer Law and Security Review*, Vol. 32(1), pp.31–54

Media Freedom and Pluralism in the Digital Infrastructure

NICOLA LUCCHI¹

1. Introduction

Advances in information technology and communication media have offered a better information infrastructure and new forms of information exchange, but at the same time they have brought with them a number of new challenging regulatory issues for the network economy as well as for society at large.² The legal response to these developments has been the subject of global controversy and litigations in numerous courts and still remains an unresolved issue.³ In any liberal democracy, the ability to participate in society (also online) can only be assured if media freedom and pluralism are improved by the availability of an open, independent and free media outlet. Media freedom implies absence of constraint from government control and involves editorial independence, the protection of journalists and open public access to information sources.⁴ On the other hand, media pluralism implies the ability of individuals to satisfy their information needs.⁵ It also means that citizens must have access to a range of information sources and services included in the digital communication infrastructure.⁶ Media freedom and pluralism are fundamental pillars of any

¹ This text is a summary of a talk given at the International trans-disciplinary workshop on “The Right of Access to Information & the Right to Privacy: A Democratic Balancing Act” - December 13, 2016 - Södertörn högskola Stockholm/Huddinge (Sweden).

² See generally Shapiro and Varian, *Information Rules: A Strategic Guide to the Network Economy*, Cambridge (1999).

³ See High Level Expert Group on Media Freedom and Pluralism, *A free and pluralistic media to sustain European democracy*, Brussels (2013).

⁴ See Becker L. et al, *An Evaluation of Press Freedom Indicators*, 69 *International Communication Gazette* 5 (2007); Siebert, F.S. et al., *Four Theories of the Press*, Urbana (1956).

⁵ See Karppinen, K., *Rethinking Media Pluralism*, 13-14 *New York* (2013).

⁶ See Hammarberg, T. et al., *Human rights and a changing media landscape*, Council of

democratic society and thus it is important to monitor any possible infringement of these rights and explore ways to support individuals who are faced with the challenge of being subject to such violations.⁷

The European Union's commitment to respecting freedom and pluralism of the media, as well as the right to information and freedom of expression, is expressly recognized in Article 11 of the Charter of Fundamental Rights, similar to the provision of Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Media freedom and pluralism are also rooted in the national constitutional tradition of the EU member states.⁸ Nevertheless, in the current legal environment, the range of obstacles to full realization of the new opportunities offered by digital media still presents a substantial challenge to full realization of media pluralism.⁹

In this new technological landscape, several questions arise: what measures and actions can be taken to guarantee freedom of expression, media pluralism and access to knowledge in the digital environment?; what are the possible solutions to protect digital freedom of expression and what actions can be taken to better protect citizens' access to information and for their participation in digital life?; what are the policy directions for allowing the free flow of information, freedom of expression and protection of individual liberties as they relate to information access?; how to structure a balanced protection for intellectual creations –at the same time–for a better respect of individual users' freedom to express themselves, to access and share content, culture, information and to innovate and create?; in the absence of scarce resources, is there still a problem of pluralism in the digital environment?

Europe (2011); Foster R., *News Plurality in a digital world*, Reuters Institute for the Studies on Journalism (2012).

⁷ See Klimkiewicz B. (ed.), *Media freedom and pluralism: media policy challenges in the enlarged Europe*, Central European University Press (2010).

⁸ See Centre for Media Pluralism and Media Freedom, *European Union Competencies in Respect of Media Pluralism and Media Freedom – Policy Report*, European University Institute, Florence (2013).

⁹ Council of Europe, Commissioner for Human Rights, *Media Pluralism and Human Rights* (2011), available at <https://wcd.coe.int/ViewDoc.jsp?id=1881589>.

Finding appropriate answers to these questions is essential to develop effective policies, legal mechanisms and social practices that can help to better secure the freedom and wealth of the digital information network.

The first part of this paper describes briefly the challenges and the opportunities posed to media freedom and pluralism by the rapidly changing digital media environment. The second part of the paper is, instead, focused on a series of regulatory reforms recently adopted or discussed in different countries and with the ability to filter and control online spaces.

