SÖDERTÖRNS HÖGSKOLA | STOCKHOLM

Privacy, Digitalization, Rule of Law

Some Contemporary Challenges

PATRICIA JONASON (ED.)

Working paper 2021:1

ISSN 1404-1480 / ISBN 978-91-89109-42-1

Introduction

PATRICA JONASON

The articles in this volume[1] address challenges for several dimensions of the Rule of Law. Such dimensions are inter alia respect for human rights – in particular the right to privacy – and the quality and the prospectivity of the law.

Two key themes emerged from the contributions – written by public lawyers, an Archival scientist and a researcher on Information, Education and IT:

1. The challenges for the Rule of Law due to the need to balance the right to privacy with conflicting interests

2. The challenges for the Rule of Law generated by the digitalization of the society

Among the articles related to the first theme, *the challenges for the Rule of Law due to the need to balance the right to privacy with conflicting interests,* two of them examine a conflict between the right to privacy and the need of protection. In the first article titled 'The Right to Privacy vs Protection of the Public: Criminal Record Certificates in UK Law', Gordon Anthony, Professor of Public Law, examines case law on the powers of the police when individuals have been acquitted of offences and subsequently require a certificate (a so-called "Enhanced Criminal Records Certificates" (ECRCs), for certain lines of employment (for instance, with children or vulnerable adults). Examining, among other cases, the recent decision of the UK Supreme Court in *R v Chief Constable of Greater Manchester*, the article explains how the right to a private life can be limited in the public interest, as long as the police

[1] The articles have been presented during two workshops, *The Right to Privacy: between Constitutional and Practical Protection* organised by Patricia Jonason (May 22, 2017) and *Privacy, Data Protection and the Rule of Law in a Digital Age organised* by Anna Rosengren and Patricia Jonason (October 19, 2018) at Södertörn University. See also the articles by Anna Rosengren, "Power to the people – or privacy in peril? A linguistic-historical analysis of the meaning and boundaries of the Swedish principle of public access to official documents", *Working Paper* 2019:2 and "Swedish Analytica: Individuals' awareness of information about them held by Swedish public authorities, 1987–2017", *Working Paper* 2019:4.

adhere to the minimum requirements of legality and proportionality. It also notes how UK law has absorbed a range of European influences, as much of the case law of the UK courts focuses on the procedural and substantive dimensions of Article 8 ECHR.

In 'Fight Against Terrorism and Protection of Privacy in Algerian Law', Nasreddine Bousmaha, Professor of International Law, provides another illustration of a conflict between the right to privacy and the necessity to protect. The right to privacy in this case is to be balanced with the necessity of protecting society against terrorism. The author shows how the Algerian Government, which at the beginning used a military response for fighting terrorism and paid less attention to Human Rights, has gradually adopted a legal framework allowing the fight against terrorism in accordance with the law and inter alia with rules aiming at protecting privacy. The author takes the example of the countering of the financing of terrorism, where a new public body, the Financial Intelligence Processing Unit (FIPU), was endorsed with the task of protecting the privacy of individuals who were to be the subject to suspicious transactions or operations. When it concerns the fight against cybercrime, compliance with the principle of criminal legality comes into question.

The next two papers focus on another sort of conflict of interests involving privacy, i.e. a conflict between right to privacy on the one hand and transparency/open government on the other hand. In 'The Right to Privacy and the Right to Open Government: Two Antagonist Constitutional Rights', William Gilles, Professor in Public Law, investigates the contours of the rights at stake and their importance and value. The author, focusing then more specifically on the French example, goes on into the balancing the French legislator does in order to limit the infringements of the right to privacy towards the traditional access to information and towards the more recent right to open data. The author concludes that the French legislator gives precedence to the right to privacy. The technology, however, sometimes generates difficulty in protecting privacy. Moreover, the generalization of the anonymization process used for protecting privacy may conflict with the right to memory of future generations. Finally, the author tackles the delicate question of the privacy of political public figures.

The next paper, written by Patricia Jonason, Associate professor in Public Law, deals with a similar theme but with the focus on civil servants. In 'The Privacy of Public Officials in The Digital Age: A Democratic Issue' the author assesses the need, for both legal and ethical reasons, to guarantee the right to privacy of public officials. A balancing of interests between transparency and

privacy of civil servants has to be carried out bearing in mind that the respect of the right to privacy does not only serve the personal privacy interest of the civil servant concerned but even the interest of having a functioning democracy. With a Swedish example as the point of departure of – the publication on the Swedish Ombudsman's website of decisions containing the name of the public servant criticized in the decisions in question – Jonason examines the implications in terms of infringements of the privacy of the individual civil servant and for the democracy that such a release of personal information may have and incur. These deterrent impacts are undeniably exacerbated by the use of new technologies.

Under the second theme, *the challenges for the Rule of Law generated by the digitalization of the society*, the following papers fall. The first, 'Digitally Ready Legislation as a new Concept in Danish Law – An Erosion of the Rule of Law?' by Michael Gøtze, Professor of Administrative Law, questions the current phenomenon in Denmark according to which new legislation is designed to be digitally compatible from the very beginning in order to pave the way for use of digital solutions in the Danish administration. The author focuses on three main questions raised by this new concept: the challenge of striking a fair balance at a legislative level between discretionary and objective regulation, the inherent preference in digitally ready legislation for binary regulation and the question of the normative impact that technology has in the design of regulation and the choice of structure of rules.

In 'Paving the Way for Google Legal Certainty Implications for Legitimising Public Cloud Services in Swedish Schools', Maria Lindh, Senior Lecturer in Library and Information Science, discusses the tensions between surveillance of pupils, their right to privacy and their right to the use of free public cloud services. The author examines, by looking at formative documents, how the implementation and use of ICTs has been legitimated within the Swedish educational sector. Her aim is to unveil power structures that have shaped discourses about the implementation and use of ICTs within the Swedish educational system. According to Lindh there is a need for a critical discussion of the complexities that free cloud services' back end affordances involve and how these affordances structure pupils' personal data privacy.

In his article**,** 'Discussions in social media regarding the implementation of the General Data Protection Regulation', Rikard Friberg von Sydow, Senior Lecturer in Archival Science, shares his findings regarding the discourse on the new data protection legislation carried out on social media by

groups of professionals before the GDPR entered into force. Analysing the discussions which took place in three Facebook groups of professionals particularly impacted by this new legislation (archivists, IT-professionals and communicators in the public sector), the author concludes that the discussions witness confusion and very varying levels of insight in the new legislation. The difficulties encountered by the groups of professionals studied in understanding the content and the impact of the new legal framework raise even the crucial question of the practicability and efficiency of the European data protection legislation, and furthermore, the question of the respect for the Rule of Law.

Contents

Managing Risk in the UK:
Enhanced Criminal Record Certificates and the Right to Private Life
GORDON ANTHONY
9

Fight Against Terrorism and Protection
of Privacy in Algerian Law
NASREDDINE BOUSMAHA
21

The Right to Privacy and the Right to Open Government:
Two Antagonist Constitutional Rights?
WILLIAM GILLES
29

The Privacy of Public Officials in the Digital Age:
A Democratic Issue
PATRICIA JONASON
43

Digitally Ready Legislation as a New Concept in Danish Law
– An Erosion of the Rule of Law?
MICHAEL GØTZE
67

Paving the Way for Google
– Legal Certainty Implications for Legitimising Public Cloud Services in Swedish Schools
MARIA LINDH
79

Discussions in Social Media Regarding the Implementation
of the General Data Protection Regulation
RIKARD FRIBERG VON SYDOW
105

Contributors
131

Managing Risk in the UK: Enhanced Criminal Record Certificates and the Right to Private Life

GORDON ANTHONY*

This is a (short) article about risk management in the UK and how a balance is stuck between, on the one hand, an individual's right to private life and, on the other hand, the need to protect vulnerable members of society from potential harms. Its focus is on the role of so-called "Enhanced Criminal Records Certificates" (ECRCs), which are issued by the police when an individual seeks employment in spheres that include education, private transport services, and health provision. The legal framework for ECRCs is found in section 113B of the Police Act 1997, as read with section 6 of the UK's Human Rights Act 1998 and the right to private life under Article 8 of the European Convention on Human Rights (ECHR).[1] While the law on ECRCs is largely unremarkable when they include details about convictions for criminal offences – albeit there can be questions about the relevance of some older convictions[2] – the matter becomes more complex when the police disclose information about criminal charges that resulted in an acquittal. Section 113B here gives the police a discretion to disclose to a potential employer any information about an individual where the police reasonably believe that the information might be relevant to the position for which the individual has applied. It is a discretion that can have far-reaching implications: certain types of criminal charges – for instance, as relate to sex offences – will carry a social stigma and disclosure may deal a "killer blow" to the individual's prospect of employment in their preferred field.[3]

* Professor of Public Law, Queen's University, Belfast. This is a revised and updated version of a paper on privacy that was first presented at a workshop at Södertöns University, Stockholm on 22 May 2017. My thanks to Professor Jonason for her invitation to the workshop and for her patience when commissioning this paper.

[1] On the Act, and its relationship to the ECHR, see M Amos, *Human Rights Law* (Hart Publishing, Oxford, 2nd ed, 2014).

[2] See, e.g., *In re Gallagher* [2019] UKSC 3, [2020] AC 185, considering the law on "spent" convictions under the Rehabilitation of Offenders Act 1974 and the Rehabilitation of Offenders (Northern Ireland) Order 1978.

[3] For the term "killer blow" see *R (L) v Commissioner of Police for the Metropolis* [2009] UKSC 3, [2010] 1 AC 410, 440, para 75, Lord Neuberger.

The article analyses the current state of the law with reference to the UK Supreme Court's recent ruling in *R (R) v Chief Constable of Greater Manchester Police* (hereafter: "*R*").[4] *R* was a case in which a man who had been working as a taxi driver was charged with the rape of a female passenger but was acquitted after a trial at which both he and his alleged victim had given evidence. The man – who was also a qualified teacher – later applied for a job as a lecturer at a further education college, in circumstances where he was required to provide his prospective employer with an ECRC. When considering the matter, the police determined that it was reasonable and proportionate to make known to the college information about the charges against *R*, precisely because he would be working with young women who may thereby be placed in a vulnerable position. On having later applied for another taxi licence and been given a further ECRC with the same disclosure, the man challenged the police's decision as contrary to, among other things, Article 8 ECHR. While the Supreme Court noted some concerns about how the law on ECRCs can operate – considered below – it concluded that the interference with his right to private life was justified on the facts of the case. The system for ECRCs thus remains largely unsettled and the right to privacy curtailed.

The article begins with a short section that considers some earlier case law on ECRCs and how the law had developed to the time of *R*. It then examines the finding in *R* in more detail, including some comments which were made by way of a post-script to the judgment and which identified something a "loose thread" in the law. The conclusion offers some more general comments about the law in this area and the balance that is struck between an individual's right to privacy and the need to protect others from potential harms.

Section 113B of the Police Act 1997: the initial case law

Section 113B was inserted into the Act of 1997 in 2005 by way of an addition to the original Act.[5] As a policy development, it is often associated with attempts to close a legal loop-hole that had allowed a convicted sex offender to obtain a caretaking job at a school in England, where he went to sexually

[4] [2018] USC 47, [2018] 1 WLR 4079.

[5] Serious Organised Crime and Police Act 2005, s 163. It should be noted that section 113B, as inserted, contains sub-headings on the law in England and Wales, Scotland, and Northern Ireland. The focus of this article is on the law as applies in England and Wales.

assault and murder two schoolgirls.[6] Formally, applications for ECRCs are made to the Disclosure and Barring Service ("DBS") in England and Wales, a body which was established by statute in 2012.[7] By section 113B(3), an ECRC "is a certificate which: (a) gives the prescribed details of every relevant matter relating to the applicant which is recorded in central records … or (b) states that there is no such matter or information". A certificate so defined can, *per* section 113B(4), be issued only once the DBS has requested the police "to provide any information which (a) the [police reasonably believe] to be relevant … and (b) … ought to be included in the certificate". Where the DBS/police propose to disclose information on a certificate, the individual can now challenge that decision by bringing it to the attention of the so-called "Independent Monitor".[8] Challenges thereafter are by way of an application for judicial review.

The nature of the police's powers under section 113B was first considered in detail by the Supreme Court in the case of *R (L) v Commissioner of Police for the Metropolis*.[9] The applicant in L had been working as an assistant at a school where she supervised children during lunchtime. She lost her job when an ECRC obtained by her employer revealed that, whilst she had no criminal convictions, her son had been placed on the child protection register as a person who was at risk of neglect (he had later gone on to commit a criminal offence). The applicant challenged the disclosure of this information as contrary to her rights under Article 8 ECHR, where she argued that the decision of the police was disproportionate in the circumstances. Her application to the High Court was dismissed, as was her appeal to the Court of Appeal. She likewise failed in her appeal to the Supreme Court.

The Supreme Court began its judgment by accepting that the challenged decision interfered with L's rights under Article 8 ECHR and proceeded to analyse the case on that basis. In doing so, it established two core points about the workings of the ECRC system. The first concerned the role of the proportionality principle, which had been key to the applicant's arguments on appeal. While the Court acknowledged that disclosure may often deal a

[6] See E Johnson, 'Why is it so important to complete DBS checks?', at https://cpdonline.co.uk/knowledge-base/safeguarding/important-dbs-checks-safer-recruitment/.

[7] *Viz*, under the Protection of Freedoms Act 2012, s 87 and Sch 8.

[8] Police Act 1997, ss 117A and 119B.

[9] [2009] UKSC 3, [2010] 1 AC 410. Note that the powers in this case were under s 115(7) of the Police Act 1997, which was later repealed and re-enacted in substantially the same terms by s 113B(4): Serious Organised Crime and Police Act 2005, s 163.

"killer blow" to an individual's hopes of working in their preferred field, it ruled that section 113B(4) does not violate the right to privacy in and of itself, as the words "ought to be included" can be read and given effect in a way which is compatible with Article 8 rights.[10] This meant that the issue became one about how the police are to strike the balance between an individual's rights and those of third parties such as, in this instance, school children. In a much-cited part of the judgment, Lord Neuberger said that the question of whether disclosure would be proportionate would depend upon a number of contextual factors, including:

> the gravity of the material involved, the reliability of the information on which it is based, whether the applicant has had a chance to rebut the information, the relevance of the material to the particular job application, the period that has elapsed since the relevant events occurred, and the impact on the applicant of including the material in the ECRC, both in terms of her prospects of obtaining the post in question and more generally".[11]

The second point concerned the matter of procedural fairness, where the Supreme Court implied that procedural failings could in themselves give rise to a breach of Article 8 ECHR. This was a not insignificant line of reasoning in the case, as the scope for procedural protection of rights had not always been clear either in case law under the Human Rights Act 1998 or in the case law of the European Court of Human Rights itself.[12] However, for Lord Neuberger, the nature of decision-making in relation to ECRCs was such that individuals should often be given an opportunity to make representations about any proposed disclosure, as, "Otherwise, in such cases, the applicant's article 8 rights will not have been properly protected".[13] While Lord Neuberger noted that it would be impossible to be "prescriptive" about when representations would be required, he equally noted that, where the deciding officer "is doubtful as to information's potential relevance to the post for which the applicant has applied, or where the information is historical or vague, it would often, indeed perhaps norm-

[10] For the phrase "killer blow" see [2010] 1 AC 410, 440, para 75, Lord Neuberger.
[11] [2010] 1 AC 410, 442, para 81.
[12] For earlier domestic authorities suggesting that procedural failings need not render a decision unlawful if the final decision itself is consistent with human rights principles see, *Belfast City Council v. Miss Behavin' Ltd* [2007] UKHL 19, [2007] 1 WLR 1420 and *SB v Denbigh High School* case [2006] 15, UKHL [2007] 1 AC 100. But compare, e.g., *Manchester City Council v Pinnock (Nos 1 & 2)* [2010] UKSC 45, [2011] 2 AC 104; and on the developing law of the ECHR see J. Gerards and E. Brems (eds), *Procedural Review in European fundamental rights cases* (Cambridge University Press, 2017).
[13] [2010] 1 AC 410, 442, para 82.

ally, be wrong to include it in an ECRC without first giving the applicant an opportunity to say why it should not be included".[14] Of course, taken to its logical conclusion, this means that an individual should also be entitled to withdraw an application for an ECRC should they prefer for any disputed information to remain private.[15]

The nature of the procedural dimension to the ECRC process was subsequently considered in a number of cases which predated *R*, of which three might be noted. The first was *R (RK) v Chief Constable of South Yorkshire Police*.[16] In this case, the applicant had been charged with, and acquitted of, offences against pupils in a school at which he had been working some eight years previously. He had since been involved in a lengthy dispute with the respondent police force about whether it was proportionate for its Chief Constable to disclose the fact of his trial on an ECRC and whether the police force had been acting in accordance with the proportionality principle when assessing evidence for the purposes of disclosure. On the facts, the judge, Coulson J., found that it had not: South Yorkshire Police had "grudgingly noted the acquittal and then gone on to address the allegations as if they had been proved",[17] and "they plainly believe that the claimant was fortunate to be acquitted and they have decided that they will treat the allegations as 'substantiated' (to use their word) in any event".[18] For the Court, "That blinkered view" hampered the police all the way through the process and meant that they could not have engaged in "a proper assessment of proportionality".[19]

The second case was *R (A) v Chief Constable of Kent*, which was an appeal against a High Court ruling that the respondent Chief Constable had acted unlawfully when disclosing information about allegations against a nurse.[20] The ruling in the High Court had noted a number of procedural deficiencies leading up to the disclosure, and these were said to have rendered the disclosure decision unlawful. Dismissing an appeal against that finding, the Court of Appeal referenced a number of domestic authori-

[14] Ibid.
[15] *Re JR59's Application* [2012] NIQB 66. Note that, while this case was decided in Northern Ireland, the legislative scheme that applies there is essentially at one with that in England and Wales. See further n 5 above.
[16] [2013] EWHC 1555 (Admin).
[17] [2013] EWHC 1555 (Admin), para 37.
[18] [2013] EWHC 1555 (Admin), para 65.
[19] [2013] EWHC 1555 (Admin), para 65.
[20] [2013] EWCA Civ 1706.

ties that had held that procedural defects need not mean that a decision is unlawful if the final decision itself does not have disproportionate effects.[21] However, the Court also referred to a number of other authorities which suggested that procedural failings could infect final decisions, notably where it was difficult to disentangle procedural aspects of the decision from the substantive.[22] Applying that reasoning to the facts of the case before it, the Court of Appeal said:

> The present case is also one in which it can be said that substance and procedure are difficult to disentangle. I have stated that I consider the balancing process where a Chief Constable is considering disclosing an unsubstantiated allegation in an ECRC to be a sensitive and not straightforward process. In the present case, the matters not taken into account included the requirement in … statutory disclosure guidance to consider whether there are 'any specific circumstances' which might have led the decision-maker to conclude that 'the information is unlikely to be true'. The specific circumstances included the evidence of resentment by two of those who complained about A, and of a racist remark about her by one of them. The requirements of the statutory disclosure guidance may put the present case into the same category [of case] in which a defective decision-making process is of some relevance.[23]

The third case was *R (MS) v Independent Monitor of the Home Office*.[24] The claimant here had sought to return to work as a taxi driver and became involved in a dispute about the police's proposal to disclose information about a number of historic and unsubstantiated allegations of indecency towards women. The matter was referred to the Independent Monitor who upheld the proposed disclosure without, in the claimant's view, properly engaging with disputed issues of facts. The High Court held that the Independent Monitor had thereby acted unlawfully because he "was obliged himself to scrutinise with a high degree of forensic care the material which is said to incriminate the claimant. He must then assess its weight with care. Only once he has reached a considered conclusion as to its weight can he

[21] [2013] EWCA Civ 1706, paras 44–47, considering *Miss Behavin'* and *Denbigh High School*, cited at n 12 above.
[22] [2013] EWCA Civ 1706, paras 48–52, considering *R (Laporte) v Chief Constable of Gloucestershire* [2006] UKHL 55, [2007] 2 AC 105 and *R (E) v Governing Body of JFS School* [2009] UKSC 15, [2010] 2 AC 728.
[23] [2013] EWCA Civ 1706, para 53. For subsequent, positive consideration of *Kent* see *R (SD) v Chief Constable of North Yorkshire* [2017] EWCA Civ 1838.
[24] [2016] EWHC 655 (Admin), [2016] 4 WLR 88.

then undertake the balancing exercise necessary to justify an interference with the claimant's article 8 rights".[25]

R (R) v Chief Constable of Greater Manchester Police

It is against this backdrop that the judgment in *R* falls to be considered. As noted above, the applicant in this case had been charged with rape whilst he had been working as a taxi driver. The allegation against him had been made by a young woman who had been one of his passengers, but he had denied that there had been any sexual contact between them. At trial, there was no forensic evidence to support or undermine the allegation of rape, and both *R* and the complainant gave evidence before he was acquitted by the jury. The date of his acquittal was January 2011 and, two months later, he applied for an ECRC in connection with his attempt to obtain a post as a lecturer. The ECRC that was subsequently issued by the police contained a statement about R's rape charge and acquittal. R, who had made representations to the police before the ECRC was issued, asked for an internal police review, but this concluded that the disclosure was reasonable and proportionate. Unable to work as a lecturer, *R* then applied for a further ECRC in 2012 so that he might again work as a taxi driver. He did not make representations on this occasion, and the second version contained the same details as the first. After the chosen form of words was again confirmed on review, *R* initiated legal proceedings to challenge the disclosure as contrary to, among other things, both the procedural and substantive dimensions to Article 8 ECHR. (The facts of the case apparently pre-dated the creation of the statutory position of Independent Monitor that was noted above – the disclosure thus could not have been referred to that body.)