Digital Media Pluralism: Challenges and Opportunities

The assumption that the Internet and all of the other new communication technologies constitute a solution to all of the concerns related to media pluralism and diversity is probably overly optimistic.¹⁰ Despite the increased diversity of media ownership, the variety of media content and the exponential growth of information sources, worries about concentration of power and creation of new gatekeepers or content aggregators are still far from being completely resolved. For example, search engines are now a new troublesome form of informational intermediary, which acts as an information processor, allowing users to access and process more efficiently information about resources, goods, services, prices and other characteristics that influence what contents are most easily accessible.¹¹ One of these search applications – Google – effectively holds a monopoly position on the search engine market. Here – for example – the question is whether there is a tension between search engines' commercial interests and pluralism, which may entail the risk of creating the so-called “filter bubble”.¹²

Another problematic area for digital media pluralism is represented by the range of new measures on Internet content governance, the aim of

¹⁰ See e.g. Eric Berendt, *Freedom of Speech*, xvi, Oxford University Press (2005); Valcke P. et al., *Media Pluralism and Diversity: Concepts, Risks and Global Trends*, 1,2, Palgrave Macmillan (2015).

¹¹ See Belleflamme P. and Peitz M., *Industrial Organization: Markets and Strategies*, 609, Cambridge University Press (2010).

¹² See Parisier, E., *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, Penguin Press (2011). According to the author, the term is defined as a “personal ecosystem of information that is been catered” by algorithms in order to provide content that matches the user's preferences.

which is to prevent illegal access to copyrighted digital content. In particular, these measures have distortive effects on the growing possibilities offered by computer-mediated communication. The debate over these online copyright enforcement efforts has intensified over the past few years, particularly with regard to blocking injunctions, digital content reforms recently introduced or discussed in Europe and in the U.S. and their implications for freedom of expression and media freedom.¹³ The growing increase in enforcement of copyright protection for digital information has – in fact – led to design choices in network architecture and copyright rules that can largely determine and influence the way in which information is made available. From this point of view, a major challenge for developing a more sustainable and free digital media system is to find an appropriate balance between respect for pluralism and the need for content protection.

This debate is not simply technical, but also political, legal and social, as it involves ethical and value-oriented solutions, but also – more importantly – awareness of the human rights dimension of this issue. The possible answers to this problem are currently at the centre of an on-going discussion concerning the regulation of digital content, the notion of freedom of expression and modern communication technologies.¹⁴

Digital Media Pluralism and Internet content restrictions

Limitations on individual rights are often a necessary precondition for the efficient functioning of these rights. This means that recognition of the rights and freedoms of others is often not just a limitation, but also a precondition for the freedom of all. Let us consider, for example, the pro-

¹³ See e.g. Council of Europe, Guide to human rights for Internet users, Recommendation CM/Rec(2014) 6 and explanatory memorandum (2014); Lucchi N., Internet Content Governance & Human Rights, 16 Vand. J. Ent. & Tech. L. 809 (2014); Lucchi N., Access to Network Services and Protection of Constitutional Rights, 19 Cardozo J. Int'l and Comp. L. 645 (2011); Dutton W. H. et al., Freedom of Connection - Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet UNESCO, (2011); Giblin R., Evaluating Graduated Response, 37 Colum. J.L. & Arts 147 (2014); Land M., Toward an International law of the Internet, 54 Harv. Int'l L.J. 393 (2013); Jørgensen, R. F. (ed.), Human Rights in the Global Information Society, MIT press (2006); Helberger, N., Controlling access to content: regulating conditional access in digital broadcasting, Kluwer Law (2005).

¹⁴ See Tambini, D., The End of Press Freedom, London (2012).

tection of the environment versus right to property; censorship versus right to expression, freedom of speech versus right to privacy etc.

In any democratic country, the state has the responsibility to regulate and make possible the exercise of fundamental rights. The only legitimate reasons for limitations to the freedom of expression or access to information are those that protect other human rights, a higher interest or a higher value compared to the one being limiting.

In Europe, 40 of the 47 member states of the Council of Europe have adopted access to information laws,¹⁵ a total of 25 European constitutions recognize some kind of right of access to official documents or information, and a total of 35 include the right of access to information or the “freedom of information”.¹⁶ Also the European Court of Human Rights acknowledged that there is a fundamental right of access to information held by public bodies that is protected by Article 10 on Freedom of Expression of the European Convention on Human Rights.¹⁷ In addition, the same Court has recently had the opportunity to decide whether a denial or a restriction of access to the Internet can be considered a violation of the Convention.¹⁸ The complaint – based on a breach of the provisions of Article 10 – had been submitted by a prisoner alleging a violation of his right to receive information, because he was refused Internet access in prison in order to pursue studies via distance learning.¹⁹ The court found that Lithuania violated Article 10 of the European Convention on Human Rights by not granting the prisoner online access to the Internet for study-related purposes. In particular, the court emphasised that there is growing recognition of the importance of the Internet for the enjoyment of a range of human rights, and that Internet access is increasingly understood as a right.²⁰

¹⁵ See Olsson A. R. (2011) Access to Official Documents, in Human Rights and a Changing Media Landscape 77, 79, Council of Europe (2011).

¹⁶ OSCE, A Guide for Journalists on how to Access Government Information, (2010), available at <http://www.osce.org/fom/67866?download=true>.

¹⁷ ECtHR 14 April 2009, Appl. no. 37374/05, *Társaság a Szabadságjogokért v. Hungary*; ECHR 26 May 2009, no. 31475/05, *Kenedi v. Hungary*.

¹⁸ ECtHR 17 January 2017, Application No 21575/08, *Jankovskis v. Lithuania*.

¹⁹ See ECtHR, *Jankovskis v. Lithuania*, Application No 21575/08.

²⁰ ECtHR 17 January 2017, Application No 21575/08, *Jankovskis v. Lithuania*. The Court has also stressed that “in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public’s access to news and facilitating the dissemination of information in general”.

The principal rationale that justifies legal protection of freedom of expression is to enable the self-expression of speakers.²¹ In any democracy, it is essential that people have access to a wide range of information that allows them to effectively participate in society.²² The Internet has now become one of the principal means of exercising the right to freedom of expression and information²³ and certainly falls within the scope of all the international legal provisions supporting freedom of expression and access to information²⁴ which also embrace the right to seek, receive and impart information and ideas.

Here, the point is to determine how to ensure that new media remain an unrestricted and public forum, where the exercise of freedom of opinion and expression can be achieved without excessive limitations. In fact – as previously mentioned – the rules governing the world of information and communication are now being subject to profound changes and tensions. This has inevitably caused conflicts and controversies in the delicate balance that underlies fundamental rights and basic democratic principles. As a general rule, regulatory policies should not interfere with or restrict freedom of expression.

However, in almost all democratic societies, new media, besides incurring definitional problems, have led to attempts to restrict and control online information.²⁵ The advent of the Internet has had a profound and revolutionary impact on the framework of media regulation and on control of the broadcasting sector in general.²⁶ This has often led to the adoption of legislative measures frequently criticized for their inability to reconcile technological progress with economic and other interests.²⁷ In particular, no

²¹ Sadurski W., *Freedom of Speech and Its Limits*, Dordrecht 18, (Kluwer Academic Publishers (1999)).

²² See Gans H.J., *Democracy and the News 1*, Oxford University Press (2003).

²³ See, e.g., ECtHR 18 December 2012, Appl. no. 3111/10, *Ahmed Yildirim v. Turkey*.

²⁴ Article 19, Universal Declaration of Human Rights, GA Res 217A (III), 10 December 1948, A/810 91; Article 10, Convention for the Protection of Human Rights and Fundamental Freedoms 1950, ETS 5; Article 19, International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171.

²⁵ Sunstein C., *Republic.com*, 138, Princeton University Press (2001).