The case was first heard by the High Court, which rejected R's arguments. While the High Court accepted that disclosure of the acquittal interfered with R's rights under Article 8 ECHR, it held that the disclosure was reasonable and proportionate given the need to protect others from potential harms.[26] On appeal, the Court of Appeal held the High Court's ruling on the proportionality of the interference was the correct one and that the substance of the Article 8 right therefore had not been breached. Moreover, on the question of whether there had been a breach of the

[25] [2016] EWHC 655 (Admin), [2016] 4 WLR 88, para 51.
[26] [2013] EWHC 2721 (Admin).

procedural dimension to Article 8 ECHR given the lack of consultation in relation to the second ECRC, the Court of Appeal held that there had not. In a paragraph that was later referenced by the Supreme Court, McCombe LJ said:

> I do not consider that overall what occurred in this case resulted in a breach of the procedural requirements of Article 8, bearing in mind the principles emerging from the *L* case. This was not a borderline case of relevance so far as the nature of the information was concerned. Indeed, no such argument was presented on the appellant's behalf. Further, the appellant had lodged his complaint in relation to the first certificate, raising points with regard to what he argued to be the manifest unreliability of the allegations having regard to his acquittal, and, in general terms, as to the employment difficulties caused by the disclosures. However, there had been no legal challenge to the first certificate. The second certificate was applied for with a view to a post in the very occupation in which the incident giving rise to the allegation had arisen. No specific new considerations appear to have been raised by the appellant at the time when the certificate was applied for and the appellant has not, in the course of these proceedings, alluded to any matter that he would have raised if he had been consulted in March 2012. The points raised in his initial complaint about the first certificate were considered again. It is to be recalled further that an application for an ECRC is made in relation to a specific post and no points were raised that would indicate that disclosure on this certificate would impact upon the appellant's employment in posts for which such a certificate was not required.[27]

The Supreme Court began its judgment by considering the legal framework governing ECRCs, the facts of R's case, and the judgments of the High Court and Court of Appeal. The judgment then considered the nature of guidance that had been given to police officers who deal with questions of disclosure, where the picture was said by the Court to be "not entirely clear or consistent".[28] This was an issue that was to assume an added importance at the very end of the judgment, as Lord Carnwath (giving the judgment of the Court) noted some potential difficulties with guidance on the ECRC system, notably as relates to individuals who have been acquitted of charges. However, before addressing that issue, the Court had to consider whether R had any sustainable grounds of appeal, which it held he did not. On the question of procedural fairness, the Supreme Court held that the Court of Appeal's reasoning – encapsulated in the above quotation – had been cor-

[27] [2016] EWCA Civ 490, [2016] 1 WLR 4125, 4151, para 66.
[28] [2018] 1 WLR 4079, 4093, para 30.

rect and that it could not improve upon it. In doing so, the Supreme Court said that the "complaint in essence is of lack of consultation" and that it had been "rightly rejected". This was because, on the facts, the police had a full understanding of the issues and the implications for R's employment prospects, where "there was no indication of any further information he would have wished to advance".[29]

The Court next considered whether the disclosure had been disproportionate, where R argued that the police should have examined more closely the evidence from the criminal trial and formed their own view about guilt. Rejecting that argument, the Supreme Court held that section 113B does not require the police to replicate the role of judge and jury, but rather "to identify and disclose relevant 'information', not to make a separate assessment of the evidence at the trial".[30] Holding that the police had discharged that task, Lord Carnwath concluded that they had been entitled to make the disclosure in question. His Lordship also noted some of the practical realities that might have followed from any non-disclosure decision that could have been taken by the police:

> It is to be borne in mind that the information about the charge and acquittal was in no way secret. It was a matter of public record, and might have come to a potential employer's knowledge from other sources. If so, a reasonable employer would have been expected to want to ask further questions and make further inquiries before proceeding with an offer of employment.[31]

Somewhat unusually, the Supreme Court's judgment contained a postscript, and this was used to address the issue of guidance on acquittals. The Court's initial query about guidance had concerned the nature of that which is given to the police and prospective employers when there has been an acquittal, where the existing guidance was sparse, at best. While Lord Carnwath did not consider that R's case stood or fell on the issue of guidance, his case was said to give "rise to more general concerns about the ECRC procedure in similar circumstances … so far as can be judged from the material before us, little attention has been given to the conceptual and practical issues arising from the relationship of the procedure to criminal proceedings".[32] Noting that the legislative framework permits the police to

[29] [2018] 1 WLR 4079, 4102, para 66.
[30] [2018] 1 WLR 4079, 4103, para 68.
[31] [2018] 1 WLR 4079, 4104, para 70.
[32] [2018] 1 WLR 4079, 4104, para 72.

disclose "soft" information, including about disputed allegations, Lord Carnwath acknowledged that acquittal after a full trial may "imply no more than that the charge has not been proved beyond reasonable doubt … it leaves open the possibility that the allegation was true, and the risks associated with that".[33] However, his Lordship also outlined his concerns about the lack of information about how employers view ECRCs in practice and whether they do, in fact, deal "killer blows" to employment prospects. On this point, he added that the Court had "been shown reports which emphasise the importance of not excluding the convicted from consideration for employment, but they say nothing about the acquitted, who surely deserve great protection from unfair stigmatisation".[34] For his Lordship, the corresponding danger was that even those ECRCs which are expressed in "entirely neutral terms" may still lead an employer to "infer that the disclosure would not have been made unless the chief officer had formed a view of likely guilt".[35]

This is, of course, the "loose thread" in the law that was mentioned in the introduction to this article, and Lord Carnwath concluded his judgment by stating: "Careful thought needs to be given to the value in practice of disclosing allegations which have been tested in court and have led to acquittal".[36] Interestingly, in the time since the Supreme Court delivered its ruling, fresh guidance on acquittals does not yet appear to have been published, albeit it can be expected that it will issue at some time in the near future. When such guidance finally comes, it may be another important element in the non-exhaustive list of factors that Lord Neuberger identified as relevant to proportionality in the earlier case of *L*, as quoted above. Indeed, in the absence of such guidance, it may well be that the uncertainty in the law might only continue and result in a further challenge based upon Article 8 ECHR's "quality of law" requirement – that is, the requirement that individuals should be able to understand clearly how their rights may (or may not) be interfered with.[37]

[33] [2018] 1 WLR 4079, 4104, para 74.
[34] [2018] 1 WLR 4079, 4105, para 75.
[35] [2018] 1 WLR 4079, 4105, para 75.
[36] [2018] 1 WLR 4079, 4105, para 75.
[37] On which requirement see *In re Gallagher* [2019] UKSC 3, [2020] AC 185.

Conclusion

This article has provided a brief overview of the law on ECRCs in the UK, as impact upon the right to private life. It has considered the leading case law on section 113B of the Police Act 1997 and how the ECRC procedure can be made to operate in a manner that it is consistent with Article 8 ECHR. While the existence of statutory discretion means that applications for ECRCs will (of course) always be assessed on a case-by-case basis, the law now requires minimum procedural protections as well as a carefully balanced approach to any final decision about disclosure. In the context of applications that are made by individuals who have been acquitted of criminal charges, these requirements can raise particularly challenging questions about how to manage risk, and there will inevitably be cases in which the police will act unlawfully. There will, however, equally be cases in which police disclosure will be lawful and where the individual will be required to carry the burden of the public interest in protecting others from potential harm. In the final scenario, that is in the very essence of qualified human rights standards wherein the rights of the individual intersect with the rights and freedoms of others.

Fight against Terrorism and Protection of Privacy in Algerian Law

NASREDDINE BOUSMAHA[1]

Following a black decade, that caused the deaths of tens of thousands of people, plus hundreds of thousands injured, Algeria knew how to find her way out of the red zone of the countries particularly affected by terrorism. Henceforth, Algeria is classified within the same category as European countries, and the United States of America.[2] Algeria has moved from the all-out fight against terrorism to the management of the terrorism threat.

Things were not that simple during the 1990s; the Algerian State through its institutions, its security services, and the Algerian society as a whole was not prepared to face such a challenge. Moreover, not even international society had a strategy. It would have to wait for the 9/11 attacks to take the terrorism threat as it really is. As a result of this event and the multiple attacks that have affected several Western countries, which have been constantly spared from the terrorism threat, the United Nations Organization was able to adopt its global counter-terrorism strategy, in order to coordinate the efforts of States Parties.[3]

As a consequence of the absence of such a strategy, at the international level as well as the internal level, Algeria opted for the policy of "total security" during the 1990s. Rapidly, the Country sinks into chaos, clashes between the security forces and armed groups are extremely violent, giving way to confusion, terror and division. During this period, respect for human rights was far from being a priority, the primary concern under these conditions was to avoid the total collapse of the country.

The allegations of human rights violations are multiplying, the Algerian government is under increasing pressure from the international community. This government will eventually notice that military response alone cannot effectively combat terrorism, without a global strategy that will take

[1] *Professor of International Law, Faculty of Law and Political Science, University of Oran 2 -Algeria*

[2]Massi M. « Pays impactés par le terrorisme/ L'Algérie sort de la zone rouge » in. politique, 20 novembre 2016. http://www.algerie-focus.com/2016/11/pays-impactes-terrorisme-lalgerie-passe-de-sortir-de-zone-rouge/amp/

[3] A/RES/60/288. La Stratégie antiterroriste mondiale de l'Organisation des Nations Unies. Soixantième session. Distr. Générale 20 septembre 2006.

into consideration the protection and respect for human rights. Gradually, Algeria developed a legal framework, allowing the fight against terrorism in accordance with the law.

The process was launched by President *Liamine Zeroual*, with his clemency act called "Rahma", aiming for the forgiveness and repentance of members of armed groups. This act will soon be transferred into the act of "civil concord" with the election of president *Abdelazziz Bouteflika* in 1999, with more flexible criteria, to better facilitate the reintegration of anyone who decides to renounce the use of armed violence. Given the success of these two acts, a referendum will be held in 2005 for the adoption of the "Charter for Peace and National Reconciliation", followed by several implementing legislations that are mainly aimed at moving on and bringing closure, by granting a general amnesty,[4] for persons who have not committed blood crimes or rape.[5]

This policy enabled more than 7000 persons to lay down their weapons, which is an indisputable success for restoring peace in the country, still far from having eradicated definitively the terrorism threat. Henceforth, Algeria will have to continue its fight against terrorism as part of a global strategy, in a society that has evolved considerably from the 1990s, and the very change in the nature of the terrorism threat.

For this purpose, Algeria should make every effort to improve its preventive and counter-terrorism measures, to make it more effective and in accordance with the international law,[6] particularly to establish a mechanism for combating the financing of terrorism (I) and the use of modern means of communication and websites in the recruitment and radicalization activities to the benefit of terrorist groups[7](II).

[4] Hassane ZERROUKY «l'Algérie après la charte pour la paix et la réconciliation nationale ». In Recherches internationales, n° 75, 1 - 2006, p. 26.

[5] The Charter for Peace and National Reconciliation reiterates the provisions of the 1999 Civil Concord Act, which provides the halting of trials and pardons of Islamists whom would lay down their arms and surrender themselves to the authorities, on the condition that they have not committed any blood crimes or rape.

[6] Ministère des Finances. Cellule de Traitement du Renseignement Financier «Dispositif national de lutte contre le blanchiment d'argent et le financement du terrorisme (LBA/FT) » p. 3.

[7] Discours de Mr. Mourad Médelci: Ministre des affaires étrangères, devant le Colloque du Secrétaire général des: Nations Unies sur fa. Lutte contre Ce terrorisme. 66ème session de l'assemblée générale des nations unies. 19 septembre 2011, Séance N° 2. Thème « Promouvoir le dialogue, comprendre l'attirance exercée par le terrorisme et lutté contre cette attirance ». p. 3.

Countering the financing of terrorism

Countering the financing of terrorism is a priority for the Algerian State. A priority justified by the ability of terrorist groups to carry out their criminal activities according to the amount of financial resources at their disposal. Moreover, the efforts of the international community in that direction, illustrate perfectly the importance of this struggle, which is situated at the intersection of the police (and intelligence), judicial, diplomatic and financial universes. And in order to be successful, this policy should be based on a genuine cooperation and participation, between the public and private sectors.[8]

In this context, it is worth recalling that Algeria was one of the first countries to have taken into consideration the danger of this type of financing, and reacted quickly by penalizing the act of financing terrorism by the Ordinance 95-11 amending and supplementing the Criminal Code. According to article 87 bis 4, all acts of financing, by any means whatsoever, shall be punishable by prison terms of between 5 and 10 years, plus a fine.

The determination was clear, but largely inadequate; only one article was consecrated to criminalize the financing of terrorism, without determining the acts that may constitute the offense, nor the procedures to be followed to prevent such acts. Combatting the financing of terrorism during the 1990s was part of the assignments of the security services and the justice, which was not qualified at the time to carry out an effective fight.

The collection, processing, analysis and use of information in connection with investigations for the financing of terrorism, usually have been operated informally, if not downright in hiding. Respect for privacy was not a priority, and some people have experienced this.

In this context, it is also important to note that the Algerian authorities were in a state of paralysis, faced with a terrorism financing that found part of its resources in some European capitals. This was mainly due to the lack of cooperation between the two rims of the Mediterranean, yet even more serious is the unofficial embargo that Algeria had been going through, during the black decade.

It would have to wait for the 9/11 attacks, until combating the financing of terrorism is no longer considered the poor relation of the global fight

[8] Anthony AMICELLE, « Etat des lieux de la lutte contre le financement du terrorisme: entre critiques et recommandations », Cultures & Conflits [En ligne], 71 | automne 2008, mis en ligne le 05 février 2009, consulté le 01 octobre 2016. URL: http://conflits.revues.org/16773; DOI: 10.4000/conflits.16773

against terrorism[9]. The reaction of the international community to the attacks of September 11th did not take long:

- The Security Council, through its resolution 1373, made a direct appeal to States, to become a member of the United Nations Convention for the Suppression of the Financing of Terrorism of 9 December 1999[10]. Entered into force on 10 April 2002.
- The creation of the Financial Action Task Force (FATF) In October 2001, to coordinate the efforts of States in combating money-laundering and the financing of terrorism.
- The development of the Financial Intelligence Units (FIU) in each Member State on the European continent, and in the countries cooperating with the EU.
- At the African level, the OAU Convention on the Prevention and Combating of Terrorism was signed at Algiers on 14 June 1999, and came into force on 6 December 2002.
- At the level of the Arab world, the late adoption of the Arab Convention for Combating Money Laundering and the Financing of Terrorism, signed on 21 December 2010, entered into force on 05 October 2013. The same Convention ratified by Algeria on 18 October 2014.

In this context, Algeria has implemented its own mechanism for combating money-laundering and financing of terrorism, by integrating international standards into the domestic law, more precisely[11]:

- The Charter of the United Nations,
- Resolutions of the United Nations Security Council,
- International conventions,
- FATF Recommendations.

[9] La lutte contre le financement du terrorisme : Beaucoup de bruit pour rien ? p. 2. www.frstrategie.org/publications/autres/dossiers/2011/aqmi/doc/finance.pdf. Consulté le 14/11/2020.

[10] « De devenir dès que possible parties aux conventions et protocoles internationaux relatifs au terrorisme, y compris la Convention internationale pour la répression du financement du terrorisme en date du 9 décembre 1999 ».

[11] Ministère des Finances. Cellule de Traitement du Renseignement Financier «Dispositif national de lutte contre le blanchiment d'argent et le financement du terrorisme (LBA/FT) » p. 2.

Indeed, it was in 2002 that Algeria was able to create its first competent body for the prevention of money laundering and the fight against the financing of terrorism, by the Executive Decree No. 02-127 of 07 April 2002. Under the supervision of the Minister of Finance, the Financial Intelligence Processing Unit (FIPU) is responsible for "*processing financial information gathered through declarations of suspicion from financial institutions and non-financial professions (notaries, lawyers, bailiffs, auctioneers, accounting experts, auditors, customs brokers, intermediaries in stock exchange transactions, real estate agents, car dealers, etc.), concerning suspicious transactions or operations* ". The (FIPU) also works in collaboration with the competent bodies for the drafting of laws and regulations in the field of its competences. In short, it is the same attributions as the existing units, in about a hundred countries in the world.

It is the responsibility of the Financial Intelligence Processing Unit (FIPU) to protect the privacy of individuals who will be made subject to suspicious transactions or operations, in accordance with the 40 recommendations of the Financial Action Task Force (FATF), which applies to all the competent authorities, in the context of a national inquiry or of international cooperation and exchange of information, to ensure respect for the privacy of individuals.

Criminal-law protection against any intrusion into the privacy of individuals' private lives is ensured by Article 226–2 of the Criminal Code and not by the provisions of the 1881 Act which penalize the offenses of the press. The difference for overlapping infringements often appears paradoxical to more than one commentator.

A number of fundamental rights are inseparable from the human personality. These include the right to the name, the right to physical integrity, the author's moral right, and in the field which interests us, the right to image, the right to honour or the right to secrecy.

The Financial Intelligence Processing Unit (FIPU) must ensure a level of confidentiality, appropriate to any request for cooperation and information exchanged, in order to protect the integrity of investigations or information retrieval, within the respect for privacy and data protection. The Financial Intelligence Processing Unit (FIPU) should, as a minimum, protect the information exchanged in the same way as it protects similar information received from national sources.

The Financial Intelligence Processing Unit (FIPU) should establish controls and protection measures to ensure that the information exchanged by the competent authorities is used only in the authorized manner. The

exchange of information should be done in a secure manner and through reliable channels or mechanisms. If necessary, The Financial Intelligence Processing Unit (FIPU) may refuse to provide the information, if the requesting competent authority is unable to protect this information effectively.

The fight against cybercrime

This is another area in which Algeria had lagged far behind in developing a legal framework, which would also make it possible to better combat terrorism, while respecting the law. Therefore, mindful of the latest developments, and absolutely determined to adapt to the new propaganda and operational methods of terrorists on the internet and social networks, Algeria has recently focused on the use of information and communication technologies for terrorism purposes, for providing a penalizing response.

This was the case in June 2016, when the President of the Republic promulgated, following adoption of the Parliament, Law 16-02, more precisely, Article 87 bis 12, which dealt with the subject.

The latter describes the act as a crime and provides for a prison term of 5 to 10 years and a fine between 100,000 Algerian dinars, and 500,000 Algerian dinars. The provision in question lays down the relevant acts liable to sanctions and which are the following:

- Recruitment on behalf of a terrorist, association, body, group or organization;
- Support for acts or activities;
- The dissemination of ideas in a direct or indirect way.

However, a simple reading will make a jurist, without being a criminal law specialist, to notice that the text has been drafted in haste, in order to compensate for the shortcomings and normative failures in this matter.

Indeed, the law is highly debatable and questionable because the legislator does not provide any definition of the areas of ICT concerned, implicitly obliging the college of magistrates to be inspired by the previous Decree 15-261 on ICT offenses, referred to in my first section, and subsequently to reconcile the two texts and proceed to a judicial construction in order to be able to make a decision. In reality, this is an infringement of the cardinal principle of criminal legality, for it must be remembered that the

criminal judge is forbidden from any creative power, and that the obligation to interpret the law strictly lies upon him.

Consequently, repressed acts pose practical difficulties as a result of the contingency they generate, once the Judge attempts to implement them; we can put this as a second infringement of the principle of criminal legality, since the legislator has the obligation to draw up specific texts.

The substantial criticisms that we can retain are:

- Recruitment
  Criticism: Should we exclude Proposals, Offers?! Or even the talks, or the exchanges not yet completed since the recruitment did not take place. And in application of the rule, the doubt is interpreted to the benefit of the defendant.

- Support
  Criticism: What types of support are covered by the text? The term remains very ambiguous, as it is complex to fix the boundary between the accomplice (help and assistance) and the author.

- Direct or indirect dissemination
  Criticism: While direct dissemination does not appear to pose problems (dissemination to show the public the atrocities, etc. repression or not?); the indirect one is dangerous by its generality, it is the typical example of the dissemination to be condemned. The companies holding exchange servers open to the public in which the files (images, audios or videos) are dropped or disseminated, even if the practice or the use make them intended to be so, due to the density and flow of internet exchanges, are they directly responsible in case that the files were manifested and the company did not withdraw them or refuse to remove them after a formal request has been received?

However, I think it is regrettable that in terms of acts, the recurrent and usual consultation of a terrorist interface (site, page, blog, application, etc.) has not been taken into consideration, regarding its high risk of psychological impact on the person.

The same is true of the provocation of terrorism, which has apparently not interested the legislator, even though the act is of major importance and cannot be neglected.

There is also another problem external to the text, it is the specialization of the magistrates; there are no specialized centres, be it from the level of the prosecution or trial judges.

The Right to Privacy and the Right to Open Government: Two Antagonist Constitutional Rights?

WILLIAM GILLES [1]

Last year, while we were discussing about the place of public law regarding private law, Professor Jonason developed arguments to explain how much public law is the future of Law. I must admit that I fully agree with her, especially due to the fact that our future corresponds to a digital society. Indeed, the digitalization creates the need to assert human rights and rules of ethics that are at the core of public law. The digital society also strengthens the need for regulation, that covers both public law and private law.[2]

It is not common to start a paper by remembering a discussion we had with a colleague, especially when this colleague is the one who supervises the publication of the book in which the paper is published. However, this point of view seems very accurate and relevant to illustrate how public law has become a major issue in our digital society. And both the right to privacy and the right to open government are among the public law components that are crucial to regulating the digital society. In 2014, the UK Shadow (Labour) Minister for Digital Government explained that: "We need to embed trust, ethics and security into digital services. To achieve this we urgently need an investigation into 'data and society' that openly and honestly [recognizes] the challenges of handling and [analysing] personal data; that assesses the true benefits and limitations of big data and open data; and that defines a set of principles/rights and builds a new legislative framework to enshrine those rights in law."[3] The issue is however to articulate them. Indeed, both are essential, but each of them can come into conflict with the other one.