²⁶ See e.g. Price M. E., *Media and Sovereignty: The Global Information Revolution and Its Challenge*, 216, MIT Press (2002); DeNardis L., *Protocol Politics: The Globalization of Internet Governance*, 20, MIT Press, (2009).

²⁷ Deibert R.J., *Black Code Redux: Censorship, Surveillance, and the Militarization of Cyberspace*, in *Digital Media and Democracy: Tactics in Hard Times* 137, 152 (Megan Bowler ed.), MIT Press (2008).

area of law has been more affected by the digital media revolution than intellectual property.²⁸ Our society and economy have become increasingly dependent upon the availability, exchange and sharing of digital information. The emergence of digital technology and computer networking has drastically changed commercial and regulatory developments in the media sector. While digital media products have experienced different degrees of market success, they are given inadequate and disproportionate protection under existing and emerging legislation. In many cases, states (democratic and authoritarian) limit, control, influence and censor content distributed through the Internet without any legal basis or authority and “without justifying the purpose of such actions; or in a manner that is clearly unnecessary and disproportionate to achieving the intended aim”.²⁹ Similar behaviours are not only serious human rights violations, but they can also have negative implications for the right to freedom of opinion and expression.³⁰

These matters need our urgent attention, especially since the recent introduction of regulatory measures that have led to significant changes in the regime of immunity, limited liability or “safe harbour” for online intermediaries regarding the content posted by their customers.³¹ In particular, this fragile regulatory framework of immunity is now marked by a profound tension between demands for freedom and demands for surveillance and control expressed by the market, enterprises and different institutional actors. A whole series of national and international regulatory measures have been implemented by governments to filter or inhibit Internet-based communications, also in the case of infringement and misappropriation of intellectual property rights. In particular, digital content reforms were recently introduced or discussed in Europe and in the U.S. The most controversial among these laws were the proposals contained in

²⁸ See Packard A., *Digital Media Law*, 127, Wiley (2010).

²⁹ United Nations General Assembly, Human Rights Council (2011) “Commission on Human Rights, Report by the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,” Frank La Rue, U.N. Doc. A/HRC/17/27 (16 May 2011).

³⁰ *Id.*

³¹ See Edwards, L., *Role and Responsibility Of Internet Intermediaries in The Field Of Copyright And Related Rights*, report Commissioned by World Intellectual Property Organisation (2011). The term “safe harbour” refers to measures designed to exempt service providers from liability under specific circumstances.

the Stop Online Piracy Act (SOPA)³² and in the Protect Intellectual Property Act (PIPA)³³ discussed in the United States, the HADOPI legislation adopted and then revised in France,³⁴ the Sinde Law implemented in Spain³⁵, the Digital Economy Act enacted in the United Kingdom³⁶ and the online Copyright Enforcement Regulation issued by the Italian Communication Authority (AGCOM) in Italy³⁷. The difficulty encountered in all of these regulatory initiatives is the lack of sensitivity to the need to maintain independence of media and avoid attempts to develop and promote private forms of controls.³⁸ In addition, all of these legal reforms are characterized by features that entail imposing legal responsibility on Internet service providers.

These circumstances show clearly how freedom of speech can become a problematic issue if the task of maintaining control over the information flow is held not by the state, but instead delegated to a private or a commercial entity. Holding intermediaries liable for the content created, uploaded and distributed by their users can significantly affect having enjoyment of the right to freedom of opinion and expression. Such an approach, in fact, naturally encourages the development of self-protective and extensive forms of “private censorship”, thereby undermining the guarantees of due process of the law and a fair trial.³⁹ Law has in fact always provided a potential legal recourse through the judicial system in cases of illegal government censorship. But what can happen when censorship is made not by a government actor, but through the application of rules imposed by independent admini-

³² Stop Online Piracy Act (SOPA) (2012), H.R. 3261, 112th Cong.

³³ Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, (2012) S. 968, 112th Cong.

³⁴ Loi 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, 135 Journal Officiel de la République Française, 13 June, 2009, p.9666

³⁵ Ley 2/2011, de 4 de marzo, de Economía Sostenible, 55 Boletín Oficial del Estado, March 5, 2011, Sec. I. p. 25033.

³⁶ United Kingdom, Digital Economy Act, 2010, 59 Eliz. 2, c. 24, § 124A.

³⁷ AGCOM, Delibera n. 680/13/CONS - Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70.

³⁸ See Lucchi N., Internet Content Governance & Human Rights, 16 Vand. J. Ent. & Tech. L. 809 (2014).

³⁹ United Nations General Assembly, Human Rights Council (2011) “Commission on Human Rights, Report by the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,” Frank La Rue, U.N. Doc. A/HRC/17/27 (16 May 2011).

strative authorities or private corporations? What recourse is available in these cases? In addition, the growing increase in enforcement of copyright protection of digital information has led to design choices in network architecture and copyright rules that can largely determine and influence the way in which digital information is made available.

Conclusion

As we have briefly outlined, the current changing digital media environment seems to be characterized by a new challenge involving a new approach to pluralism. As noted by other scholars, it is no longer a matter of concentration of media power or “limitations on producing content, expressing divergent ideas and opinions” and “availability of distribution systems”;⁴⁰ instead, the new problem seems to be having the capacity to effectively reach – without undue restrictions – many different audiences. The digital environment appears to be increasingly characterized by attempts to filter and control online spaces and – at the same time – by the presence of only a few aggregators and intermediaries of content, which entails the risk of putting access to digital information into the hands of a small number of global gatekeepers.

An interesting observation from recent studies is that “the concentration of where the audience goes—in terms of aggregators and sites—is every bit as damaging to pluralism as limitations on spectrum and concentration of ownership”.⁴¹ Media pluralism is therefore a concrete issue in the digital world as well, but with different features and contexts. In order to be useful in the contemporary digital media landscape too, media pluralism should be reinterpreted in light of the new reality. The control over information flows has become – in fact – a very effective form of power over the Internet. These new forms of control can be highly pervasive and ubiquitous in many different areas of digital communication. For example, legal tools for online copyright enforcement, protection mechanisms over digital content, aspects of the network architecture, net neutrality policies and other environmental variables can unreasonably obstruct or interfere with the free flow of information online.

⁴⁰ Valcke P. et al., *Media Pluralism and Diversity: Concepts, Risks and Global Trends*, 2, Palgrave Macmillan (2015).

⁴¹ *Id.*

In particular – as we have seen – there are several challenges to the possibilities of new media fostering pluralism: the first one is the lack of a real universal access to online media. In addition, another relevant set of challenges is posed by different forms of internet content restrictions increasingly used to protect information goods. Finally, there are no sector-specific and effective policies fostering pluralism through new media. It is therefore clear that while technology can improve and strengthen freedom of speech and the plurality of voices, it can also generate new risks and challenges. Consequently, the crucial task for current regulatory policy is not just to elevate the features and benefits of technology, but also to find a way to balance the problems and values that technology brings with it.

Abstracts

Ethical Destruction?

Privacy concerns regarding Swedish social services records

SAMUEL EDQUIST

Historian and archival scientist **Samuel Edquist** uses the Swedish social services system as a case study to identify and analyse ideological structures related to access and privacy. In the article *Ethical destruction? Privacy concerns regarding Swedish social services records*, Edquist shows that the social services constitute a more than adequate choice for this kind of analysis. There are several reasons for this. First and foremost, a social services system always constitutes an important part of every modern society and is, therefore, of interest to analyse. Secondly, social services files often contain very sensitive personal data related to the individuals being the subject of investigation, and arguments may be found both for retaining the data – for the sake of researchers, national heritage and the individuals – and for destroying them for the sake of privacy. The strong arguments for entirely opposing measures indicate a topic of great interest. The analysis Edquist carries out of debates leading to new social services legislation from the 1980s onwards is therefore of great interest to discern the various actors involved in the debate, as well as the types of interests represented by these actors. Much research has stressed the relation between privacy concerns and technical development and digitalisation. Edquist, however, shows that privacy concerns were high on the agenda already in the “analogue” era, before the social services records became digital. Among the interesting results of the article, Edquist shows how the political debate ultimately led to the retention of vast amounts of personal data for some individuals and some parts of Sweden, and the destruction of much of the other social services files. The study of the history of ethical destruction carried out by Edquist thus teaches us that the situation today is the result of several com-

promises between different actors and interests carried out during a long period of time.