[1] Associate Professor at the Sorbonne Law School, President of IMODEV.

[2] Marie-Anne Frison-Roche, « Le droit de la régulation », *Dalloz*, 2001, n° 7. See also Bertrand du Marais, « Le consentement du droit public à la "régulation", une lecture du Rapport 2001 du Conseil d'État », *Droit 21*, 2001, Chr., AJ 457.

[3] UK Labor Shadow Minister for Digital Government, *Making Digital Government Work for Everyone*, 25 November 2014, accessed at : http://archived.org.uk/digitalgovernmentreview/.

§ 1 –The Right to Open Government and the Right to Privacy as Fundamental Rights in a Digital Society

The Advent of a Right to Open Government

Popularized by President Obama in 2009,[4] "the term 'open government' refers to the development of approaches aimed at publishing, on the Internet, data concerning governmental action in order to favour a greater participation of citizens, of civil servants or other stakeholders involved in the implementation of public policies."[5] In other words, open Government means the right to have a government that is transparent and accountable, and that ensures citizen participation and collaboration in the decision-making process.

In the information society, open government includes the access to public information and the reuse of public information (open data), citizen participation and collaboration, government accountability, and the use of ICTs to meet the three goals mentioned above. This also means that open government is less a single right, than a composition of several rights.

Some of them are ancient, such as the right to transparency or the right to citizen participation. Most of the time, in democratic countries, these rights are protected by the Constitution itself, or by the highest standards of human rights. For instance, in France, the open government principles mentioned above can be found through the Declaration of Rights of the Man and the Citizen, of 26 August 1789, a text that is of constitutional value.[6] By recognizing to the French citizenry a right to take part, personally or through their representatives, in the law-making process,[7] Article 6 of the

[4] Barack Obama, T*ransparency and Open Government, Memorandum for the Heads of Executive Departments and Agencies*, January 21, 2009. About this memorandum, see also Russell Weaver, "President Obama's Open Government Initiative", *Revue Internationale des Gouvernements Ouverts / International Journal of Open Governments,* 2017, No. *1,* pp. 1-10.

[5] *See* Irène Bouhadana, "Introduction. Transparency and Open Government: Which Possible Convergence?", in Irène Bouhadana, William Gilles, Russell Weaver (eds), *Transparency in the Open Government Era,* Imodev, 2014.

[6] *See* Constitutional council, decision No. 71-44 DC of 16 July 1971, Law supplementing provisions of Articles 5 and 7 of the Act of 1st July 1901, relating to association contract, the so called "Freedom of associations".

[7] Article 6 of the Declaration of Rights of the Man and the Citizen of 26 August 1789 states that : "The Law is the expression of the general will. All citizens have the right to take part, personally or through their representatives, in its making. It must be the same for all, whether it protects or punishes. All citizens, being equal in its eyes, shall be equally eligible to all high offices, public positions and employments, according to their ability, and without other distinction than that of their virtues and talents."

Declaration of 1789 asserted, more than two centuries before Open Government era, the principle of citizen participation and collaboration. For their part, Article 14[8] and 15[9] of the Declaration of Rights of the Man and the Citizen already recognized both a right to transparency and a right to accountability. From this point of view, the right to access to information can be regarded as a declination of the two rights aforementioned, as there is no possibility to be transparent or to monitor the Government without access to public information.

Yet, open government also means new rights,[10] such as the right to open data, or the right to co-build a public decision.[11] As these rights are more recent, they are, most often, not protected in themselves, by the Constitution. However, some of them can be hung up with older ones. For instance, can we not regard the right to open data as a new form of transparency? If transparency is not equivalent to open data, a goal of open data is to favour transparency. On the same lines, why not also analysing the right to co-build public policies as a modern form of the right to civic participation?

The Change of the Right to Privacy

For its own part, the right to privacy is more ancient[12] and would come from the end of the 19th century when Samuel D. Warren and Louis D. Brandeis recall that the need for the individual to "have full protection in person and in property is a principle as old as the common law".[13] There is no question that privacy should not be grasped in the same way in 1890 and in 2018, even though Samuel D. Warren and Louis D. Brandeis already claimed that "recent inventions and business methods call attention to the next step

[8] According to Article 14 of the Declaration of Rights of the Man and the Citizen of 26 August 1789, "All citizens have the right to ascertain, by themselves, or through their representatives, the need for a public tax, to consent to it freely, to watch over its use, and to determine its proportion, basis, collection and duration."

[9] Article 15 of the Declaration of Rights of the Man and the Citizen of 26 August 1789 recognizes the right for Society "to ask a public official for an accounting of his Administration".

[10] *See* Irène Bouhadana, William Gilles, « De l'Esprit des Gouvernements Ouverts », *Revue Internationale des Gouvernements Ouverts/International Journal of Open Governments,* 2017, No. *4,* pp. 1–22.

[11] See also Irène Bouhadana, William Gilles, The 10 principles for an Effective Open Government, 2016, available at: http://cms.imodev.org/nos-activites/europe/france/academic-days-on-open-government-issues-december-5-6th-2016-paris-france/10-principles-for-an-effective-open-government-10-principes-pour-un-gouvernement-ouvert-effectif/.

[12] Dorothy J. Glancy, "The Invention of the Right to Privacy", *Arizona Law Review,* No. 21, 1979.

[13] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review,* No. 5, 1890, pp. 193–220.

which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'."[14]

Two centuries ago, threats to privacy did not come from pictures or videos published on the Internet, but from simple writings: at that time, infringements of the right to privacy resulted from publishing personal information in manuscripts. Even then, the issue was to conciliate the right to privacy with other rights, and especially the right to know, even though the protection of the right to privacy came more from other rights (such as the right to copyright or the right of contracts) than from the right to privacy itself, as this right was not really asserted *per se* at that time. For instance, in *Pollard v. Photographic Co*, a case opposing a photographer to a lady pictured, the issue deals with the circumstances of the picture exhibition, the selling of copies of it, but also with the breach of an implied term in the contract, and a breach of confidence.[15]

There is no doubt that the protection of the right to privacy is a more complex issue in our society. Not only earlier threats mentioned have been exacerbated with the creation of the radio, then the television and the Internet. But with the advent of Big data and the Internet of things, former threats of privacy seem outdated. Certainly, publishing personal information in writings or disclosing pictures to the public still infringes the right to privacy. However, now, privacy issues are often more complex.

At least three reasons explain this complexity. First, with the technological development, people have changed their practices themselves. Most of them publish their pictures and videos on the Internet and social networks, disclosing privacy details to the public, and claim for a right to privacy at the same time. This is the privacy paradox[16]. If we analyse the right to privacy as a right of controlling personal details[17], we understand the difficulty in conciliating both the right to privacy and the practices leading to the disclosure of personal data in social networks.

Second, the definition of privacy has also become complex itself, involving more difficulties to protect this right. Simson Garfinkel explains that: "Privacy isn't just about hiding things. It's about self-possession, autonomy,

[14] Ibid.

[15] Pollard *v.* Photographic Co., 40 Ch. Div. 345 (1888), quoted by Samuel D. Warren and Louis D. Brandeis, op. cit.

[16] S. B. Barnes, "A privacy paradox : Social networking in the United States", *First Monday,* vol. 11, No. 9, 2006, available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/ article/view/ 1394/1312.

[17] Simson Garfinkel, *Database nation: The death of privacy in the 21st century*, O'Reilly, 2000, p. 13.

and integrity. As we move into the computerized world of the twenty-first century, privacy will be one of our most important civil rights. But this right of privacy isn't the right of people to close their doors and pull down their window shades – perhaps because they want to engage in some sort of illicit or illegal activity. It's the right of people to control what details about their lives stay inside their own houses and what leaks to the outside."[18]

Third, the protection of the right to privacy is itself more complicated, especially because new technologies make the private life more difficult to protect.[19] For instance, data anonymization exists, but this process is not always reliable and robust. In the age of big data, anonymization can be broken by linking several anonymized data together.[20] Thus, it is not surprising that the President of the French Data Protection Agency[21] observed in 2012 that: "each individual is now subject to a double tracing, in space and in time. In space, because of the growing use of CCTV systems and video surveillance, biometrics geo-location, impacting the freedom of movement. But also, over time, by profiling and targeting through search engines and social networks which lead to the creation of an absolute and general memory on people's expression and behavior."[22]

In such a context, giving a constitutional protection to the right to privacy is a necessity. In France, this constitutional right was recognized by the Constitutional judge[23] through article 2 of the Declaration of 1789.[24] Indeed, the French Constitutional council ruled that freedoms mentioned in this provision suppose the respect of the right to privacy.[25] [26]

[18] Simson Garfinkel, *Database nation: The death of privacy in the 21st century*, O'Reilly, 2000, p. 13.

[19] For instance, *see* Irène Bouhadana, William Gilles, "From the Right to Be Let Alone to the Right to Be Forgotten: How Privacy Is Moving in the Collecting Data Age", in Russell Weaver, Steven Friedland, William Gilles, Irène Bouhadana (eds), Privacy in a Digital Age. Perspectives from Two Continents, The Global Papers Series, Volume IV, Carolina Academy Press, 2017.

[20] *See* Irène Bouhadana, William Gilles, « De l'Esprit des Gouvernements Ouverts », *Revue Internationale des Gouvernements Ouverts / International Journal of Open Governments,* 2017, No. *4,* pp. 1–22.

[21] The French Data protection Agency is called the Commission Nationale de l'Informatique et des Libertés (CNIL) : https://www.cnil.fr/.

[22] *See* quoted and translated by Irène Bouhadana, "Introduction. Transparency and Open Government: Which Possible Convergence?", op. cit.

[23] *See* Constitutional council, decision No. 99-416 DC of 23 July 1999, Law establishing a Universal Health coverage.

[24] Article 2 of the Declaration of the Rights of Man and of the Citizen states that: "the aim of every political association is the preservation of the natural and imprescriptible rights of man. These rights are liberty, property, security, resistance to oppression."

[25] *See* decision No. 99-416 DC of 23 July 1999.

[26] For further information on that subject, *see* Irène Bouhadana, "The Right to Digital Oblivion in the French System: Corollary of the Right to Privacy or Emergence of a New Generation of Rights", in Anna-

§ 2 –The Right to Access Public Information Suppressed by the Right to Privacy?

The Limitation of the Right to Access Public Information in Case of Sensitive Data Susceptible to Violating Privacy

Among the elements of Open Government, there is the right to access public information. This type of information sometimes comprises sensitive data. For example, the French Law determines that the access to information that contains personal data can only be requested by the people concerned by the documents. In this regard, this means that the law restricts the communication of administrative documents to the concerned people in three cases: i) first, regarding administrative documents that can violate privacy, medical confidentiality and commercial and industrial secrets; ii) second, regarding the administrative documents that contain assessment or a value judgement of a physical person, who is either identified or easily identifiable; iii) finally, regarding the administrative documents that make "evident the behavior of a person and where the diffusion of this behavior can cause him or her harm".[27] However, these documents become once again susceptible to disclosure to any interested person after the parts that prevent disclosure have been suppressed or detached.[28] In other words, a person that is not concerned by the document can only have access to it if the suppression or detachment of these parts is possible.

Sara Lind, Jane Reichel and Inger Österdahl (eds), *Information and Law in Transition. Freedom of Speech, the Internet, Privacy, and Democracy in the 21st Century,* Liber, 2015, pp. 265–283.

[27] See Article L. 311-6 of the Code of Relations Between the Public and the Administration, which states: "The following administrative documents can only be transmitted to the person concerned: 1. Those which the disclosure will violate privacy, medical secret and commercial and industrial secrets, which includes the secret of procedures, of economic information and financial and commercial or industrial strategies; and that are evaluated by taking into account, when applicable, the fact that the administration's mission of public service, mentioned in the first line of article L.300-2, is subject to competition; 2. Those which show a value judgement or assessment of a natural person, especially if he or she is identified or is easily identifiable; 3. Those that make evident the behavior of a person, *if the disclosure of this document can harm the concerned person;* The medical information is communicated to the person concerned directly or indirectly through a designated doctor, depending on the person's choice, respecting the determinations of article L. 1111-7 of the Code of Public Health."

[28] See article L.311-7 of the Code of Relations Between the Public and the Administration, which states "When a request concerns a document that contains excerpts that are not communicable due to the application of articles L. 311-5 and L311-6, but where it is possible to suppress or detach these parts, the document will be transmitted to the requesting person after the suppression or detachment of these excerpts."

This first example shows that there can occur a conflict between the right to access information and the protection of privacy.

This conflict can also be found in the right to reuse information, another dimension of the right to open government, as explained above. In fact, in order to make the right to reuse public information effective, it is important to open extensively public information. A policy of open data barely makes sense if it is limited to a few documents. On the contrary, it is necessary to make public the greatest number of documents possible in order to allow the reprocessing of interesting data.

However, this bulk of information in itself can also pose problems from a privacy standpoint.

Thus, to conform with the law, at least in the French case, documents made public have been cleansed of the identifying data for, as explained earlier, documents containing identifying information cannot be disclosed. In short, they have been anonymized. The conflict between the disclosed document and privacy isn't present *a priori*, but occurs *a posteriori*. For these reasons, it is much harder to protect privacy because there are only potential violations. This potential violation consists of information cross-referencing that may never happen. However, if it does happen and it leads to the *posteriori* identification of a person, the harm is real.

These two examples show the difficulty of conciliating two rights that are equally necessary in a democracy. The issue is to evaluate how to coordinate these two rights, and to question which one should prevail in case of conflict. In both examples, it seems that the legislation prioritizes the right to privacy. For example, it was in seeking to protect privacy and identity that the French legislator sought to suppress identifying data.

The Difficult Application of the Rights of Sensitive Data Protection Against the Power of the Technological Resources Available to the Right to Access Public Information

Although the right to privacy predominates over other recognized rights, it is not always easy to protect it, particularly because technology is usually ahead of the law.

For example, it is possible to mention the difficulty of anonymizing documents, given that there are instruments capable of breaking the anonymization.

Also, regarding a political example, one can recall the work *Le Grand Secret*[29] written by the former doctor of President Mitterrand, published in 1996 by Plon éditions, and which had its sales banned 24 hours after release. This book reveals that François Mitterrand, elected as French President on the 10th of May of 1981, discovered that he had a cancer which reduced his life expectancy to something between 3 months to 3 years. The president established a strategy to hide this disease from the French people during two seven-year mandates. The sensitive nature of this work has led French Justice to forbid its sales[30], even though its publishing came after the death of the French President.

Though banned from sales with much effort, the work has been diffused through the internet, overcoming the effectiveness of the court decision.

Moreover, this primacy of the right to privacy also poses difficulties regarding the right to information. Particularly, the will to anonymize administrative documents can be understood in the sense that its goal is to protect privacy. However, the process of anonymizing also collides in some cases with the right to memory, or the right to remember the past. There has been a regain in interest in the right to memory, especially since it emphasizes the need to recall the tragedies of the past[31]. In this regard, it is worth mentioning Ch. Taubira[32] who affirmed "Memory is a right. Which results from the abuse of right. An abuse of people's rights, since the legislations have not banned torture, deportations, genocides, war crimes and crimes against humanity. From a violation of Positive Law since these crimes are described and penalized by codes. This right to memory precedes and transcends the duty to memory"[33]. Nonetheless, the right to memory has a large scope and should not concern solely the dark period of History. Such a right encompasses the ensemble of historical facts that are necessary to understand the evolution of our societies.

It is possible to question if the generalization of the anonymization process that we are currently experiencing will not conflict with the right to

[29] Cl. Gubler, M Gonod, *Le Grand Secret*, February 9 2006, éditions Rocher.

[30] See Tribunal de grande instance de Paris (Regional Court of Paris), ordonnance (court's order) of 18 January 1996; Cour d'appel de Paris (Court of appeal of Paris), 13 March 1996; Cour de cassation (court of cassation), 16 July 1997.

[31] On this topic, see A. Moussa Ive, "Du devoir de mémoire au droit de la mémoire », *Revue Internationale des sciences sociales,* vol. 188, no. 2, 2006, pp. 201–203.

[32] Christiane Taubira is a French politician. She is a former candidate for the French Presidential election (2002) and a former Minister of Justice (2012-2016).

[33] Ch. Taubira, « Le droit à la mémoire », *Cités,* vol. 25, no. 1, 2006, pp. 164–166.

memory of future generations. In fact, if all published documents were to be made anonymous as of tomorrow, would it be possible to retrace historical facts in the future? How would we be able to learn the history of France or of Europe if all the documents were anonymized at their times? The anonymization of documents to ensure the protection of privacy can provoke such issues in the future. Documents that are conserved in the future in archives will be anonymized by default in order to anticipate possible future requests for the disclosure of information. This default anonymization will clearly present the goal of making the management of the processing of administrative documents easier, especially if an open data policy is envisioned. Anonymized by default, the documents will be accessible to everyone without the administration needing to reprocess the information at every new request for disclosure. This search for efficiency, if carried out, can pose threats to the conservation of our History.

The issue is to know whether all documents should be anonymized since they might be disclosed or should we conserve the identification of such documents in certain cases, particularly those concerning public people.

§ 3 – The Right to Privacy Suppressed by the Right to Open Government?

The Right to Privacy Suppressed Because of Transparency and Integrity Needs

As explained before, the right to access public information is not a synonym of the right to open government. The former comprises the latter as one of its elements, but they are not identical. The right to open government is broader and also includes the important dimension of having honest governments. The right to open government regarded from the perspective of governmental ethics allows us to consider differently the question of coordinating the right to privacy and the right to open government, and more precisely to ensure the integrity of the elected and their absence of corruption.

This question also leads us to wonder whether public persons should have the same right to privacy as ordinary people. The issue can cause debate.

Indeed, we could assert that the particular nature of public persons explains that they do not benefit from the same right to privacy as the ordinary people. When it comes to politicians, they occupy functions that can

require the disclosure of certain aspects of their private life; for example, to ensure the integrity and good use of the public funds that are conceded to these people for the purposes of fulfilling their missions (mission expenses…).

There is also the issue of coordinating the privacy of political figures and the integrity of the elected, regarding the right to know how the elected are employing their compensations and indemnities in order to fight corruption.

In France, a minimum level of privacy is guaranteed for the elected. Two laws of 11 October 2013 set a new legal framework[34] with the creation of the High Authority for the transparency of public life (HATVP)[35], replacing the former Committee for Financial Transparency in Politics (CTFVP). The new body is charged with verifying probity and integrity in public life. For that, the HATVP checks the accuracy of two declarations, filled in by main actors of public life, that is to say : candidates to the presidential election, national and European parliamentarians, key local authorities, members of the Government and their associates (employees in ministerial cabinets and in the office of the President of the Republic), and the holders of various public offices and jobs (members of independent administrative authorities, holders of offices who are appointed by Government decision, heads of major public companies).

Both declarations contain personally identifiable details, the publication of which could be a threat to the declarant's right to privacy. Indeed, on the one hand, the declaration of interests aims to identify interests held at the date of election or appointment and within five years prior to that date. The interests are, for instance, a financial stake in a company, consulting activities, participation in the management of public or private entities. The High Authority for the transparency of public life can decide to disclose these declarations whereas voters can submit written observations regarding the declarations. On the other hand, the declaration on assets mentions all personal property of the declarant such as real estate, life insurance, bank accounts, vehicles, ships and aircraft, businesses, or assets and accounts abroad. As the declaration of assets contains data that present a greater risk

[34] Organic Law No. 2013-906 of 11 October 2013 on Transparency in public life, and Act No. 2013-907 of 11 October 2013 on Transparency in public life.
[35] https://www.hatvp.fr/en/.

to the right to privacy, transparency is more limited than with the declaration of interests[36].

Along the same line, the French legislator decided to have two different approaches regarding the possibility to reuse the information filled in on the two types of declarations. If the legislator introduced open data for declarations of interests, allowing the reuse of data reported in such declarations, he made a different choice for the declaration of assets that are available only in the prefectures, to people registered on the electoral lists and only for the purpose of consultation. Aiming to avoid that open data lead to "voyeurism", the legislator intended to protect the right to respect for the private life of politicians when sensitive data are at stake[37].

The Right to Privacy Restored Due to Lack of Public Interest

Even in the case of public persons, the right to privacy is essential. The right to information should only prevail if it serves general interest.

As explained before, balancing the right to public information and the right to privacy is a complex issue. Regarding politicians, this complexity is stronger. As ordinary people, the privacy paradox concerns political figures. They take photographs of themselves everywhere, and widely share them on social network in order to advertise their political life. And at the same time, they complain about newspapers, TV shows or social network that disclose pictures or videos showing them in a compromising situation. They try to master both their e-reputation and right to privacy, but this challenge has become too difficult in a society where data is omnipresent. Once a politician is the cause for the diffusion of information, should he/she dispose of the same rights? The answer is not easy. On the one hand, the politician is part of the vicious circle by him-/herself sharing personal data on social networks, and at the same time having everyone photographed and filmed with him/her. On the other hand, political figures have a right to privacy, but at the same time, as mentioned before, they have more commitments of ethics and integrity. It explains that the right to know is stronger for those who embrace political life.