Medical Records – the Different Data Carriers Used in Sweden from the End of the 19th Century Until Today and Their Impact on Confidentiality, Integrity and Availability

RIKARD FRIBERG VON SYDOW

Rikard Friberg von Sydow, archival scientist and doctor in ethics, addresses the development of medical records in a historical perspective, with an emphasis on the last 150 years. In *Medical records – the different data carriers used in Sweden from the end of the 19th century until today and their impact on confidentiality, integrity and availability*, Friberg von Sydow identifies the different types of data carrier through which medical records have been managed during this period. The author shows that the data carrier notebook gradually transformed into paper files, which, in turn, could be compiled into filing cabinets. Towards the end of the period, finally, the digital file became the main data carrier. For each of these types of carriers, the author applies the so-called CIA Triad from the contemporary information security discourse. “CIA” stands for confidentiality (ability to protect data from persons not allowed to access it), integrity (ability to hinder and monitor changes of data) and availability (ability to reach data). The analysis shows that confidentiality and integrity deteriorated over time, as protecting data from persons not allowed to access it and hindering and monitoring changes of data became more difficult. As for the possibility to reach the data, however, the historical development of data carrier made reaching the data increasingly easy. By applying theoretical concepts from the contemporary information security field on a historical material, Friberg von Sydow is able to identify information security related problems applicable not only to our times, but to historical periods as well. In similarity with Samuel Edquist, then, Rikard Friberg von Sydow urges us to remember that privacy concerns are relevant not only in our present time of digital records, but applies also for the analogue records of previous times.

The Right to Access Health Data in France: The Contribution of the Law of January 26, 2016

WILLIAM GILLES

In his paper *The Right to Access Health Data in France: the Contribution of the Law of January 26, 2016*, **William Gilles**, associate professor in law, shows how the issue of privacy in the medical field has been tackled by the French legislator in the context of the recent reform of the Health Code. Central for the paper is the issue of the use of health data for administrative and other public purposes, and of its balancing with the need to protect the privacy of the beneficiaries of health care services. The paper is divided into two parts. In the first part, Gilles provides information on the previous system consisting of a large medical administrative database of individuals' Health data. Within this system, health data were "pseudonymised" to protect privacy of the health care users. In the second part, Gilles examines the new system put in place by means of the Law for Modernising the French Health System adopted in 2016, a law which leads to the replacement of the earlier database with a new national Health database. The new system constitutes, according to Gilles, an improvement in relation to the prior system, by offering a better opening of health databases and a high level of protection of the rights of the beneficiaries of health services. The law imposes *inter alia* an obligation to preserve privacy and to better secure the processing of the data by organising the access to databases through two separate channels, depending of the sensitivity of the data. As Gilles points out, the new system contributes to making the data more accessible in comparison to the previous one. The challenge remains for the different actors, however, to protect privacy and to respect the objectives of public service at the same time.

The Swedish Black Box.

On the Principle of Public Access to Official Documents in Sweden

ANNA ROSENGREN

In *The Swedish Black Box*, historian and archival law expert **Anna Rosengren** proposes a model for the Swedish principle of public access to official documents. Having found that models used in archival science were not entirely applicable on the Swedish case, concepts from black box theory were proposed to shed light over the Swedish principle of public access to

official documents. Black box theory is used when a system is not directly observable, and knowledge about it must be obtained through the analysis of the relation between input brought to the system, and the output emanating from it. From a literature study on archival science research, Rosengren had identified seven different factors as having an influence on the creation and release of official documents. These factors were combined with concepts of black box theory into a model, the *Swedish Black Box*, to shed light over the principle of public access to official documents in Sweden. The high number of factors having an impact on the creation and release of official documents makes it hard to predict the total amount of accessible documents at a specific point in time, i.e. the “system” cannot be directly observed. The article also describes a test of the model using the theoretical case of a pupil handing in a text for assessment to the teacher in 2003 and 2016, respectively. The analysis showed that changes occurred in two factors, resulting in more official documents being accessible towards the end of the period. As the factors were related to technology and routines, not to legislation, the effect on the creation and release of official documents was difficult to predict. The Swedish principle of public access to official documents, therefore, seems to resemble a black box.