Because people think that they should know and that everything should be transparent, they track every journey of politicians and try to record any

[36] See William Gilles, "Constitution and open government in France: About the Laws on Transparency of Public Life of 2013", in Irène Bouhadana, William Gilles, Russell Weaver, *Transparency in the Open Government Era*, Imodev, 2015.
[37] Ibid.

conversation, just in case something interesting could be disclosed and shared on social network. Politicians have now to face the "sousveillance", meaning 'watching from below',[38] in a panopticon[39] society. Indeed, new technologies such as smartphone now enable citizens to surveil their governments and their representatives at any time, for the best – making the principle of public accountability effective[40] – but also for the worst, when the aim is only to make the buzz and feed it.

In such a context, how to re-establish a right to privacy for public figures? First, there is a need to recognize that the scope of the right to respect privacy is different with public persons and that there exists a right to know. Second, we should make a distinction between the information disclosed depending on its utility. The aim is to protect the public interest.

We should consider the public interest regarding two criteria at least.

First, public interest depends on the presence of other rights or freedoms to balance with the right to privacy. Among those rights are the right to information, as aforementioned, and freedom of expression. For example, in the case of *Le Grand Secret*, French courts[41] have banned the diffusion of a work upon its publication and the President's former doctor was pursued for the violation of medical confidentiality. However, the European Court decided in a different sense and authorized the publication of the work based on article 10 of the ECHR which protects freedom of expression. The court also notes that the work had already been largely disseminated through the Internet and that the medical information it contained was not confidential, but known by a significant number of people.[42] In this case, general interest was to preserve freedom of expression, considering that the information was already available online. Going further, we can notice that this kind of decision should alert political figures who suffer from the

[38] The term « sousveillance » was coined by Steve Mann, *'Reflectionism' and 'Diffusionism': New Tactics for Deconstructing the Video Surveillance Superhighway*, Leonardo, 1998, No. 2, pp. 93–102.

[39] Jérémy Bentham, *Panoptique*, 1776 ; published again in 1776 with the title: Panoptique. Mémoire sur un nouveau principe pour construire des maisons d'inspection, et nommément des maisons de force, Imprimerie nationale. On the same field, see also Michel Foucault, *Surveiller et punir,* Gallimard, first publication 1975, 1993.

[40] *See* William Gilles, "Open Government, French Parliamentary Allowances and the 'Réserve Parlementaire' in a 'Sousveillance Society'", in Irène Bouhadana, William Gilles, Iris Nguyên-Duy (eds), *Parliament in the Open Government Era*, Imodev, 2016.

[41] See Tribunal de grande instance de Paris (Regional Court of Paris), ordonnance (court's order) of 18 January 1996; Cour d'appel de Paris (Court of appeal of Paris), 13 March 1996; Cour de cassation (court of cassation), 16 July 1997.

[42] See also ECHR, éditions Plon v. France, case No. 58148/00.

privacy paradox. Politicians who regularly disclose and share personal data will have more difficulties making their right to privacy respected.

Second, the scope of the right to privacy also depends on the reputation[43] and the quality of the people concerned. For instance, a President of the Republic should expect less right to privacy than an ordinary MP, and a MP less than a mayor. The French Constitutional court made this distinction, when ruling on laws on Transparency in public life,[44] taking into consideration the context in which the position or the occupation is exercised.[45] Thus, the decision of the Constitutional Council on the laws of transparency of public life is interesting because it offers a differentiation of rights according to multiple criteria.

Probably, this way of ruling is the more balanced, because it takes into account the complexity of the situation by creating a tailor-made right to privacy. It helps arbitrate between both commitments of an open government and the need to respect privacy or to be forgotten, even for most important people. In other ways, it serves democracy by feeding transparency without being voyeur, an argument that is often pointed out by supporters of secrecy.

[43] Christophe Bigot, « La protection de la vie privée des hommes politiques dans la jurisprudence de la Cour européenne des droits de l'Homme », *Legicom*, 2015/1, No. 54, pp. 113–118.

[44] *See* decisions No. 2013-675 DC and 2013-676 DC of 9th October 2013, on Organic and Ordinary laws on Transparency in public life.

[45] For further details, see William Gilles, "Constitution and open government in France: About the Laws on Transparency of Public Life of 2013", op. cit.

The Privacy of Public Officials in the Digital Age: A Democratic Issue

PATRICIA JONASON[1]

The title of this paper may sound like an oxymoron. Yet, it may be considered as "incongruous, seemingly self-contradictory"[2] to speak about the privacy of public officials.[3] Indeed, may persons who held a public function deserve a right to privacy in their capacity of precisely public official? Is it not, on the contrary, a logical consequence of his/her public official status, which implies the carrying out and performing of public tasks and the exercising of public power, that they have to be transparent for the public in regard of these public tasks and may not be entitled a right of respect to one's private life? Indeed, a certain transparency is required in order to control that those in charge of the concrete decisions affecting on a daily basis citizens' rights, human rights and freedoms, do act in compliance with the law and are guided by the pursuit of the common good – also in regard to the use of public funds.

At the same time, there are to be limits to how far transparency of public officials can extend as well as there may be constraints concerning the way to make information about public officials transparent. Indeed, "inadequate" transparency, if we may call it that, may generate threats for public officials themselves and also, indirectly and simultaneously, for the democratic state.

The issue of balancing transparency and privacy is becoming more and more intricate and delicate along with the growing erasure of the frontier between private life on the one hand and professional and public life on the other hand; a phenomenon which may be largely explained by a combination of the technological development (including better performance of web searching tools) and the societal developments (expressed by a wide-reach-

[1] Associate Professor of Public Law, Södertörn University. This paper is a 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.

[2] An oxymoron may namely be defined as "*a figure of speech by which a locution produces an incongruous, seemingly self-contradictory effect, as in "cruel kindness". See https://www.dictionary.com/browse/oxymoron*

[3] See interesting reflections on the question whether civil servants deserve a right to privacy when it concerns information related to how they perform their public activities Bull, Thomas, "Personlig integritet för det offentliga?" in: Vänbok till Claes Sandgren (2012), p. 105–118.

ing use of social media and what seems to be less concerns for personal secrecy). To the transparency/privacy balancing debate regarding public servants should also be added an ever-harsher social climate, which concretizes itself by growing occurrences of threats and violence against the "Democracy workers" that civil servants constitute.[4]

The perspective adopted in this paper is not a philosophical-sociological-political scientific one on the question of the pertinence or not of speaking in terms of a right of protection to privacy for the public official capacity. I would rather have a legal, ethical and pragmatic approach on the issue and point out the potential (damaging) consequences that disclosure of personal data permitting to identify a public official, may have and highlight the need therefore to have a transparency/privacy-aware approach.

Privacy is handled in this paper as a question of anonymity and more precisely a question of anonymity in documents uploaded on the Internet.

Indeed, the example I use for illustrating the issue at stake and for demonstrating the need for a broader reflection is the publication on the Internet of documents containing names of public servants. More specifically the example concerns decisions taken by the Swedish Parliamentary Ombudsman (JO) which contain the mention of civil servants' names and are published in the online case law database of this authority.[5]

The point of departure of my interest for a reflection on the need to think in terms of public official's privacy – or more precisely in terms of anonymity of the public officials on the Internet – was indeed the reading of decisions found in the online database of the Swedish Parliamentary Ombudsman.

Common elements of the selected decisions are (a) that an individual public official has been pointed out[6] by the decision and criticized by the Ombudsman for having behaved in an unprofessional and inappropriate manner, (b) that the civil servant subject to the criticism has a position at a

[4] See BRÅ report, p. 10.

[5] Although this example may seem as typical Swedish because of the particular Swedish circumstances, I believe that the use of such an example may easily make understandable the issues and risks associated with public disclosure of information concerning public officials. It may also be that the selected examples are not even relevant anymore for the current Swedish context as it seems that the Parliamentary Ombudsman has changed his routine concerning its online database and does not anymore publish the names of the civil servants in the database. It should be an effect of the enter into force of the General Regulation of Data Protection which has eventually convinced the monitoring authority to have a privacy friendly approach.

[6] The decision criticizes an individual public official and not the public administration or the department the civil servant belongs to.

quite low level in the administrative hierarchy, (c) that the decisions are published in the online case law database on the public website of the Ombudsman, (d) and finally that the name and surname of the criticized civil servant appear in the decision.

These selected documents illustrate in my view an *inadequate transparency*. Inadequate in the sense that the transparency the system provides may generate inappropriate and disproportionate infringements for the civil servant as a person, and may, in turn, adversely affect the democratic society. Inadequate also in the sense that the transparency such as encountered in the cases studied is unnecessary from the point of view of a democratic control as in the current cases it exist means – the sets of rules on the right of access to official documents – for having access to the names of the public officials if needed.

It is the conjunction of the publication *on the Internet* and the fact that the decision contains the *name* of the civil servants that constitutes the crucial problem.[7] The privacy of the civil servants – and beyond the democratic character of the society – may be put in danger in two ways. (a) because if one wants to gather information about a person and this person's name is to be found in a decision published in the online database, then this decision might appear in the search results performed by the search engine one made use of[8] (b) but also – and it is the situation I aim to focus on – because the one who may want to gather information about the civil servant whose name is indicated in a specific decision very easily can map not only the professional profile of the civil servant but also his/her private life.[9]

Because the decision reveals the civil servant's identity, it becomes indeed easy with means of search engines – with Google at the forefront – to

[7] With other words the publication on the Internet *per se*, if it occurs without the mention of names looses in general its dangerousness. Similarly, the mention of the names in a decision that is not posted on the Internet has much less propension to lead to the privacy and democracy infringements that are discussed in this paper.

[8] This was an argument used by the Swedish Data Protection authority, the Datainspektion (DI) for criticizing the online publication ("*When using search engines on the Internet"* the DI says "*there is also the risk that a search for a certain name, which is done for completely different reasons to find out if the person has been subjected to review by the Ombudsman, will also include the information that the person in question has been criticized by the Ombudsman*"), DI's decision (No.663-2010) of October 5, 2010, p. 6. See footnote 13 below.

This kind of privacy infringements have been tested by Tomas Bull who conclude that "*general searches about a person's name, place of residence or the like do not pose any significant risk of just spreading JO's criticism of that person*". (my translation). See in *Personlig integritet för det offentliga?* See p. 115–116.

[9] My approach is then different than Bull's approach.

find a wealth of information related to the civil servant in his/her capacity of individual/citizen, such as their home address and pictures of the residence (thanks to Google Maps), their date of birth, picture of the individual him/herself and sometimes of his/her relatives and/or friends. Additionally, search engines may collect information of the brand of the car (as well as of the colour of the car!), hobbies, the name of the neighbour, the average salary in the neighbourhood and the voting patterns etc.

Moreover, the societal changes that express themselves through new ways of communicating (via social media such as Facebook, Blogs, Instagram, Twitter etc.) and the fact that always more information about individuals is available on the Internet, whether the persons concerned by the information want it or not, whether the persons concerned by the information know it or not, lead to an interlacing of the private and public/professional life and a blurring of the boundaries between the two spheres.

This is not contested, for getting back to the type of decision handled in this paper, that the personal information (i.e. the name) found in the Ombudsman's decisions is linked to the individual in his capacity as civil servant. However, a large amount of information that search engines easily can gather, on the basis of the name of the civil servants contained in the decision, are of a purely private nature. In other words, the publication of the civil servant's name in the case law database of the Ombudsman facilitates the mapping of the civil servant's private life. Furthermore, the fact that on the Internet, the decisions will be available for an unlimited number of persons, even outside Sweden, and for an unlimited time, i.e. circumstances that Mayer-Schönberger calls for a spatial and temporal panopticon,[10] adds to the vulnerability of the persons concerned.

I intend in this paper to address legal (1) and ethical (2) issues that the mention of the names of public servants in decisions published on the Internet crystallize.

The publication of the names of the civil servants in the online database: legal considerations

The publication of the civil servant's names in the online database of the Ombudsman is to be legally considered as a question concerning the right

[10] Mayer-Schönberger, Viktor, Delete: The Virtue of Forgetting in the Digital Age.: 2009. Published by: Princeton University Press, p. 111.

to privacy and more specifically as a question regarding data protection. Such a publication consists of a processing of personal data as defined by the data protection legislation.[11][12]

In fact, the issue of the publication of the civil servants' names in the Ombudsman's online case law database has been dealt with in depth by the Swedish Data Protection Authority, the Data Inspection Board (Datainspektion, DI) in its Decision *Supervision according to the Personal Data Act (1998: 204) - The Ombudsman's Publication of Personal Data in the online case law Database* (No.663-2010) of October 5, 2010,[13] hereinafter called the "DI's decision". The decision originally concerned a complaint relating to the mention of a *private individual's name* – the plaintiff's name – in a decision published in the online case law database of the Parliamentary Ombudsman,[14] but the DI took the opportunity to enlarge the scope of the reasoning and to comment on the publication of *public officials' names* in the same database.[15] In the decision it rendered, the DI stated that the publication of the plaintiff's as well as of the civil servant's personal data (i.e. the names) in the Ombudsman online database violated the Swedish data protection legislation in force at that time, the Personal Data Act (Personsuppgiftslagen, PuL).

Although the specific legal argumentation of the DI is not entirely transposable into the new data protection framework, as the General Data

[11] Indeed according to the GDPR processing of personal data is defined as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" (Article 4 (2)).

[12] I will not go into the protection provided by article 8 of the European Convention of Human Rights and in the case-law of the European Court of Justice. However, it might be said that cases involving question of data protection issues are dealt by the Strasbourg Court in a procedure integrating data protection legislation. Indeed, the search of whether a "law" is provided for, according to Article 8.2, justifies the alleged privacy infringement consists of appreciating if data protection rules/principles are in place. See for example M.M v. the United Kingdom (n° 24029/07). Judgment 13.11.2012 (para 195) and L.H. v. Latvia (n° 52019/07), Judgment 29.4.2014.

[13] Tillsyn enligt personuppgiftslagen (1998:204) – Justitieombudsmannens publicering av personuppgifter i praxisdatabas på Internet.

[14] See Jonason, Patricia (2017), *Online Proactive Disclosure of Personal Data by Public Authorities. A balance between transparency and protection of privacy*, The Right of Access to Information and the Right to Privacy: A Democratic Balancing Act [ed] Patricia Jonason; Anna Rosengren, Huddinge: Södertörn University, pp.125–126.

[15] Several civil servants had lodged a complaint to the DI, see Sören Öman https://www.sorenoman.se/blendow/april2011.pdf

Protection Regulation (GDPR)[16] that has replaced the Data Protection Act differs from it in some aspects of relevance for the type of cases we analyse here, the legal reasoning the Datainspektion held 2010 is still of interest for understanding the privacy issues at stake.

I will therefore begin the legal analysis of the publication of the names of the civil servants in the Ombudsman's online database by exposing the argumentation of the DI based on the former Swedish data protection legislation (1.1). I will then examine the question of the conformity of the online publication with the current applicable legislation, i.e. the GDPR (1.2).

The publication of the civil servants' name in the Ombudsman's online case law database and its conformity with the Personal Data Act

The Datainspektion carried out the examination of the Parliamentary ombudsman's online publication in the light of the Swedish Personal Data Act (Personsuppgiftslagen (1998:204), PuL), issued 29 April 1998 and based on the Data Protection Directive 95/46/EC.[17]

Like the European legislation, the PuL contained a substantial set of rules that the data controller had to comply with, such as the rules which concern *fundamental requirements for processing of personal data* or the rules laying down *requirements regarding the legitimation of the processing of personal data*. However, the Swedish legislator wishing to lessen the compliance with the data protection legislation for " *such everyday data processing of personal data that typically does not entail any greater risk of violation of the data subject's privacy*"[18] wished to move away from this traditional regulatory model (hanteringsmodell[19]) for these kinds of situations and introduced 2007 in a new provision (Section 5a) of the Personal Data Act a regime called *abuse centered model*. This new regime, which applied to processing

[16] 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.

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[18] "[A] *number of circumstances indicate that the data protection regulation should be lessened for such everyday data processing of personal data that typically does not entail any greater risk of violation of the data subject's privacy*", Prop. 2005/06:173, p. 19.

[19] See SOU 1997:39, pp.179 and Prop. 1997/98:44, pp. 36.

in *unstructured material*[20] consisted of exempting the data controller from most of the provisions of the Personal Data Act, as for instance the provisions on fundamental requirements for processing of personal data and on the conditions of legitimation of the processing[21] as well as the provisions on sensitive data, on legal offences and on transfer to third countries. A data processing should not be performed however if it leads to an infringement of the data subject's privacy.[22]

It is on this provision regulating data processing in unstructured material that the Parliamentary Ombudsman assessed the online publication on its website of decisions containing names. The Datainspektion was sceptical in regard to the application of the regime laid down in Section 5a for this kind of processing and stated that "*it can be put into question if the legislator had intended that the abuse rule should apply to such a type of processing the Ombudsman performs when it makes its case law database accessible on the Internet*". The Data Protection authority added that it had "*doubt as to the intention* [of the legislator] *was that the simplified regulation in 5a§ Data Protection Act should apply to public authorities when they make big database blocks (samlingar) of decisions containing individual's personal data accessible on Internet*".[23] Faced with the impossibility to refer to concrete statement in that direction in the preparatory works,[24] and after having established that the processing had not had the characteristics of a processing in *structured material,*[25] the Datainspektion made an appreciation of the lawfulness of the publishing on the basis of the provision the Ombudsman referred to.

[20] Which are "*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 to facilitate the search or the compilation of personal data*"- For more details on the Personal Data Act and on Section 5a, Öman, Sören, Lindblom, Hans-Olof, *Personuppgiftslagen: En kommentar,* 2011, pp. 129–160.

[21] Section 5a of the Personal Data Act from 1998 was labelled as followed: Undantag för behandling av personuppgifter i ostrukturerat material. *Bestämmelserna i 9, 10, 13–19, 21–26, 28, 33, 34 och 42 §§ behöver inte tillämpas på behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter som har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter. Sådan behandling som avses i första stycket får inte utföras, om den innebär en kränkning av den registrerades personliga integritet. Lag (2006:398).*

[22] This approach provides the name to the type of regime, the "abuse center model".

[23] DI's decision, p. 3. See also the comment of Sören Öman who discusses the applicability of the abuse centered model in the case https://www.sorenoman.se/blendow/april2011.pdf

[24] DI's decision p. 3.

[25] "*This is not a collection in which the Ombudsman appears to have structured the information in a way that has significantly facilitated the search or compilation of personal data*", DI's decision, p. 4.

This appreciation of the lawfulness of the processing in regard to PuLSection 5a - or, in other words, the appreciation on whether the processing led or led not to a privacy infringement, consisted in, the Datainspektion explained, of carrying out, in the individual case, a balancing between on one hand the data subject's interest of a private protected sphere and on the other hand other opposite interests.[26] The appreciation of the balance of interests should furthermore, the DI assessed, not only be done in taking into consideration the kind of personal data being processed, but should also take into account the *context of the purpose*[27] in which the data appear and the data *dissemination* that "*has occurred or is likely to occur and what the treatment can lead to*."[28] The DI reminded additionally that PuL's provisions relied on an EU Act (the Data Protection Directive), which meant that "*The balance shall not be based on an interpretation that would be in breach of, inter alia, the fundamental rights protected by Community law, such as the right of every human being to the right of respect for his/her privacy in accordance with Article 8 of the Convention of the Council of Europe*". As last element for appreciating if data processing leads to a privacy infringement or not, the Swedish Data Protection authority mentioned the application of the principle of proportionality, expressed by the Data Protection Directive and in Article 8 of the Council of Europe Convention[29] and which may even been drawn from "*the method the Swedish legislator refers to when it concerns the application of the abuse centered rule*".[30]

In the current case, the purpose (interests) of the Ombudsman regarding the processing in form of the publication on the Internet was "*primarily to award the public 'insight' in the Ombudsman's activities*" and "*to disseminate knowledge on the legal assessments expressed in the decisions, with the intention to provide public authorities and public officials (befattningshavaren) guidance for acting properly*".[31] This had to be weighed out, according to the DI, against the fact that when an official has been criticized by the Ombudsman this "*may have significant consequences for him/her even beyond the*

[26] DI's decision, p. 4.
[27] DI's own italics.
[28] DI's decision, p. 4. The DI recalled further, referring to the preparatory works, i.e. Prop. 2005/06: 173, p. 29, that there are the ones who are in charge of applying the law (the practitioners – rättstillämparna) whose task is to carry out the balance in the individual case.
[29] DI's decision, p. 4.
[30] Id., p.5.
[31] Id., p. 6.

service" (tjänsten). This should also be taken into consideration in the appreciation that the way of publishing made the publication "*particularly sensitive*"[32] and that the purpose of the Internet publication could have been fulfilled even though the decisions did not contain the name of the civil servants. Moreover, argued the DI, if someone is interested in the name of the civil servants who is subject to the Ombudsman's criticism it is usually enough to make a request directly to the Ombudsman for accessing the decision containing the name.[33]

The Data Inspection Board concluded that the balance test spoke in favour of the protection of the civil servants' privacy. It even assessed that the publication of the name of the Civil servants in the Ombudsman's case law database was "*normally not permitted under the abuse centered rule in the 5a§ Personal Data Act* "but needed a "*special support in the law*".[34]

In clear, data processing as that carried out by the Ombudsman could potentially and in principle have been permitted according to the abuse centered rule of the Swedish Data Protection Act – but was not – the DI stated - due to the specific circumstances of the current processing.

The entering into force of the GDPR changed the playing field as the abuse centered regime disappeared from the data protection legal framework – and has even got the better of the Ombudsman reluctance to follow the conclusions of the DI concerning the publication of civil servants' names.[35]

[32] The DI refers to the search functions on the database which offer the possibility to "*produce comprehensive compilations of executives who have been criticized by JO*". See DI's decision, p. 6. "*Publishing on the web also means*", the DI adds, "*that the information becomes considerably more accessible, especially with the help of so-called search engines as well of various solutions for compiling and reusing materials available on the Internet*." See DI's decision, p. 6.