Online Proactive Disclosure of Personal Data by Public Authorities.

A balance between transparency and protection of privacy

PATRICIA JONASON

From a legal point of view, **Patricia Jonason**, Associate Professor in public law, examines the balancing between the right of access to information and the right to privacy in the context of online proactive disclosure of personal data. Proactive disclosure is understood as disclosure of information made by public authorities without a request having previously been made for such disclosure. Interestingly, the release upon request of official documents containing personal data normally does not activate data protection legislation in Sweden. In the case of *proactive disclosure* of official documents containing personal data, however, the data protection legislation must be followed. Jonason presents and analyses the legal framework, and shows how it has evolved over time. She illustrates the legal framework through the analysis of cases on proactive disclosure handled by the Swedish Data Protection Authority. In addition, guidelines concerning online proactive disclosure, drafted by the same authority for the benefit of local authorities,

are taken into consideration. Jonason is especially interested in the balancing between the interest to protect privacy of the data subject and the interest of ensuring openness and transparency, and how this balancing is conveyed in the letter of the law, the preparatory works, as well as in the concrete implementation made by the Data Protection Authority. The conclusion reached by Jonason is that the current legal framework, constituted by different “layers”, is intricate. Changes on data processing made by public authorities should be expected, however, due to the General Regulation on Data Protection that will enter into force in 2018. This might constitute an opportunity for the legislator to rationalise the current legal framework.

Data Protection Authorities in Central and Eastern Europe: Setting the Research Agenda

EKATERINA TARASOVA

In the paper of **Ekaterina Tarasova**, *Data Protection Authorities in Central and Eastern Europe: Setting the Research Agenda*, the institutional aspect of the protection of the right to privacy is in focus. More precisely, Tarasova carries out an extensive analysis of research on Data Protection Authorities (DPA), i.e. the national authorities monitoring the compliance with data protection legislation. She presents her results around three themes. The first theme covers the functions, responsibilities and roles of DPA's. It shows that the functions and the responsibilities of the DPA's have been the subject of extensive research while other issues, such as how the DPA's implement their functions, remain quite unexplored. As for the second theme, Tarasova shows that the issue of international networks of privacy advocates still leaves room for further exploration, not least in relation to the transnational cooperation between DPA's. Concerning the third theme, the independence of the DPA's, the study reveals that this is a question of great importance for the protective tasks of the DPA's. Furthermore, a distinction between formal independence and independence in practice made in the previous research is important. Tarasova argues, and this constitutes the heart of her analysis, that the context for data protection authorities is different for DPA's in Central and Eastern Europe, as compared to that in the Western European and North American countries. The “political turbulence” as well as the lower level of trust in society in the region in comparison to the Western European countries may have an

impact on the work of DPA's in Central and Eastern Europe, Tarasova claims, and concludes by pointing out a need for future research of DPA's in Central and Eastern Europe for a better understanding of DPA's in general.