[33] Ibid.

[34] "*Särskilt författningsstöd*", DI's decision, p.7.

[35] Indeed, while the Ombudsman seemed to have accepted the arguments and conclusion of the DI concerning the names of the complaints as it has, after the decision of the Swedish Data Protection Board, only put the initials or neutral designations such as NN or AA or these individuals in the decisions published on its online database, the Ombudsman has continued until recently (Autumn 2019) to – although not systematically – publish the entire names of civil servants.

1.2. Publication of the name of the civil servants in the Ombudsman online case law Database and its conformity with the GDPR legislation

While the Swedish legislator was of the opinion that the Data Protection Directive from 1995 allowed for national rules such as the abuse centered rules it introduced 2007 in the Personal Data Act,[36] the standpoint is different in regard to the GDPR which entered into force 25 May 2018. The latter European data protection instrument does not allow room for such arrangements, the Swedish legislator says.[37]

In the absence of a centered abuse model the appreciation of the conformity or not of the online publication of decisions containing the names of public officials has to be assessed in regard to the set of protective rules laid down in the General Data Protection Regulation, rules that are directly applicable in the Swedish legal order.[38]

The rules of relevance for appreciating the conformity of the online publication with the GDPR are especially the ones laying down the principles of the lawfulness of processing (Art. 6) and the ones on the principles relating to the processing of personal data (Art. 5).

Indeed, processing of personal data must comply with the conditions for the lawfulness of the processing provided by the GDPR. This means that each processing has to be founded on a ground provided for in Art. 6.1 of the Regulation. We will look closer at the grounds applicable to processing of personal data performed by a public entity,[39] the category to which the online publication studied in this paper belongs to.

I. A first possible ground, as it relates to processing performed within the public sector is the one set out in Art. 6.1.e, second part of the sentence, according to which consisting the processing is lawful if it "*is necessary for the performance of a task carried out* […] *in the exercise of official authority vested in the controller*". This ground

[36] Prop. 2005/06:173 Översyn av personuppgiftslagen, p.31.

[37] See Prop. 2017/18:105, Ny dataskyddslag, p. 85 "*Missbruksregeln i 5 a § PUL har dock ingen motsvarighet i dataskyddsförordningen*".

[38] They had their counterpart in the Data Protection Directive – and consequently in the Swedish Data Protection Act – but were not applicable in cases where the abuse-centred regime applied.

[39] Among the grounds some only apply to the public sector, others may apply both to the public sector and the private sector as for example the ground consisting of "*compliance with a legal obligation to which the controller is subject*", see SOU 2017:39, p. 114.

may nevertheless directly be excluded from the ones applicable in the case we study as the publication of personal data concerning civil servants on the Internet as treated in this paper is undoubtedly not done in the context of the *exercise of official authority toward citizens,* which is, the Swedish legislator assesses, *"characterized by decisions or other unilateral measures which ultimately are an expression of the powers of society in relation to the citizens"*.[40]

II. Non-problematic is even to exclude the ground laid down by Art. 6.1. c) according to which the "*processing is necessary for compliance with a legal obligation to which the controller is subject*".[41] Indeed, to publish online personal data, as the Ombudsman did, does not correspond to a legal obligation and certainly not to the obligation to disclose information/documents that follow from the principle of publicity regulated by the Freedom of the Press Act (FPA). Indeed, the framework on the right of access to official documents, constituted by the second Chapter of FPA, lays down the obligation for public authorities to disclose documents upon request (reactive disclosure) but not to disclose documents of its own accord (proactive disclosure)[42] as is the case when the Ombudsman publishes decisions on its website.

III. Would the online publication of the names of the civil servants be able to be supported by Art. 6.1 e), first sentence, i.e. when *"processing is necessary for the performance of a task carried out in the public interest"?*

Arguments might be found for defending the thesis that the processing, consisting of publishing the names of the civil servants on the Ombuds-

[40] "*Myndighetsutövning mot enskilda karaktäriseras av beslut eller andra ensidiga åtgärder som ytterst är uttryck för samhällets maktbefogenheter i förhållande till medborgarna*". See SOU 2017:39, p. 119. The preparatory works accompanying the entry into force of the GDPR legislation (Prop. 2017/18:105, p. 62) noticed, as the preparatory works dating from the time the Data Protection Directive had to be transposed into Swedish law did, that the concept of *exercise of official authority* had a European common content but that the point of departure in Swedish law would be so far to use the concept as understood in Sweden. See SOU 1997:39, p. 365.

[41] It may be noted that Article 6.c 1 may apply to both the private and the public sector. "*There is nothing in Article 6 (1) (c) of the General Data Protection Regulation which limits the application to the private sector.* See SOU 2017: 39, pp. 116–17.

[42] See Jonason, P. (2018), The Swedish legal framework on the right of access to official documents. In: Perlingeiro, R. and Blanke, H. J. (eds), *Access to Information: An International Comparative Legal Survey*. Heidelberg: Springer, p. 239.

man's website, may be seen as a processing related to the performance of a task carried out in the public interest. The definition of the term "*task carried out in the public interest*" is broad. According to the Data Protection committee[43] it is "*meant to refer to something that is of interest to or affects many people on a broader level, as opposed to special interest.*"[44] Additionally, according to the government "*All tasks that the Riksdag or the government have given to state authorities to perform are* […] *of public interest*".[45] And as the Committee expresses it "*The concept of task of public interest does not only encompass what is performed as a consequence of a public law and explicit obligation or task. To the contrary to what is applicable regarding art. 6.1 c) GDPR the data controller does not need to have an obligation to perform the task for the legal ground e) may be applicable*".[46]

So, whether the task of public interest is interpreted in the current situation as the very task of the public authority – the monitoring of the application of the law within the public sector, [47] which is regulated in the *Ombudsman's* instructions[48] – or as a more nebulous task of the public authority but still related to the primary task of the Ombudsman, one could say that the online publication of the names of the public servants is related to a "task carried out in the public interest". One may consider indeed that the publication of names as the one performed by the Ombudsman enables the transparency of the activities of the Ombudsman and gives insight into the responsibility of individual civil servants.[49]

[43] This Committee (Dataskyddsutredningen) was in charge of the preparation of the entry into force of the GDPR. It was composed of a special investigator and about 10 experts.

[44] The notion of public interest, as stated in the regulation, should be considered, according to the Swedish Data Protection Committee, to have a broader meaning in the GDPR than it had in the Directive. SOU 2017:39, p.123. This is because, contrary to the Directive, the Regulation does not allow public authorities "*when carrying out their duties, to process personal data on the legal basis which departs from a balance between the legitimate interests of the controller and the rights and interests of the data subject*. SOU 2017:39, p. 104. See also p. 123.

[45] See Prop. 2017/18:105. See also according the Data Protection Committee, SOU 2017:39, p. 124.

[46] SOU 2017:39, p. 124.

[47] According to the Riksdag Act (Riksdagsordning (2014:801), Chapter 13, Section 2 "*The Riksdag has, according to Chapter 13, Section 6 of the Instrument of Government, elect ombudsmen who are to supervise the application of laws and regulations in public activities*".

[48] Lag (1986:765) med instruktion för Riksdagens ombudsmän.

[49] "*As the Datainspektion interprets the assessment of the Ombudsman, the purpose of the Internet publication is primarily to give the public insight into the Ombudsmans' activities. In addition, the purpose of the database should be to disseminate knowledge of the legal judgments expressed in the decisions, with the intention of giving the authorities and executives guidance on how to act correctly*". See DI's decision, p. 6.

The task of public interest "*shall*" in the meanwhile – it is an additional requirement set in the GDPR "*be laid down by Union Law or Member State law to which the controller is subject*" (art. 6.3). Indeed, when using article 6.1 e as legal basis it is not possible to only refer to the general ground in the General regulation.[50] According to the Swedish legislator, this does not mean nevertheless a requirement that the data processing itself has to be regulated. It means that the task itself has to have a basis in the legal order.[51] Neither the Committee nor the government considered that there was a need to further regulate the public authorities' mandatory tasks on a general level in order for authorities to take the necessary processing measures to fulfil their duties: "*The actions taken by the authorities for the purpose of performing these tasks* […] *have thus themselves a legal basis that has been published through clear, precise and predictable rules*".[52]

Two solutions: the online publication is considered to be related to the performance of a task of public interest and then the requirement of the existence of a legal basis is fulfilled through the legality principle, or the online publication of names is not to be considered as related to the performance of a task of public interest and then the possibility to proceed that way is submitted to the introduction of such a task in the law (as the requirement to adopt specific legal instrument, declared by the Datainspektion 2010).

In any case, for being conform to (art. 6.1e) second part of the sentence, the purpose of the processing must moreover be *necessary* for the performance of the task of public interest. (art. 6.3).

[50] Kommittédirektiv 2016:15. 5. See also in Prop. 2017/18:105, p. 49: "*In the case of processing necessary to fulfil a legal obligation (Article 6 (1) (c)), as part of the exercise of authority or to carry out a task of general interest (Article 6 (1) (e)), there must also be other support in the legal order than the one provided in the Data Protection Regulation".*

[51] Prop. 2017/18:105, p. 48.

[52] SOU 2017:39, p. 129. Anyway, for art. 6 1.c and e, the Data Protection committee and the government proposed – and this solution has been adopted by the Parliament – that the Swedish Act with supplementing provisions to the EU Data Protection Regulation contains a reference to the necessity of having a legal basis for these processing. Indeed, Chapter 2, with the heading *Legal basis*, contains provisions related to the processing of personal data when there is a legal obligation, when a task is carried out in the public interest or when a task is carried out in the exercise of official authority. According to the preparatory works is this provision intended to provide guidance for the application of the law (in Sweden). Prop. 2017/18:105, p. 189. For more information on the Swedish Act see *(Lag med kompletterande bestäïmmelser till EU:s dataskyddsförordningen (*2018:218). On this Act see Jonason, Patricia (2019), *The Swedish measures accompanying the GDPR* in National Adaptations of the GDPR, Collection Open Access Book, Blogdroiteuropeen, Luxembourg, Mc Cullagh K., Tambou O., Bourton S. (Eds.), pp. 42-51.

As commented by the government "the method the data controller chooses for performing his task has however – as all public administration – to be adequate in relation to its purposes, effective and proportional and may therefore not generate unnecessary infringement of individual privacy".[53] More clearly, it says that "the requirement that the purpose shall be necessary for performing the task of public interest means an obstacle against totally no indispensable processing of personal data or processing which constitute an disproportionate infringement of privacy that was not foreseeable".[54]

In other words, also if the online publishing of the names of the civil servants is to be considered to be authorized on the basis of art. 6 1.e first sentence because it can be said to fulfil the conditions of a processing for the performance of a public interest, the requirements concerning the purpose of the processing stated in the same provision may create an obstacle for the processing.

Moreover the existence of an adequate legal basis is "*not a sufficient condition for a processing of personal data to be authorized*".[55] Indeed, the processing has to comply with the other requirements laid down in the GDPR and not least with the "Principles relating to the Processing of Personal Data" stated in "Article 5 of the GDPR". The general requirements enumerated in this provision are about lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and apply to all personal data processing.[56]

Among the above-mentioned principles, I would like to emphasize the existence of the principle of fairness. This principle, which means that the data must be processed in a "fair" manner in relation to the data subject[57] and which application could impede the authorities to publish personal information on their websites despite the existence of a legally founded and

[53] Prop. 2017/18:105, p. 60.
[54] Ibid.
[55] See SOU 2017:39, p. 129.
[56] Id., p. 106.
[57] The Swedish term contained in the GDPR is the term "correct" (*korrekthet).* The Data Protection committee which questions the choice of the Swedish term and whether it corresponds to the intention of the provision (SOU 2017:39, p. 106) prefers to use the word *fairly* (*skälig* or *rimlig* in Swedish). SOU 2017:39, p. 129.

necessary processing in accordance with Article 6.1.e, – is indeed not far from the ethical principles[58] that I will analyse in the next section.

Indeed, to publish on the Internet personal data related to civil servants may engender – as will be demonstrated in the following – serious negative consequences for the civil servants themselves as for the Rule of Law. So, whatever the law allows, an ethical approach is required in this field.

2. Publication of the civil servants' names in the online case law database of the Ombudsman: ethical considerations

The publication of the names of the civil servants in the Ombudsman's online case law database engenders, as the Swedish Data Protection Authority assessed in its decision of 2010, "*significant consequences for the executives (befattningshavaren) even outside the service*".[59] The risks for such consequences increase due to the possibility of using search engines and, on the basis of the name found in the Ombudsman's decision, to easily and quickly collect a wealth of information related to the named civil servants' and his/her relatives' private life. The privacy infringement that the names' publication triggers constitutes both a threat and an unfair punishment for the civil servants concerned. The publication of the names thus raises a number of ethical issues in relation to the individual civil servant criticized in the decisions. Furthermore, the blurring of the civil servants' names as well as information related to the civil servants' private sphere, which publication on the Internet enables, increase the vulnerability of the public employees and impact the exercising of their freedoms, which, in the long run, constitutes a threat to the democracy and the Rule of Law. The unfair punishing effect of the publication may also have a deterrent impact on the body of civil servants (*tjänstemannakåren*) which also impact the Rule of Law.

The publication of the names of the civil servants in the case law database thus raises ethical questions[60] in relation to the individual civil servants

[58] See a definition of fairness found on the Internet https://josephsononbusinessethics.com/2010/12/fairness/ *Fairness is concerned with actions, processes, and consequences, that are morally right honorable, and equitable. In essence, the virtue of fairness establishes moral standards for decisions that affect others. Fair decisions are made in an appropriate manner based on appropriate criteria.*

[59] DI's decision, p. 6.

[60] I will not go in depth into the concept of ethics. I take the term ethics and ethical behavior as a way to act that is right and that will not negatively influence others or what constitute humanity. https://www.oxfordscholarship.com/view/10.1093/0199285721.001.0001/acprof-9780199285723

themselves (2.1), and even in relation to the democratic state and the Rule of Law (2.2).

2.1 Ethical issues with regard to the individual civil servants

In order to give a more concrete understanding of the situation the affected civil servants may experience, I begin with a description of two illustrative cases I have found in the online case law database of the Ombudsman.

A first case concerns a public official working at a "medical" unit[61] who, after having from the same person, nights and days, received a huge number of phone calls, one day answered in an inappropriate and impolite manner to her interlocutor. The interlocutor in question has then lodged a complaint to the Ombudsman and sent him, as a proof for what had happened, the sound recording of the conversation with the public official she had an altercation with. The decision of the Ombudsman (hereinafter referred to as the *medical unit decision*) reproduces in written the recorded phone conversation and identified the civil servant with her name and surname.

Another decision concerns an inspector who,[62] in two emails sent to an individual who had contacted him/her in a matter concerning a project, had answered in an impolite manner.[63] Here also the conversation – in the form of an email correspondence, is reproduced in the decision (hereinafter referred to as the *inspector decision*).

The decisions have several similarities. In both cases the Parliamentary Ombudsman criticized the civil servants' behavior as infringing the requirement of objectivity laid down in Chapter 1, Section 9 of the Instrument of Government. The principle of objectivity includes indeed the obligation for the employees by the public authorities to treat the individuals contacting

[61] The vagueness concerning the task of the civil servant is on purpose. The same applies for the other decision presented below.

[62] We found even several decisions concerning police officers criticized for expressing themselves on social media belonging to the police administration in a way that has been considered as not acceptable. The interest in these decisions lies not least in the fact that they disclosed the name of police servants, civil servants who occupy a special and vulnerable position. According to *2015:12 Hot och Våld – Om utsatthet i yrkesgrupper som är viktiga i det demokratiska samhället.* (see footnote 78). p.107, the police, in common with the customs officials, coastguard officials are apparently the most vulnerable groups in the legal field.

them in a correct manner.[64] Both civil servants were "severely criticized"[65] by the Ombudsman.

Common for the decisions was even the raw reproduction of the paroles of the civil servants, said or written, always indelicate – and in one case furthermore in an incorrect Swedish language, which leads to the fact that the publication of the conversation combined with the name of the public servant – a non-Swedish name may generate an even stronger stigmatization.

As the names of the criticized civil servants were indicated in the decisions (and were not common Swedish names) it has been possible, using search engines, to easily and rapidly collect a large amount of information concerning the private life of the civil servants and their relatives. I made that experience. It took me about 3 to 4 minutes in these above-mentioned cases to find out where the civil servants lived and to get a picture of the place of their residence, to get a (private) picture of the civil servant themself and sometimes of his/her relatives, to collect information about their civil status and on their hobbies…I stopped my Google search there but I guess there would have been much more information to access.

The cases described put to the fore a number of (varying) ethical issues[66] related to the situation of the individual civil servants.

They concern the question of who bears the burden for shortcomings occurring in the administration, the question of stating examples, the stigmatization and inequality due to the names of the civil servants, the question of the assessment to indicate, or not, the name of the civil servant in the decision, the question of the selection of the decisions to be made subject to an online publication.

I. A first ethical issue concerns the question of the burden bearer for the shortcomings taking place within the administration. Indeed, one may question if it is ethical to point out by name a person as responsible for the occurred problem when, in fact, the errors made by the civil servants when they carry out their duties often could be said at least

[64] Inspector decision, p. 3 and Medical Unit decision, p. 2. The Ombudsman refers to the preparatory works 2007/08:KU6 pp.14 "*Kravet på saklighet innebär bl.a. att anställda vid myndigheter har en skyldighet att bemöta dem som vänder sig till myndigheten på ett korrekt sätt*".

[65] "*Förtjänar allvarlig kritik*", Medical unit decision p .4 and Inspector decision, p. 4.

[66] I present here some issues without pretending to be exhaustive.

> partially to be linked to defects that can be attributed to the public authority itself.[67]

It is clear that the impolite way of behaving by the medical unit's employee as well as by the inspector are wrong and shall be sanctioned by criticisms pronounced by the Ombudsman (which is what the Ombudsman did). However, it is not unlikely that such acts of maladministration by civil servants could have been avoided if the public authority had taken adequate measures. It could have been, for example, measures to protect civil servants from harassment, a situation that seems to have occurred in the case of the public official working at the medical unit and to some extent in the inspector case. The extract from the phone conversation between the public official criticized by the Ombudsman and the plaintiff indicates namely in the case concerning the medical unit the use of a harassing if not threatening tone from the plaintiff towards the civil servant.[68] Such a poisonous situation that not only seems have its origin in the civil servant's behavior may also be read between the lines in the inspector case. The lack of routines and other measures in order to avoid or at least manage situations such as those encountered may undoubtedly affect the work environment of the civil servants, inside the organization as well as outwardly, and therefore how the public officials perform their work in relation to the citizens.

With the point of departure that the public authorities themselves have acted wrongly – because of their passivity, lack of satisfying routines etc. – it sounds unreasonable and unethical to publish the public official's name on the Internet, which consequently concentrates all responsibility on the individual public official while the public authorities themselves implicitly get out of responsibility. In these cases, the sanctioned civil servants were moreover at a low level in the hierarchy of the administration and had probably little capacity to influence the circumstances/routines of the public authorities.

[67] One may notice that according to Section 8 of the Act with Instructions for the Parliamentary Ombudsmen (1986:765) "*The Ombudsman should not intervene against lower-ranking executives without independent powers, unless there are special reasons for an intervention*".

[68] The plaintiff wanted to get answer to the question why she was not allowed to visit a certain patient. According to the Health and medical board in charge of the service, the plaintiff "*has on several occasions, several hours in a row, day and night for several weeks continuously called the patients' phone as well as the expedition's phone. This has meant limited opportunities to call for other patients*", Medical unit decision, p. 2.

II. – a means to state cautionary examples for other public officials and discourage and prevent them from behaving wrongly. However, such an "exploitation" of an individual public official to "educate" other public officials may be considered to be contrary to the Kantian maxim according to which human beings should be treated as an end and not as a means. The fact that public officials are being criticized – even if they are anonymous in the online published decision – should suffice to have this deterrent effect.

III. The same ethical element of Kant's moral philosophy could be used to counter the argument that the Ombudsman used towards the Swedish Data Protection Authority in order to defend the publication of the names of civil servant in his online case law database, namely as mentioned earlier, the argument according to which "*Transparency* [in the form of publication] *is an essential element in exercising official authority that constitutes the core of the mandates of the Ombudsman*".[69] In the meantime, to "sacrifice" in this way an individual's privacy (may he/she be a public official) to achieve openness is not defendable, especially since the transparency of the Ombudsman's activities can also be met, as the Datainspektion also pointed out, while the names of the criticized officials are not included in the decision. In addition, those who wish to further investigate the cases handled by the Ombudsman has the possibility, by exercising his/her right to request access to public documents, to gain insight into the entire decision, including the civil servants' names.

IV. A further ethical issue is related to the Ombudsman lack of consideration for the "hanged" public official's own circumstances – more precisely the names they bear – and the higher risk of stigmatization and inequality these circumstances generate when the names are published online.

Clearly, if the public official has an unusual name, the publication may cause him/her a greater risk of privacy infringement than if he/she carries a more common name. The accuracy and thus the possibility to chart a person's privacy is higher or even dramatically higher if the name – (our modest survey confirmed) and especially the first name /surname combination - is unusual. In fact, it is much easier to map the private life of a civil

[69] DI's decision, p. 6.

servant called Patricio Jonasonoskiou than the private life of a civil servant named Anders Johansson. Having a (for Sweden) unusual name, which many of the citizens "with other ethnical background than Swedish" have, is in this context a stigmatization factor,[70] even related to the question of citizen's equality.

The manner the Ombudsman (more especially the Bureau of the Ombudsman) did assess, for each decision taken, whether the name, the initials, or neutral letters (as AA or NN for example) should be used in the decision for identifying the civil servants also triggers ethical questions related to equality and justice. A review I made of a certain number of decisions could not show any clear and coherent policy on that point: neither the gravity of the faults, the Ombudsman who the decision came from, the sector concerned nor the common or uncommon character of the name of the civil servant could be found to be explaining factors for the decision of the bureau of the Ombudsman to indicate or not the name of the criticized civil servant in the decision.

In the same "lottery" vein, why should the "sanction" pronounced by the Ombudsman be more noticeable (in fact a double sanction – the criticisms itself and the disclosure on Internet of the name) for those civil servants who happen to be involved in a matter that the Ombudsman considers to be "of particular interest"[71] than for the lucky ones whose case has been judged less interesting and consequently not worth being included in the online case law database? Here again, the argument of equality and justice may be of importance.

In summary, there are several aspects that indicate that, from an ethical point of view and with regard to the civil servants considered individually, it constitutes an inappropriate routine to include the names of the public officials in decisions published on the authority's website.

[70] The stigmatization of public officials with foreign names may affect the concerned civil servants even more if the decision contains a raw transcription of a text written by the criticized civil servant and containing several linguistic errors. The stigmatization may even affect the "community" of civil servants of foreign origin. In a general manner I have no criticism to raise against the transcription of the sayings of the civil servants (email and phone conversation *inter alia*) in the decisions published online. From a pedagogical point of view, the method may help to concretely understand the types of behavior the Ombudsman judges to be inappropriate. The ethical problem with such a transcription stems from the easy-to-read link between the conversation published in the decision and a named civil servant.

[71] They therefore ended up among the decisions the Ombudsman chose to publish on its website.

2.2. Publication of Official's Name in JO's Web Based Practice Database and its compatibility with the requirements of the democratic Rule of Law

The publication of the names of the public servants does not only lead to negative consequences for the individual civil servants themselves (in terms of, *inter alia*, privacy infringement, stigmatization and "double punishment") but also to problematic consequences for the democracy and the Rule of Law. Thus, the Internet publication of decision containing the name of civil servants also raises ethical questions in relation to the Rule of Law. In the following I will focus on two prerequisites for a well-functioning democracy which may be challenged when the civil servants' names are published on the Internet.

The first is the need for civil servants to be protected against harassment, extortion and other inconveniences. The second is the need for the public officials to enjoy their full human rights. These two aspects are interrelated in such way that the first mentioned prerequisite is *a sine qua non* condition for the second prerequisite.

A well-functioning democracy requires the individuals composing the civil service to be protected against harassment and other threats. Indeed, threats and harassment affect the public official's performance of tasks. That is one of the conclusions the Swedish Crime Prevention Council (BRÅ) comes to in a report submitted[72] on *Threats and violence – On vulnerability corruption for professional groups of particular importance to democratic society*. The report establishes that some of the civil servants who have been victims of harassment or other inconveniences say that they since then are not comfortable making certain decisions[73] and are "*passive in various situations*".[74] It happens for example that civil servants give over the cases they handle to colleagues in order not to have to deal with a case which with they have had trouble.[75] Some of them even question the correctness of their own professional practice.[76]

[72] *2015:12 Hot och Våld – Om utsatthet i yrkesgrupper som är viktiga i det demokratiska samhället.* The report summarizes and analyses the different studies that have been conducted on this issue.
[73] "[…]one can hesitate more before taking decisions", BRÅ report, p. 101.
[74] "behaves passively in different situations", BRÅ report, p. 13.
[75] Ibid.
[76] BRÅ report, p. 102 "*Almost one of ten who is threatened states that they themselves are affected in such a way that their authority can be called into question*".

In addition to the fact that the vulnerability of public employees affects the quality of day-to-day performance of activities (including public authority), this exposure to harassment and other inconveniences has implications for the administration's ability to retain officials and perhaps in the long run to recruit people. And indeed, the number of civil servants who have suffered inconvenience indicates that they would like to change jobs. As BRÅ's report states, this vulnerability can "*reduce the attractiveness of different professions*".[77] "*It's negative for democracy if people do not want to work in important professions because they feel uncomfortable about threats and violence*".[78] At the same time the report shows civil servants are subject to these types of inconvenience in a greater extent than ordinary workers and that the civil servants working with tasks related to exercising of power (myndighetsutövning) are "*particularly vulnerable*".[79]

Among the "relatively common forms of harassment" (except for unpleasant phone calls and unpleasant letters /e-mails) mentioned in the report is also noted one's mapping of the employee or doing "malicious reports",[80] whatever that means.

It could not be excluded, in my view, that the publication on the Internet of the names of public officials may contribute to a greater concern about the threats and other inconveniences the civil servants are affected by[81] and in parallel to a greater discomfort for the civil servants.

A well-functioning democracy should furthermore presuppose that citizens, including those working in the public sector, can enjoy human rights and freedoms.

As this paper has shown, the fulfilment of this condition can be questioned regarding the right to privacy/data protection[82] when public officials' names are published on the Internet. The online publication enables, as we

[77] BRÅ report, p. 7.
[78] Id., p. 16.
[79] Id., p. 10.
[80] "*Okynnesanmälningar*", BRÅ report, p. 96.
[81] Actually, there are already examples on the Internet of "harassment campaign" against civil servants who have been criticized by the Ombudsman not least via websites such as Flash back.
[82] Beyond data protection the right to privacy is, as known, guaranteed not least by Article 8 of the European Convention on Human Rights, which enjoys a legal status in Sweden through the Act (1994: 1219), See also the Swedish Instrument of Government, Chapter 2, Section 6, which guarantees some aspects of privacy. This provision protects inter alia individuals against 'significant infringements [made by the State] on the individual's privacy if they occur without consent and consist in surveillance or the mapping of the personal circumstances of the individual.

have seen above, an intrusion into the private sphere of the civil servant,[83] an intrusion due especially to the technical and societal development and the erasure that followed, of the border between the public/professional sphere and the private sphere.

In the meantime, it is not only the individual aspect of the right to privacy, i.e. the possibility of self-realization of the individuals that is of concern when the civil servants' right to privacy is under threat. Even the "collective" side of their right to privacy, may be infringed. By "collective" side of the right to privacy is intended the conditions that allow the individuals to contribute to a pluralistic society in which people enrich society with the choices they make and their exercising of freedom of expression and other rights. On the contrary, a person who fears that his/her privacy may be under threat, for instance because his/her position as a public official can be linked to the individual and the citizen he/she is, could tend to restrict his/her freedom of expression on social media for example. Such fears to be tracked may impact on the civil servant's participation in social life in general as almost all kinds of participation in social and political life leave tracks on Internet: participation in sport events, membership in an association, etc. Here again, the publication on the Internet of the names of the public servants may be deterrent for democracy if the civil servants' human rights and freedoms are limited by self-censorship in this way.

Concluding remarks

Having regard to the interests at stake, i.e. interests that go beyond the very interests of the civil servants to have their privacy protected and includes interests for the democracy and the Rule of Law, legislation, while necessary is insufficient. An ethical approach is in addition required.

In other words, before publishing personal information related to civil servants, beside the necessary analysis of the legal conditions set out for the publication, an ethical reflection should take place. The questions to be posed are not least what kind of consequences the online publication of the names of the civil servants could have in the short term and in the long term for the civil servants themselves and for democracy and the Rule of law. Another given question to pose – both ethical and legal – is if the infringement of privacy and the risks in terms of a diminishing of the Rule of

[83] If not as a civil servant at least as an individual.

Law be overweighed by the benefits such a publication is expected to generate and if there are less damageable way to attain the goals. The ethical reflection must be performed by the individual actors who, in the particular case, take the decision to publish the names of the civil servants online. This in turn requires that an ethical reflection takes place within the publishing authority itself. Ideally, such a reflection is also brought to a higher level and given a concretization in general guidelines.

The case of the online publication of personal data performed by the Swedish Parliamentary Ombudsman is, as mentioned in the beginning of this paper, only to be taken as an illustration of the legal and ethical problems which may occur when personal data concerning civil servants are subject to a publication on the Internet. In other words, the paper aims to arouse a reflection of principal nature. Some of the considerations analyzed in the paper – if not all – may be applicable to situations of various kinds which entail the publication of the names of the civil servants on the Internet.[84] When it concerns the institution of the Ombudsman, it seems to have changed its policy. Where the Datainspektion failed, the GDPR did. I warmly welcome the changes made by the Ombudsman, which as a leading authority in the legal and institutional Swedish landscape has a great responsibility to show the way for other public authorities!

[84] The reasoning may also be applicable mutatis mutandis concerning the publication of the names and other personal data regarding politicians, a professional group of particular importance to democratic society and also particularly subject to threats and violence.

Digitally Ready Legislation as a New Concept in Danish Law – An Erosion of the Rule of Law?

MICHAEL GØTZE[1]

In Denmark, new legislation is currently designed to be digitally compatible from the very beginning. The new legislative concept has been named "digitally ready legislation" denoting legislation that is ready to be transformed into subsequent digital requirements. The pro-active digital focus at the hatching of new regulation may have a price, however, as far as the rule of law is concerned reducing the flexibility and "elastic quality" of regulatory templates. This article sheds light on principles of digitally ready legislation and on that backdrop, I discuss various rule of law scenarios. It is a challenge to strike a fair balance between regulation with an open-end and discretionary design or with a close-end design based on regularity and objective criteria. This is so far a debate deficit in that respect in Danish law. Although the concept of digitally ready legislation has advantages, and although Denmark ranks in the top end of the digital class in Europe, the ongoing digital reform comprises several problems. Arguably, the reform may represent a drawback towards a more simplified legal geometry to the detriment of the diversity of citizens and enterprises subject to Danish law.

1. A political push for digital reform of legislative culture

A strong current focus in Danish politics and Danish law is how to optimize the opportunities and potentials that the digitalization of the public sector arguably entail. A concrete manifestation of this is found in the political agreement from 2018 on digitally ready legislation between the Danish Government and all other political parties in the Danish Parliament.[2] The political agreement and the efforts in translating it into legislative practice will be high-lighted in the following.

The agreement on "digitally ready legislation" is a new milestone in Danish legislation taking a proactive approach to subsequent digital solu-

[1] Professor, Ph.D. the Faculty of Law, Copenhagen University

[2] "Politisk aftale om digitaliseringsklar lovgivning" af 16. januar 2018, "The political agreement", cp. the governmental publication Regeringens aftale med alle øvrige partier i Folketinget: "Enkle regler, mindre bureaukrati – lovgivning i en digital virkelighed", The Danish Ministry of Finance, October 2017.

tions in the public sector. According to the agreement, legislation must pave the way for use of digital solutions in the Danish administration. With the introduction of digitally ready legislation, the abstract debate on digitalization in Denmark – and many other European countries - is transformed into a more present and a more concrete element during the pre-legislation phase in the Parliament. Therefore, further elucidation and discussion of the implications of the agreement is called for although such debate – at least in Denmark – is surprisingly absent so far.

One of the main points of the article is the challenge in striking a fair balance at a legislative level between discretionary and objective regulation. Moreover, the inherent preference in digitally ready legislation for binary regulation is discussed. The article further questions whether the general assumption that law is a technology-neutral phenomenon, can be upheld if digitally ready legislation ends up creating a general regulatory culture based on algorithms. It is often said that legal principles and rules do not change materially by switching from analogue to digital format.[3] In my opinion, conversely, it can be emphasized with equal justification that the consequence of the new concept of digitally ready legislation in the long term may be that technology has a normative impact in the design of regulation and the choice of structure of rules.

With regard to the chosen model of analysis in the article, it can be mentioned that my aim is to examine the possibilities and dilemmas of digitalization at a *legislative level* and thus from a primarily constitutional law perspective. In addition, many important issues in relation to the digitalization at governmental and citizen level can be raised, nevertheless these issues are not addressed within this work due to spatial reasons. In this article my focus is legislative rather than administrative.

2. Political agreement with a dual focus: more digital state and fewer digital "scandals"

Denmark is top ranked when it comes to digitalization from a macro perspective. In 2020, Denmark is ranked at the very top globally when it comes

[3] The Danish Ministry of Justice claim that administrative law principles are substantially neutral to technological changes, cp. "Justitsministeriets notat om forvaltningsretlige krav til offentlige digitale løsninger, 2015".

to e-Government according to the UN.[4] Within the EU, Denmark has in 2018 been ranked among the most digital societies in a broad study on various levels of digitalization.[5] The survey covers all 28 Europeans countries (in 2018) with Sweden, Finland, and the Netherlands also being among the highest ranked. At the lower end of the ranking we find countries such as Italy, Bulgaria, Estonia and Romania. The measurement of the levels of digitalization of the European countries is based on six dimensions, including digital infrastructure, the digital skills of the population, the use of digitalization by businesses, and the levels of digitalization in the public sector. From a dynamic perspective indexing may appear less positive for Denmark. In 2017 Denmark had 'only' a digital development rate of 2% while the average for the EU was 3,2%. In relation to the dimension of digitalization that concerns digital citizens, it is estimated that 71% of the Danish population in 2018 has at least the fundamental digital skills. Even here, the rate of development is slightly stagnant. To this overall picture, it can be added that it is obviously more difficult for digitally well-developed countries to maintain a high development curve than less digitally developed countries.

Given this background, it is not surprising that the political parties in Denmark – from all ends of the political spectrum – give priority to digital options. The agreement on digital-ready legislation is based on the fundamental view that a proactive and agile approach is needed if digital solutions must function as intended in relation to both efficiency and the rule of law within the public sector. The underlying idea is that digital perspective is not only a practical, administrative and a matter of IT, but also a regulatory matter.

The sooner digital solutions are considered, the better the forecast of well-functioning digital solutions in the subsequent stages. Therefore, the agreement stipulates that the Parliament addresses the digital potentials in the administrative implementation of the law, and that the digital perspective is put on the agenda even when the political parties consider new regulation.

Another, and substantively important part of political agreement is that the legislature should generally take a critical look at discretionary regulation. Digital solutions typically advocate the avoidance of discretionary and

[4] E-Government Survey – Digital Government in the Decade of Action for Sustainable Development, United Nations, New York, 2020. www.publicadministration.un.org.
[5] Digital Economy and Society Index (DESI), European Commission, May 2018.

dynamic elements. According to the Danish Ministry of Justice's updated guidelines on the quality of law, new legislation should be designed in order to facilitate "a full or partial digital administration and application of new technology that support a better and far more efficient task solution'.[6]

In my opinion, the overall aspiration of the agreement to be more digitally agile is as such convincing, especially looking at past mixed experiences. However, it is also quite ambitious in many aspects. From digitalization being an issue that has been typically been a secondary consideration in the work of politicians and government officials in preparing legislation and administrative regulations (if it has been considered at all) to now becoming a mandatory and initial consideration during the hatching of regulation. This legislative culture in Denmark is thus in a fundamental transition phase.

Although the agreement on digitally ready legislation is not based on an expert report or on published systematic analysis or empirical research, when reading the agreement, you get the impression that the agreement has a double purpose.

It is written in clear wording that political parties with the agreement want to embrace the many opportunities offered by the digital community. If we look at the agreement from a single-case perspective, the agreement can also implicitly be read as an initiative that wants to distance itself from a number of "problem-cases" and "scandals" concerning the use of digital solutions within the Danish public sector. An example which is often referred to is the challenges of a digital tax law system, the EFI-system (one common IT system to recover tax debts). The mere cost of recovery steps to dismantle the default system made by the automated recovery tax system is estimated to amount to 200 million Euro (1,5 billion DKK).[7] In addition, the well-known challenges of the Danish public property valuation system have a strong digital dimension. In 2013 the Danish tax authorities had to suspend the public property valuation system with the consequence that the valuations are technically frozen and suspended. In that regard, it is stated, - somewhat understated – in the political agreement on digitally ready legis-

[6] Cp. Guidelines on drafting new legislation by the Danish Ministry of Justice ("Justitsministeriets vejledning om lovkvalitet, opdateret december 2017, afsnit 4.2., side 172.". The guidelines can be found at www.lovprocesguide.dk.

[7] The Danish "EFI-scandal" is briefly described by the Danish ombudsman in a report from 2014 (FO 2014-24: "Overholdelse af forvaltningsretlige krav i forbindelse med udviklingen af SKATs IT-system, EFI"). The report can be found at www.ombudsmanden.dk.

lation that there are "several examples of public IT projects being considerably more expensive and delayed" because the legislation is framed without the necessary consideration for the subsequent digital implementation.

The well-known 'problem-case' – despite illustrating the challenges rather than benefits of digitalization of the public sector – thus seem to have added momentum to the concept of digitally ready legislation.

3. The broad embrace by the aspiration of digitally ready legislation

The agreement on digital-ready legislation has a wide scope, and it targets not only new legislation (new bills) but also administrative regulations and political agreements.

Firstly, the agreement has effect vis-à-vis new laws (new bills) that are enacted after July 1, 2018, i.e. bills that are put forward during the Danish parliamentary year 2018/2019 (October 2018 until October 2019). Secondly, the agreement has effect vis-à-vis administrative regulations ("bekendtgørelse"), that are issued from July 1, 2018 onwards. Thirdly, the agreement envisages an assessment of the consequences of digital implementation in regard to political negotiations and agreements following July 1, 2019. Fourthly and fifthly, the agreement stipulates, in the context of revision and amendment of existing laws and the revision of existing administrative regulation, that a pro-active digital perspective must be included. When it comes to significant changes to current legislation it should be considered in accordance with the agreement, whether a more fundamental revision of the legislation is needed to make it fully digitally ready.

Against this backdrop, the political agreement on digitally ready legislation is more far-reaching than its name – comprising also e.g. administrative regulations that play a very important role in Danish law – and the digital reform will have an impact on the entire body of law, or a significant part of it in the years to come. It could be added that a revision clause has been included in the agreement, and the political parties in the Danish Parliament will in 2020 assess whether the legislation is sufficiently digitally ready and discuss further initiatives to support and enhance digitally ready legislation in the broad sense.

As a comment on the broad scope, it can be said that it will presumably require resources during the phase in which legislation is prepared to carry out the legal considerations of digitalization. More specifically, the number of bills submitted per parliamentary year, exceeds just over 200. It may also

be noted, that no indication seems to have been made of how much of the mentioned regulatory body consists of discretionary provisions. The agreement's emphasis on simplification of discretionary laws and regulations seems to assume that it is a large number. The agreement is supplemented by general guidelines ("vejledning") issued by the Danish Agency for Digitalization ("Digitaliseringsstyrelsen"), stating new legislative principles and various methods for impact assessment. The guidelines have public law legislation and regulation as their main focus.[8] In respect of commercial law, a political agreement has been concluded between a number of political parties with a view to digitally ready legislation that is important for business. Thus, legislation and regulation are currently – regardless of being a subject matter within public or private law - also subject to general principles digitally ready and "agile" legislation.[9]

4. The distinctively technocratic approach to digitally ready legislation

According to the guidelines from the Danish Agency for Digitization, legislation can formally be characterized as digitally ready if it meets – or at least receives sufficiently positive assessment of a list of seven principles. The approach to digitally ready legislation is highly technocratic, and as far as the Agency of Digitalization is concerned, it is primarily as a matter of "good legislative technique" rather than a matter of democracy and good administration. The seven – technocratic – principles must be a part of a mandatory procedure in the future, in which the relevant ministry will assess a bill's implementation consequences. These consequences should always be addressed and described in the general preparatory comments of the bill (preparatory works). The seven principles are as follows:

[8] Cp. "Justitsministeriets vejledning om lovkvalitet, op. cit., pkt. 4.2. (Digitaliseringsklar lovgivning)."
[9] Cp. "Erhvervsministeriets vejledning om principperne for agil erhvervsrettet regulering, juni 2018."

1. Simple and clear regulations. Legislation should be simple and clear, so it is easy to understand for citizens and businesses. Simple and clear regulations are easy to manage and contribute to a more consistent administration and digital support.
2. Digital communication. The legislation must support digital communication with citizens and businesses. For those citizens and businesses that do not use digital solutions, other solutions must continue to be an option.
3. Automatic processing. The legislation must support that the administration of the legislation can be done in whole or in part digitally with due regard to legal security of citizens and businesses. This means among other things, that the legislation is basically designed so that the objective criteria are used when it is considered relevant and when there is no need for a discretionary professional judgment.
4. Coherence – uniform concepts and data reuse. Data and concepts should, as far as possible, be reused across authorities.
5. Safe and secure data management. High levels of digitalization require high priority on data security. Therefore, in legislative work, the focus should be on whether new legislation gives rise to special points of attention in relation to safe and secure handling of citizens' and companies' data.
6. Public infrastructure. Legislation must take into account that it is possible to use existing public infrastructure such as NemID, BankID, digital mail and other e-IDs.
7. In the drafting of legislation, the possibility of a monitoring and preventing abuse and errors should be taken into account. Legislation must allow efficient IT use for control purposes.[10]

If we take an initial analytical look at the seven principles, it can be said that they are based on the following presupposed and simplified transformation – or 'before and after'-dichotomies: (1) from unclear regulation to clear regulation, 2) from analogue/manual communication to digital communication, 3) from discretionary/open-end regulation to objective/close-end regulation**.** 4) from sectoral concepts to intersectional/coherent concepts, 5)

[10] The principles are quoted as stated in the guidelines of the Danish Minsitry of Justice ("Justitsministeriets vejledning om lovkvalitet, op.cit, page 172". A somewhat more comprehensive explanation of the principles can be found in the guidelines of the Danish Agency of Digitization ("Digitaliseringsstyrelsens vejledning").

from less secure/uncertain data management to secure data management, 6) from decentralized infrastructure to public infrastructure and 7) from less efficient/ineffective control to effective control. In time, quite significant developments are thus expected.