Media Freedom and Pluralism in the Digital Infrastructure

NICOLA LUCCHI

Nicola Lucchi, Associate Professor in law, addresses the topic of access to information from the angle of the information provided by the media. In his paper, *Media Freedom and Pluralism in the Digital Infrastructure*, Lucchi considers the global impacts of digital communication technologies and how they can influence media freedom (editorial independence, absence of government control and open public access to information for journalists) and media pluralism (the possibility for individuals to satisfy their information needs). He argues that the development of information and communication technology has offered possibilities to improve the information structure, just as it has offered new forms of information exchanges. Lucchi suggests, however, that while new media may potentially help pluralism, there are also significant challenges. Notably, Lucchi points out the concentration of power and creation of new gatekeepers and content aggregators. One example given, is the concentration of power to search engines that may influence what contents are most easily accessible, and so help creating “filter bubbles” that will effectively keep certain information outside of reach of the individual. Another area of concern are the measures taken to monitor Internet content, the aim of which could be to prevent illegal access to copyrighted digital content. These challenges on how to achieve effective freedom and pluralism through new media, are notable not in the least for the regulator. He also focuses on the ways in which legal systems aim to support and protect media freedom and pluralism within the context of ongoing technological developments. As stressed by Lucchi, this debate certainly is not simply technical, but also political, legal and social. The ethical and value-oriented solutions that it calls for concern us all.

About the authors

SAMUEL EDQUIST, historian and archival scientist, Senior Lecturer in ALM subjects (archival studies, library & information studies, and museum & heritage studies) at the Department of ALM, Uppsala University. Research interests have covered subjects such as nationalism, heritage studies, popular education and archival science, and current research projects include the study of the history of retention and destruction of archival documents.

RIKARD FRIBERG VON SYDOW, archival scientist and doctor in ethics, Senior Lecturer at the School of Historical and Contemporary Studies, Södertörn University. Rikard Friberg von Sydow is responsible for the discipline archival science at Södertörn University, and current research includes the analysis of the historical development of medical records, the application of methods from contemporary information security discourse, as well as global archival science.

WILLIAM GILLES, Associate Professor at the Sorbonne Law School. Gilles is the director of the Master's degree in Digital Law, a member of the board of the Sorbonne Law School and of the Academic Board of the University Paris 1. He is the president of IMODEV, an international research network on open government and digital issues, and the director of the *International Journal of Open Government* and of the *International Journal of Digital and Data Law*.


PATRICIA JONASON, Associate Professor in Public Law, School of Social Sciences, Södertörn University. Patricia Jonason teaches administrative and constitutional law as well as European law and Human Rights. Her current research interests are mainly linked to privacy and the right of access to information and the difficulties in striking a balance between the two, as

exemplified in recent investigations of the right to be forgotten and proactive disclosure.

NICOLA LUCCHI, Associate Professor in Law, Jönköping International Business School, Jönköping University. The research and academic interests of Nicola Lucchi focus on comparative law and the interaction between law and innovation. His current research agenda is dedicated to exploring the interfaces between law, science and technology and the legal and ethical issues arising from recent development in these fields.

ANNA ROSENGREN, Senior Lecturer, School of Engineering, Jönköping University. Anna holds a PhD in history and has taught archival law at Södertörn University. Her current research is oriented towards the Swedish principle of public access to official documents. How such official documents come into being, and the awareness among citizens about how the Swedish principle handles their data, constitutes her current focus.

EKATERINA TARASOVA, PhD in Political Science, Södertörn University. Ekaterina is affiliated with the project *Like Fish in Water: Surveillance in Post-Communist Societies*, Södertörn University. She studies Data Protection Authorities in Central and Eastern Europe. Her research interests include energy transitions, social movements, technologies and society.



This publication gathers presentations from an international and trans-disciplinary workshop held at Södertörn University in December 2016.

The workshop entitled *The Right of Access to Information and the Right to Privacy: A Democratic Balancing Act* was one of the many events which celebrated the 250th anniversary of the Swedish Freedom of the Press Act, the first legal instrument in the world laying down the right of access to official documents.

A starting point for the workshop was the assumption that the right of access to information and the right to privacy are both necessary pre-conditions for a democratic society. Researchers from a broad range of fields were invited to discuss how these assumptions should be examined, and how the balance between the two interests should be assessed when conflicting with each other. The objective of the workshop was to broaden our understanding of various national and disciplinary approaches to the democratic balance between the right of access and the right to privacy.

Among the conclusions we may draw from the workshop, and the articles emanating from it, is the confirmation of the need to strike the balance between the right of access and the right to privacy. This is certainly difficult, but since the two interests are both of such importance for democracy, we constantly need to make the effort. The articles in this volume contain information on some of the areas that need our further attention.