In addition, the Danish Agency for Digitalization's guidelines contains methods for assessing the consequences of implementation and recommendations on digital-ready legislation. This includes a description of the requirement that the ministries of 2018 should submit legislative proposals with implementation consequences in consultation with the Agency for Digitalization, as far as six weeks before consultation. The mandatory consultation with the Agency for Digitalization applies only to legislative proposals, not administrative regulations such as notices.

Looking at the organizational set-up of enhancing digitally ready legislation it is striking that it is now the Agency for Digitization under the Ministry of Finance in the field of public law that has been assigned the task of providing legal technical assistance to the different ministries. The Agency for Digitalization must undertake screening of draft legislation and to assist the ministries with guidance on the new impact assessment and support the work on digital-ready legislation. In this way, the task of guiding is split between the Danish Ministry of Justice, as an expert in the classical legal field as to drafting new legislation, and the Agency for Digitization, as an expert in the digital field. There is some coordination of the dual efforts, but the Ministry of Justice's accumulated competence is – to my mind – relatively reduced within the new set-up which represents a shift of approach to fundamental rule of law concepts.

5. The rule of law dilemmas of non-discretionary templates

We now move on to one of the inherent challenges that face the concept "digitally ready legislation", namely the basic reservation towards discretionary regulation. When legislation is to be translated into algorithms and systemic programmes, open-ended and discretionary rules are to be avoided. They cannot be transformed into binary language. Although discretion is a feature of law that is frequently considered difficult by lawyers, discretion is nonetheless often a useful and relevant way of regulating a subject matter. Discretion entails a high degree of flexibility and case-to-case readiness. However, when we turn to the concept of digitally ready legislation, the existence of discretionary and framework-based regulation is to a large degree seen as a negative and counterproductive choice.

A large part of the political agreement consists in a call for the legislature and the responsible parts of civil service preparing new legislation to if not avoid, then at least to minimize, the use of discretionary rules. As mentioned above, the Danish Agency for Digitalization has established a legislative rule of priority in favour of objective, simple and close-ended rules and in favour of regularity because of the possible benefits that such regulation gives in relation to subsequent digital management. It is embedded into the digital paradigm that ambition of the legislature is to break down legislation in binary logic and unambiguous categories.

Conversely, the legislature should reserve the use of more discretionary, dynamic and contextual rules in as few areas as possible. However, the desire to reduce discretionary is not without exceptions. The agreement opens the possibility that there may still be reason to legislate by means of flexible regulatory frameworks e.g. in certain welfare law areas such as coercive removal of children from the parents. However, the examples of such permitted open-ended regulatory areas are few in the agreement. The rationale behind the preference for binary legislation is that such regulation may allow professionals to spend more time on more complex cases, where an individual judgment is needed, e.g. in cases concerning the child's well-being and support for particularly vulnerable citizens.

The challenge of a significant increase in the use of close-end regulation in Danish legislation is to my mind downplayed in the concept of digitally ready legislation. This applies primarily to a digital scenario where the task of making decisions towards citizens is coded into computerized decision-making systems. Looking into the crystal ball we may envisage that digitally ready legislation will create a legal landscape characterized by "squareization" and simplified legal geometry. In my opinion, this may involve a loss of eye level with the citizen and a smaller space for individual considerations compared to a multi-faceted and increasingly individualized reality. There is a risk that future administrative decisions being made on the basis of digital administration will be less suited to embracing the diversity of citizens. The emphasis in the political agreement on efficiency and equal treatment benefits is only to a certain extent justifiable and the downside is, of course, that digitally ready legislation can put pressure on regulatory instruments that involve human discretion.

Although there is some awareness in the political agreement about maintaining discretion, the agreement is not specific on this point. In addition, as already mentioned, there will be no explicit comment in the preparatory works of new legislation as to whether the Parliament has opted out of the

use of a discretionary rule model. The choice of close-end regulation is thus presented as the only choice when new legislation is designed. It is my assessment that too few and too single dimension examples have been included in the agreement on digitally ready legislation. Confidence in legislation as such may be weakened if new legislation is largely designed in templates where important decisions are not based on individualized and well-considered judgements, but on algorithms that in a largely inexplicable way calculate a result.[11]

Finally, new legislation that is not flexible can make it difficult in practice to gain experience in the regulation and then find the appropriate legal level of rights. If legislation is designed in rigid templates, there is no room for subsequent adjustments in practice. If new legislation proves to be inappropriate or erroneous, it will also take time to change the legislative structure requiring new legislation to correct and replace the original template. Although the goal of increasing the regulatory outlook for digital solutions can hopefully be a constructive opportunity to focus more on the relationship between the state and the citizen, it may seem paradoxical that the introduction of digitally ready legislation into Danish law is so far based on a highly technical discourse.

Finally, it may be pointed out that digitally ready legislation is not only about digital potentials for the sake of digitalization but also to a large extent for the sake of efficiency. It has been emphasized as a counter-idea that efficiency considerations may risk becoming the main factor. The introduction of digitally ready legislation is by some commentators seem as a camouflage exercise with a view to implementing cuts within the public sector. The new organizational set-up where responsibility for implementing new legislation is divided, between the Agency for Digitalization under the Ministry of Finance on the one hand and the Ministry of Justice on the other, the Ministry of Justice and the Agency for Digitalization under the Ministry of Finance, may itself push towards prioritizing the efficiency, thus downgrading the rule of law.

[11] The problem of reduced confidence has been put forward by inter alia practising lawyers (Cp. "Advokatrådets retssikkerhedsprogram").

6. Waiting for Godot and the broad debate on digitally ready legislation

Up till now, the introduction to digitally ready legislation has been a matter for politicians and for various officials within the central parts of Danish administration. The project has not aroused a wide popular debate or a discussion among legal experts. It will strengthen the legitimacy of the project if it is given a higher priority to share knowledge of the concept and to facilitate a public debate on the pros and cons of digitally ready legislation. The agreement on digitally ready legislation has made the digital theme more concrete to the readers of the agreement, but the agreement may also have put a damper on a possible debate comprising counter-arguments due to the agreement's relative blindness to obvious dilemmas and drawbacks. The guidelines of the Danish Agency of digitization were submitted to a public hearing in 2018 with a rather narrow timeframe – 2 weeks – considering the complexity of the subject matter.

Summing up, there are promising elements in the new concept of digitally ready legislation. It can pave the way for efficient digital solutions, and it is obvious that using digital solutions can generate benefits in many practical respects, such as self-service solutions, case management, digital 24/7 accessibility, more uniformity in the administration's work and a shortening of case processing times etc.

On the other hand, the ongoing of Danish legislative culture also face rule of law challenges. The positive assessments in proposals for new legislative as to digital potentials can be seen as manifestations that the Danish legislature has endeavoured to avoid discretionary regulation. It must be assumed that the number of discretionary rules is being reduced for the time being, illustrated by the fact that the vast majority of new legislation so far (that is in the fall of 2020) are based on positive pro-active assessment of digital solution. This may in itself represent a problem, and the framing in new legislation for subsequent digital solutions may have a deeper impact on the regulatory culture. The use of categorical regulatory models will now become more dominant and this development may have a negative impact on the meeting between the state and the citizen. The bulk of legislation as a whole risks losing dynamics and flexibility. A more fundamental objection to digitally ready legislation is that one of the worst-case scenarios is/would be that the legislative power becomes more concerned with digitalization than with the citizen.

To avoid this scenario, a wider range of substantive benchmarks may be needed for the choice between discretionary and binary regulation than are sketched out in the political agreement of digitally ready legislation. A limitation of discretionary regulation may, in my opinion, appear to be substantially relevant and suitable in some areas – e.g. within tax law – but the primary reason for opting for a close-end and "square" regulatory template should not be the need of digitalization in as many administrative functions as possible. With a view to this, the ongoing transformation of Danish legislation into a digitally compatible regulatory architecture can end up being both a step forward and a step backward.

Paving the Way for Google – Legal Certainty Implications for Legitimising Public Cloud Services in Swedish Schools

MARIA LINDH[1]

Introduction

> In the age of statistics, there is increasing slippage between the rule of law and the rule of conformity. Contemporary law makers increasingly believe that, if most people are doing it, it cannot be wrong, and should be legalized (van Leeuwen 2007, p. 97)

Digital technology is becoming embedded into everyday life all over the globe, including in education, where pupils are enthusiastically educated with the help of digital applications. It is important to investigate this development, as implementation of these new technologies is progressing at a far faster pace than relevant regulative processes in society that safeguard the rights of individual citizens, such as students' right to privacy. The opening quotation frames this article, which takes a critical approach to education's adaptability. The text will focus on how educational systems implement information and communication technologies (ICTs) with back end affordances, such as the harvesting and processing of students' personal data. Most importantly, this article does not question free public cloud services' usability as such, but instead highlights their drawbacks concerning privacy issues for users. In line with Jones' (2015) statement that "[t]*he affordances of technology do not reside in essential features of socio-technical assemblages rather they are found in the relationships between assemblages and those that use them*" (p. 345), the point of departure is that technologies are never neutral. Instead, they can be perceived as "*a site of social struggle*". This article explores the legitimation of ICTs such as free public cloud services in schools. It is also known that services like these utilise user-generated data to create algorithmic identities (Cheney-Lippold 2011) for purposes not fully known. The point of departure in this study is that such practices clash with the Swedish public educational traditions because they

[1] Senior Lecturer at the Swedish School of Library and Information Science, University of Borås.

infringe students' privacy and are therefore problematic in relation to legal regulations that protect personal data,[2] such as GDPR.

This study contributes to research on tensions between surveillance of pupils, their right to privacy, and their right to use these services (e.g. Livingstone 2016; Lupton & Williamson 2017).[3] Additionally, it builds on previous research within education, i.e. educational governance and learning analytics (e.g. Edwards 2015; Edwards & Carmichael 2012; Roberts-Mahoney et al. 2016; Williamson 2016a, 2016b). Furthermore, this study complements previous research, as it explores how the implementation and use of ICTs such as free public cloud services[4] have been legitimated within the Swedish educational sector (e.g. Lindh 2017).

There is a common understanding in Sweden, as well as within the EU, that e-initiatives are necessary to further innovation and development. This tendency also applies to the educational sector. In 2015, the Swedish government decided to develop national IT strategies for the educational system (Utbildningsdepartementet 2015), issuing a memorandum in 2017 (Regeringskansliet 2017) concerning the strengthening of digital competence/literacy in the educational goals. These incentives are not new, preceded by previous strategic e-initiatives, some of which are presented below. Based on this development, the aim of this article is to discuss the legitimation of free public cloud services in the Swedish public educational system in order to unveil power structures that have shaped discourses about the implementation of these new technologies. The following questions are discussed:

1. How have ICTs in education been depicted and legitimised, and how can this legitimation be understood?

2. What are the implications of ICT legitimation in relation to affordances of free public cloud services?

In order to answer these questions, two Swedish policy documents have been scrutinised. These documents articulate why digital technologies

[2] EU defines personal data on their website *What is personal data?* Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [2021-01-12]

[3] These sources' primarily focus on children's rights, rather than the rights of pupils.

[4] Free public cloud services, such as Google's G Suite for Education is here defined as a type of ICT.

should be implemented and used. The policies were issued in 2011,[5] when free public cloud services, such as Google's,[6] were first introduced in the Swedish public educational system.[7] The choice to delimit the study objects to the Swedish context is due to the identification of Sweden as an early adopter of new technology (World Economic Forum 2016). Since their introduction, these services have expanded significantly. Google and its free cloud services are frequently used as an example in this study because of the company's position as one of the most influential actors within the digital economy. Consequently, its services are widely known and have a manifest impact on users and institutions. Google's free cloud services have also been introduced into the schools of the City of Gothenburg.[8]

As a point of departure, the policy documents are regarded as reflections of norms and values in society during this specific time period. The policies represent both national and municipal levels. These documents are: A memorandum entitled *IT in the General Public's Service – A Digital Agenda for Sweden* issued by Näringsdepartementet (Ministry of Enterprise and Innovation 2011) and an ICT strategy for education – *Gothenburg schools InTime* – issued by the City of Gothenburg (2012), written by district education officials within the City of Gothenburg.[9]

ICT initiatives in Swedish education[10]

Since the 1990s, the idea of implementing ICTs in teaching and learning has greatly influenced Swedish education. An early initiative was based on the idea that each student should have their own computer, which led to the introduction of a "*one-to-one laptop*" policy in Swedish municipalities (e.g. Player-Koro & Beach 2014). Initiatives like these have been furthered by the

[5] "Salems kommun går över till Google Apps för både anställda och skola". Press release 13 January, 2011. Available at: https://www.mynewsdesk.com/se/google/pressreleases/salems-kommun-gaar-oever-till-google-apps-foer-baade-anstaellda-och-skola-562150 [2021-01-12]

[6] Google is a cloud provider that among other things has developed free cloud services for education, called *G Suite for Education* (previously called *Google Apps for Education*). Another cloud provider with the same type of free cloud service is Facebook, with a service called *Facebook for education*.

[7] A school managed by municipalities or independently, supported by public funds.

[8] "Göteborgs stad skriver helt nytt avtal med Google". Published 26 March, 2014. Available at:http://www.pearltrees.com/anneliemedoc/integritet-och-pul/id15368305#item108937047 [2021-01-12]

[9] Swedish titles of these documents can be found in the method's chapter.

[10] There is a huge amount of research that explores this subject area from various perspectives. In this section, the references are delimited to critical studies of the implementation of ICTs in Swedish education.

discourse of the "*information society*" or the "*knowledge-based economy*" (OECD 1996). Implementation of ICTs may not always have been driven by educational concerns but instead more by economic incentives (Player-Koro 2013). Due to a decrease in public funding, governments have been pressed to shift from public resources to private (e.g. Lindh & Nolin 2016), also described as "*cycles of public to private transformation*" (Player-Koro & Beach 2014, p. 75) and discussed by Ball (2018) as "*neoliberal doubles*" between education and business.

The implementation of ICTs in the Swedish educational system has grown alongside their development within the ed-tech industry. This industry has, in various ways, pushed technological innovations into education. Simultaneously, the ed-tech industry has influenced policymakers, who have pursued several initiatives that aim to push learning technology and methods into Swedish education. In this way, the ed-tech industry has influenced how networks of actors understand various ideas about education (Player-Koro & Beach 2014).

One initiative that involves both policy makers and the ed-tech industry is the national trade show, SETT,[11] which is shaped by its international equivalent, BETT.[12] Player-Koro et al. (2018) emphasise the top-down perspective and the "*(re)circulation of global policy ideas*" (p. 696) in these events, as teachers are targeted with tangible solutions and "*persuasive messages*" (Player-Koro et al. 2018, p. 697).

These initiatives have been powered by government agencies in Sweden with ambitions to render public governance more efficient using ICTs. In 2011, the previously mentioned memorandum (Näringsdepartementet 2011) was issued, furthering the implementation of digital technologies on a national level. According to the memorandum, Sweden should aim to become the "*best in the world at using the possibilities of digitalization*" (p. 6). An outcome of this agenda was the initiation of a commission to work on implementation. According to the commission's interim report (Digitaliseringskommissionen 2013), IT holds "*immense opportunities, which are not exploited in proportion to its potential*" (p. 9), including within areas such as the Swedish educational system. Furthermore, arguments and reasons as to why digitalisation should be implemented are almost invisible,

[11] SETT's official website. Available at: https://settdagarna.se/ [2021-01-12]
[12] BETT's official website. Available at: https://www.bettshow.com/ [2021-01-12]

except for buzzwords, such as 'powerful' and 'effective' – words used frequently within the IT sector.

Initiatives like these have been hard to criticise, as they are depicted as mechanisms for change and as pedagogical problem solvers. These texts avoid discussing the various complexities and shortcomings of ICTs (Player-Koro 2013, Player-Koro & Beach 2014). Furthermore, it is important to view the implementation of free public cloud services, such as Google's, in educational systems as a form of interaction between public and private actors, shaped by an ambition to reduce costs and to increase efficiency in different processes.

Cloud services' back end affordances and privacy protection

In the wake of digitalisation initiatives in education, there has been a process within EU to strengthen data protection legislation. The Swedish government has issued several official reports examining privacy concerns, including in relation to the new EU data protection legislation, GDPR (e.g. Jonason 2018). Official reports related to the protection of student data have addressed *personal privacy* in relation to the use of IT (Integritetskommittén 2016) and *additional regulations* in relation to GDPR within schools (Utbildningsdatautredningen 2017). These official reports have been followed by government legislative proposals (e.g. *Ny dataskyddslag: regeringens proposition 2017/18:105*. (2018); *Behandling av personuppgifter på utbildningsområdet: regeringens proposition 2017/18:218*. (2018)).

In these official reports, serious problems are recognised, i.e. that students' information is collected through learning platforms, without public knowledge about how that data is processed by the supplier of these free public cloud services and for what purposes. The reports state that:

> Four out of ten upper secondary school teachers use social media to communicate with students and, according to school representatives that the committee has been in contact with, it is becoming increasingly common to use social media in teaching in Swedish schools.
>
> The use of social media can accidentally expose to others a large amount of personal data about individuals. Furthermore, it is apparent that social media [companies] use the data for their own purposes and distribute it to other companies. It is also difficult for users to understand how data is handled once the terms of use have been approved. The individual's choice is usually limited to either approving all the conditions, or declining and thus standing completely outside the social medium. In Chapter 13 on social media, the Committee maintains that the use of certain social media poses a serious risk

> to personal privacy. This risk will not lessen when used in school and furthermore, students will be unable to decide for themselves. Rather, they are encouraged by the school to use social media as well as how to use it. This may lead to an undesirable confusion of data between the student's private and school-related activities in social media.
>
> At the same time, it must also be taken into account that the use of social media in schools can contribute positively to teaching, for instance by making it easier to monitor the outside world, communicate and share material with other students, teachers and parents. (Integritetskommittén 2016, pp. 200–201) [author's translation][13]

The committee expresses a major concern regarding data collected from individual students and recognises that these datasets are of great value. The report also notes that ICT technologies, such as free mobile apps, request the processing of personal data, such as:

> ...the user's location, stored contacts, unique identification number of the device, the user's name, credit card and payment information, logs of phone calls and text messages, browsing history, user's posts on social media, email, pictures, video footage and biometric data (e.g. facial recognition and fingerprints). (Integritetskommittén 2016, p. 365) [author's translation]

Privacy policies are often opaque (Integritetskommittén 2016), not elaborating on how student data is processed, extracted and used. Gathering information on how teachers (perhaps inspired by SETT) use ICTs that may extract student data in the classroom is, therefore, a sensitive process for school management.

As we know, algorithmic identities can be created exclusively through data collected from a student's web behaviour, even without connecting this information to personal identification data (compare results in Lindh & Nolin 2016). This implies that mere implementation and use of this type of technology will infringe on students' privacy, whatever precautions are taken to protect students and comply with current regulations.

Previous research – pupils' vulnerabilities

Recently, research addressing the problems with free public cloud services has increased, including new studies of digital surveillance, the creation of

[13] Since this text was written, the Personal Data Act (PUL) has been replaced by the new, stricter regulation of GDPR together with complementary national regulations within education.

algorithmic identities and the use of predictive analytics, amongst other areas. The prerequisite for such practices is the large-scale collecting, storing and processing of personal data through the internet. This practice furthers seamless services for the user while certain user traits can be utilised by the service provider and third parties. Scholars have also examined these practices in relation to new business models, in work such as Andrejevic (2013; 2014), Cheney-Lippold (2011), Franklin (2013), Fuchs (2011; 2012), Keen (2015), Kitchin (2014), Sullivan (2014), and van Dijck (2014).

As these practices are introduced and pupils' data are utilised within the educational sector, traditionally a trusted set of institutions, pupils' vulnerabilities and privacy are increasingly the subject of study. From various research fields within social sciences, researchers have taken on the task to scrutinise digital practices. Studies have dealt with areas such as the power of code, surveillance and children, learning analytics in digital governance, the legitimation of technology, and pupils' personal information utilisation (e.g. Edwards 2015, Edwards & Carmichael 2012; Lupton 2015; Williamson 2016a, 2016b). Other research has examined how digitalisation allows for easier access to documents, such as pupils' test results, access that can impinge on pupils' privacy (Rosengren 2017).

Lupton and Williamson (2017) state that there have been very few incentives to safeguard children's rights concerning digital surveillance, despite its prevalence within education. Lupton (2015) underlines an important issue in relation to digital technologies and their use within education: how much choice, if any, are students offered? This is essentially a question about children's rights, particularly children's rights to the protection of their personal information in the context of education. In a similar vein, Livingstone (2016) discusses digital technologies as 'media effects' from a rights-based and participatory approach to children. The question she asks is similar to Lupton's, i.e. if the risks and opportunities identified in relation to digital technology usage should also be reframed in terms of children's rights "*or, are there scientific or political reasons why we should not?*" (p. 2). Livingstone (2016) argues for a plurality of approaches that acknowledge both sides of conflicts over rights, i.e. rights to use these digital technologies versus rights to personal data protection.

Discourses of digital technologies in education

The study of discourses can reveal power structures within society, structures that shape common understandings of various phenomena. Lindh (2016) has discussed how approaches to IT have changed since its introduction. She argues that the common understanding of IT has shifted from an uncomplicated perception of IT as either neutral, i.e. utilities, or revolutionary, i.e. tools that drive change. A perception of IT as a set of powerful tools in their own right and as intrinsic to life itself has shaped the explanation of cloud computing (Lindh 2017). One study examined the power structures that shaped one Swedish private school's implementation of Google's cloud services. Google's privacy policies were examined (Lindh & Nolin 2016) and discussed in relation to the sales pitch of cloud providers (Lindh & Nolin 2017). Cloud services have been proclaimed as 'powerful tools', 'game changers', 'enabling', 'empowering', 'simple', 'flexible'. Results show that cloud providers have taken the interpretative prerogative in furthering an understanding of these new technologies as 'intrinsic' to peoples' lives (ibid.).

Additionally, Selwyn's study (2013) identified discourses concerning digital technologies and education. In his work, he explores how accounts of digital education have been constructed within various discursive political, professional, academic and commercial fields. He poses the question of what wider philosophies, priorities and intentions shape the ongoing drive towards digitalisation throughout education. The discussion is dominated by politicians, businesspersons and other powerful actors, who play an outsized role in shaping public understandings of educational change and disruption (Selwyn 2013).

Legitimation through language as a theoretical base

According to Berger and Luckmann (1966), language can transcend time, place and social limits, shape reality, and create social order, to create meaning. Through language, people understand and create realities. In this way, an ongoing dialectic process characterises language use, i.e. externalisation, objectification and internalisation. Along these lines, language is used to legitimate, a repository for large collections of collective experiences and perceptions of reality. These explanations and understandings are stored on top of each other as a "*stratigraphy of understanding*" – a coherent whole. Without knowledge of how these 'strata' have been created, layer upon layer, new and entirely different understandings can be legitimised, i.e. old

experiences will be given new meaning (p. 69). All legitimations can be comprehended as "*universe-maintenance machineries*" influenced by structures of power (Berger & Luckmann 1966, p. 109).

These ideas can also be applied to language use about technology. Built on the principles of legitimation, Johansson (1997) views explanations of technology as a biased communicative dialectic process, i.e. "*How we think and talk about technology matters* [...] *and thus form our technology*" (p. 12) and vice versa. Technology and talk about IT "*are rhetorically 'charged' by the actors, both users and producers, as well as other propagandists and critics*" (p. 12). Therefore, discourses surrounding new ICTs are interesting research objects in the light of theories of the social construction of realities, as they provide a frame for discussing how ICTs, such as free public cloud services, have been legitimised within education.

Legitimation strategies

van Leeuwen (2007) has constructed an analytical framework based on Berger and Luckmann's (1966) theory, where the social construction of reality is closely related to legitimation. His framework can be used to facilitate an analysis of how legitimation occurs within social practice discourses. As such, the framework can be used to examine everyday interactions and public communication. It was first developed in a study on "*the first day at school*" and analyses legitimation processes in text material produced to introduce children to their school environment (van Leeuwen 2007).

The empirical material (further described in *Method*) was analysed by using this framework, which consists of four key categories: *authorisation*, *moral evaluation*, *rationalisation* and *mythopoesis*. *Mythopoesis*, deals with legitimation through narrative. As there is no evidence of this category in the empirical material, only the first three categories will be discussed here. In *authorisation*, legitimation is built on references to tradition, custom, law and persons, *i.e.* individuals entrusted with institutional authority. In *moral evaluation*, legitimation is constructed through discourses of value, *i.e.* value systems. In *rationalisation*, legitimation is achieved by referring to common sense and the usefulness of social actions and social knowledge that are institutionalised and accepted as valid. However, the analytical frame contains several factors and subcategories that were not considered in this analysis. Instead, a limited approach has been taken, using the main categories to describe the principal traits in the material.

The value of van Leeuwen's (2007) analytical framework for this study is in its deconstruction of the discourses used to legitimate social practices in public communication, as well as its relevance when it comes to the study of ICT legitimation strategies. The policy documents scrutinised here can be understood as products of social construction.

Method

The empirical material consists of two policies that represent national and municipal levels:

- A memorandum *IT in the General Public's Service – A Digital Agenda for Sweden*[14] issued by the Ministry of Enterprise and Innovation (Näringsdepartementet 2011) and
- An ICT strategy for education – *Gothenburg schools InTime*[15] – published by the City of Gothenburg (2012).[16]

As a point of departure, the policy documents are understood as reflecting the social practice of public communication, which deploys accepted values and norms in describing the implementation of ICTs.

Both the state and the municipality needed to communicate the need to implement ICTs in the educational system and wider society. The memorandum *A Digital Agenda for Sweden* (Näringsdepartementet 2011) relates the government's intention to create good conditions for development and innovation in society by way of digitalisation. Gothenburg's ICT strategy for education (City of Gothenburg 2012) was an effort to facilitate the implementation of ICTs in education by providing uniform standards. The overarching purpose of these documents was to persuade citizens of the necessity for more fully embedding ICTs within society and the schools of the city of Gothenburg.

These documents are significant because they were produced just as free cloud services were being introduced and sold as a 'powerful' technology for societal transformation (Lindh 2016). The two documents also enable the exploration of dialogue between government and local educational officials on integrating ICTs into society. Furthermore, the municipality had made

[14] Swedish title: *It i människans tjänst – en digital agenda för Sverige.*
[15] Swedish title: *Göteborgsskolor ITiden.*
[16] Written by district education officials within the City of Gothenburg.

efforts since 2006, at least, to work on a common ICT strategy within the educational sector and therefore had previous experience of implementing ICTs (City of Gothenburg 2012). Yet, another more instrumental reason to choose Gothenburg is its place as Sweden's second largest municipality with extensive, accessible resources, including online protocols and other documents related to political processes.

Qualitative content analysis was used to analyse the documents. Accounts consisting of a sentence or several sentences were identified on the premise that they were formulated as *reasons as to why technology should be implemented and used* within society and the educational system. All accounts that included this kind of reasoning were included in the empirical material. In principle, almost all text in the Gothenburg document was analysed, while only the introductory section and the section dealing with the digitalisation of education were considered in the case of the memorandum.

This material was then analysed using van Leeuwen's (2007) descriptions of legitimation strategies: *authorisation*, *moral evaluation* and *rationalisation* (explained in *Legitimation strategies* above). The analysis process can be described as iterative, or as a movement back and forth between the empirical material and the various categories. One difficulty in the process of analysis was that the categories moral evaluation and instrumental rationalisation tended to overlap. van Leeuwen (2007) emphasises that morality is central to moral evaluation and of secondary consideration in the case of instrumental rationalisation. Different categories can also be combined. However, there are always difficulties in using a framework that has been developed within another context. This must be taken into consideration with regard to the results, as differentiations between some of the categories in the framework are not always clear-cut. Despite these shortcomings, the use of this framework made it possible to discuss embedded legitimation strategies, as well as the assumptions underlying various reasons to implement ICTs.

The quotations in the following sections are translated by the author.

Legitimation strategies – A Digital Agenda for Sweden

This section will present and analyse the memorandum's way of arguing for *why* digitalisation is important for Sweden and its citizens. This source draws heavily on the nation or the citizens as actors. The legitimation strategies identified are *moral evaluation* and *rationalisation*.

The first example of legitimation is a quotation from the Minister of Enterprise, Energy and Communications, describing the state of Sweden as "a leading IT nation":

> Sweden is in many ways a leading IT nation with good infrastructure, advanced services and with a large proportion of the population who regularly use IT and the internet. But if we think that we live in the best of worlds, where nothing remains to be done, then I am afraid that we will lose our edge. (Näringsdepartementet 2011, p. 5)

An image of Sweden materialises as exceptional, far ahead of other nations when it comes to IT. A 'leading' nation has 'good' IT infrastructure with 'advanced' IT services, with many regular users – i.e. many Swedes use the internet for different types of digital services on a regular basis. In the sentences after this quotation, it is stated that this fact can give people in Sweden a false sense of security. Instead, development is continuous and Sweden must keep up its pace of development to prevent sliding to a lower position.

These arguments of technological determinism are frequently used within the IT industry to push for the latest technology as the single alternative ahead (cf. Lindh & Nolin 2017). Along the same line, determinism surfaces: "[w]*e are likely to have seen only the beginning of all the advantages that the use of IT may mean*" (Näringsdepartementet 2011, p. 8). The impression is that the government has a deterministic approach, i.e. IT usage is the promise of the future.

Moreover, arguments refer to values connected to the image of Sweden as "*a leading nation*". The state values a citizen who "*regularly uses IT and the internet*", as these individuals contribute to the idea of Sweden as "*a leading IT nation*", countering the risk of Sweden "*losing* [its] *edge*". Instead, the public is expected to do its part and contribute to Sweden retaining its position as an IT nation. Embedded in this statement is the assumption that "*the best of worlds*" is a digitalised world.

Furthermore, the government's goal is that "*Sweden shall be best in the world at using digital opportunities*" by "*removing obstacles to development*" (Näringsdepartementet 2011, p. 6). It is an ambitious goal. This statement gives rise to new questions, such as why Sweden should be "*best in the world*", as it seems to be a goal. It is taken for granted that it is possible to be 'best' and, as such, is a goal worth pursuing, regardless of motivations. Furthermore, in this quote, it is obvious that it is 'good' to "*remove ob-*

stacles", no matter what these problems are. Yet some obstacles, as is discussed in the conclusion below, may exist for a reason.

In addition, it is stated that the agenda has a user perspective and that "*anyone who wants to"* should be able to *"use the opportunities that digitalisation offers"* or "*participate in the information society*" (Näringsdepartementet 2011, p. 6). This statement implies that usage should be encouraged but not mandatory. Digitalisation will give citizens 'opportunities'. Citizens can choose to be a part of the "*information society*", as if this was a parallel world into which individuals can opt in or out. This choice will also have effects, namely the ability to "*use the opportunities offered*" without any examples of what is meant by 'opportunities'.

In these formulations, legitimation is achieved through moral evaluation. All accounts include values and norms, hidden or explicit, which frame how the reader should perceive and think about digitalisation; facts, truths, and logic are absent. Some arguments refer to the effects of digitalisation and may hold an element of rationalisation, but these arguments reflect moral values rather than concrete effects.

Furthermore, the document contains arguments related to security. It outlines a case for privacy, with implications for both private and public sectors: "*public and private information systems must be secure in order to defend different values in society such as democracy, personal privacy, growth, and economic and political stability*" (Näringsdepartementet 2011, p. 9). This account mentions values central to democratic society such as security and the defence of people's privacy. Here, legitimation is based on rationalisation in combination with moral evaluation. The phrase "*secure information systems*" suggests that it is possible to defend these core values.

A Digital Agenda for Sweden – accounts concerning education

In this section, passages in the memorandum related to *why* digitalisation is important in Swedish education are presented and analysed. The argumentation is based on *use* and *users* of ICTs, i.e. pupils and teachers. Legitimation strategies identified in the material are *rationalisation* and *moral evaluation*.

In the memorandum it is pointed out how 'correct' use of technology can be effective. One of the examples mentioned in its foreword addresses education: "*If we use technology right, students with learning difficulties, can, with a personal computer, become best-in-class on searching, editing and presenting information*" (Näringsdepartementet 2011, p. 5). Here, the strategy

for legitimation is rationalisation – the actor 'we' acts purposefully to facilitate learning by means of the 'correct' use of technology. Technology is expected to function almost as a "*miracle cure*", especially for children with learning difficulties. These children are not only supposed to be helped by technology but could become "*best-in-class*" if "*we use technology right*", thus legitimising through moral evaluation.

Furthermore, there is an implicit fear that technology will not be used correctly, and that the desired effects will fail to materialise. A challenge, therefore, is how technology will be used in education: "*A strategic challenge is the issue of students' access to computers and how they are going to be used in teaching*" (Näringsdepartementet 2011, p. 33). Here the strategy of legitimation is again rationalisation, as it refers to usefulness and is based on logic and rational values. The challenge is how computers, or rather ICTs, will be used in teaching. Here, digitalisation is described as a remedy that will solve problems in education.

Instead of discussing how pupils can learn and teachers can teach using ICTs, it becomes obvious that education concerns digital development as such – as a driving force for 'modern' education, teaching and learning. The following ideas are outlined:

> Pupils and teachers ought to have access to modern learning tools for an up-to-date education. After nine years in the compulsory educational system, every pupil should be able to use modern technology as a tool for knowledge seeking, communication, creativity and learning. (Näringsdepartementet 2011, p. 8)

This account justifies the introduction of IT in education by referring to the need to 'modernise'. The word 'modern' equates with the implementation of new technology, rather than employing arguments related to educational development and learning. The legitimation strategy in the first sentence can be interpreted as moral when adjectives such as 'modern' and 'up-to-date' are combined with 'ought to' and 'should', thus shielding arguments about ICT implementation from criticism (compare van Leeuwen 2007). In the second sentence, therefore, legitimation can be categorised as a mix of rationalisation and moral evaluation, as both effects and values are emphasised. For instance, the effect of the compulsory educational system is the knowledgeable usage of technology for various purposes. In the last sentence, several areas are listed in relation to pupils' ability to use 'modern technology'. An interesting detail is that 'learning' is mentioned as the last

item on the list, which also includes 'knowledge seeking', 'communication', and 'creativity'.

Legitimation strategies in the Gothenburg ICT strategy for education

This section presents and analyses passages in the City of Gothenburg's ICT strategy in education (2012) that explain *why* ICTs should be used in education. In the strategy, ICT is articulated as an actor. Legitimation strategies identified in the material are: *authorisation*, *rationalisation* and *moral evaluation*. In the following quotation, *authorisation* is used to legitimise through references to the influential national agenda:

> When the Government in 2011 presented A Digital Agenda for Sweden, explicit elements of ICT were marked as mandatory for ensuring the development of digital literacy among children, young people and students. (City of Gothenburg 2012, p. 6)

Legitimation is achieved by referring to the authority of the government as a trustworthy institution. Furthermore, the agenda argues that "*anyone who wants to*" (see above) can "*use the opportunities that digitalisation offers*", *thus framing* digitalisation as a gift. However, the strategy also pictures ICTs and digitalisation as mandatory and "*impossible to deselect*". The strategy "*...clarifies ICT as part of the work which cannot be deselected*" (City of Gothenburg 2012, p. 3). This imperative is stated twice in the document.

Accounts referring to global developments in education and to discussions about how education can be transformed by the use of ICTs are other examples of authorisation: *"internationally, ICT in education has been increasingly focused on and in many countries governments and ministries are discussing how ICT can transform education"* (Gothenburg City 2012, p. 6). Implicitly, this quotation suggests that Sweden should work in the same direction. Legitimation is achieved by explicitly connecting Sweden to an international context.

Authorisation is also used as legitimation, with reference to the city budget. In the city budget from the same year, it is indicated that ICTs are a prerequisite for and should infuse the educational system, as ICTs have 'power' and 'potential' that can be used to strengthen educational development in the city:

> The city budget for 2012 outlines ... that education should be permeated with information and communication technologies (ICT). Using the potential of

> ICT is a prerequisite for strengthening the development of education including preschools in Gothenburg. (City of Gothenburg 2012, p. 5)

In this quotation, the ed-tech industry's selling arguments are clearly recognisable (compare Lindh & Nolin 2017). Adjectives connecting ICTs with 'permeated', 'power' and 'potential' are combined to point out an entirely new reality within education. This new reality is a 'prerequisite' for strengthening educational development. The legitimation strategy is rationalisation relating to "*how things are*", framing ICTs as a natural part of educational improvement. It includes reasoning phrased as axioms or self-evident conclusions, including a section relating the activity "*of using*" ICT's potential power for the 'strengthening' of educational development. Again, arguments are based on usability and logic.

Additionally, to further strengthen the argument for using ICTs in education, the vision of the 'knowledge city' is prominent in the document. ICT implementation will create a city "*with world-class training*" (City of Gothenburg 2012, p. 6). This phrasing is analogous to the idea of Sweden as a "knowledge-nation" with positive connotations that adhere to a previously legitimised discourse. The legitimation strategy here is to refer to moral values. Moreover, the ambitions of the City of Gothenburg converge with those of the state.

Another argument, identical with the national agenda, is that education should be 'modern': "*Gothenburg should offer children, young people and students training that is equal, timely and relevant*" (City of Gothenburg 2012, p. 7). Again, the legitimation strategy is moral evaluation, with the use of adjectives that favour certain qualities in training such as 'equality', 'timeliness', and 'relevance', thus protecting the ICT strategy from criticism (compare van Leeuwen 2007).

In the following quotation, several reasons for implementing ICTs are mentioned. Note that ICTs are portrayed as an actor providing a variety of opportunities:

> ICT in teaching provides the opportunity for participation and co-creation and provides equally good prerequisites for all children, young people and students. Therefore, learning takes place, in both physical and digital environments, with continuous access. (City of Gothenburg 2012, p. 7)

In this statement, the legitimation strategy is mainly rationalisation influenced by moral values, as it implies truths about ICT and learning, for instance that participation and co-creation are assumed to be positive. Furthermore, the idea that everyone will have "*equally good prerequisites*"

due to the provision of ICTs seems like a rational argument but simplifies the idea of teaching and learning. Similar arguments for the use of ICTs in education state that everyone should have "*equal opportunities to use ICT*", opportunities that are "*created by ICT*", which in turn "*presupposes diversity and breadth*" (City of Gothenburg 2012, p. 3). Consequently, it is ICTs, rather than teachers, that will create the "equally good" opportunities and prerequisites for students. The explicit assumption is that ICTs will further 'diversity' and 'breadth', without any references to what these terms mean in this context. Here, again, is a much-simplified explanation of ICTs in education. This resonates with previous research, which shows that the implementation of ICTs and their use in education varies widely, both between schools and between teachers (Lindh et al. 2016).

Furthermore, based on the prerequisites afforded by ICTs, learning takes place in both 'physical' and 'digital environments'. Here, "*continuous access*" is stressed as a positive value. This access to learning is made possible through digital rather than physical environments. The next sentences in this paragraph stress different values afforded by ICTs:

> Work with ICT in education creates conditions for high quality teaching and increased goal achievement and is a prerequisite for schools to be able to be a part of community development. ICT can also contribute to an increased desire to learn and is a prerequisite for schools' work on ethics and critical thinking. (City of Gothenburg 2012, p. 7)

ICTs are ascribed values, such as "*high quality teaching*" and "*increased goal-achievement*". ICTs are also a condition for education as a democratic actor in society. Here, the legitimation strategy is a combination of rationalisations and moral evaluation. Again, ICTs are the positive actor that can add value and improve education, an actor that "*creates conditions*" to achieve goals, such as 'high quality', 'goal achievement', 'ethics' and 'critical thinking'.

Another section with the same argumentation holds that ICTs can "provide opportunities for the development of children's, pupils' and students' democratic attitudes and the ability to critically and ethically evaluate information and content." (City of Gothenburg 2012, p. 8). In line with these arguments, legitimation is achieved by moral evaluation:

> All students and personnel are offered challenging and invigorating learning environments that create the conditions for active, creative, and engaging participation in a global network society. (Gothenburg City 2012, p. 3)

Furthermore, the city mission statement that "*all students and personnel should feel the desire to learn, participate and to contextualise their knowledge and skills*" (City of Gothenburg 2012, p. 3) is supported by the use of ICTs in education, or, as stated, "*where ICT can play a crucial role*" (City of Gothenburg 2012, p. 6). Similarly, this argument is legitimised through moral evaluation. The value here is that all involved in education ought to "*feel the desire to learn*". Participation is perceived as morally good. 'Contextualising' knowledge and skills is not further explained or defined and constitutes another example of legitimation involving empty phrases.

It is notable that the ICT strategy does not only tell the actors in education what to do, it also explains how they should feel by using words such as 'desire', and 'inspiration':

> Learners [both students and personnel] are inspired to expand their learning beyond what they thought was possible. Sensitivity, power and flexibility are key words. (City of Gothenburg 2012, p. 7)

In this mission statement, the arguments transform accounts of inspiration, surprise and amazement into natural by-products of ICTs. Not only is technology powerful, the user should also believe in its ability to empower, thus enabling learners to transcend their initial learning limitations. It is implied that power, sensibility and flexibility will be valuable resources, facilitated through the use of ICTs. What this means is not made explicit. Instead, the mere use of these terms communicates positive values. Legitimation is thereby achieved through moral evaluation. 'Learners' will excel in learning "*more than they thought was possible*".

ICTs will also change how teaching and administration are carried out:

> ICT as an integral part of everyday educational life offers the opportunity for new pedagogical and administrative methods of working for greater goal fulfilment. With the help of digital technology, the development of teaching and learning is made possible. Access to modern technology creates working methods that were previously not possible. (City of Gothenburg 2012, p. 8).

These sentences convey high, almost impossible, expectations for ICT applications. In these sentences, legitimation is achieved by the use of rationalisation, where ICTs again are the actor: "*ICT offers*", "*digital technology helps*", "*access creates*", with certain goals: "*for greater goal fulfilment*", "*development of teaching and learning is made possible*", new "*working methods*".

The most obvious rationalisation legitimations draw on discourses of "improved effectiveness": "For improved effectiveness and more effective use of time, money and personnel, the power of technology is utilised to transform processes and structures" (City of Gothenburg 2012, p. 3).

Another similar account uses the same legitimation strategy and stresses the "*ICT perspective*" in every activity, to facilitate a perspectival shift:

> In all processes and decisions, there is an underlying ICT perspective. This applies both to development work and in everyday educational work. In order not to restrict or hamper the possibilities of educational and administrative development with the help of ICT, old structures are reviewed. (City of Gothenburg 2012, p. 8)

The following quotation notes the variety of ICTs, and that not all of them are 'appropriate' to various "*teaching situations*":

> Each child and each individual student will have access to appropriate tools for their learning and take advantage of these opportunities in well adapted teaching situations that produce a creative environment for testing ideas and solving problems. (City of Gothenburg 2012, p. 9)

Here, moral evaluation is used, as the account draws on value systems related to creative learning, positioning ICTs as tools for problem solving and creativity.

Another argument is related to the interconnectivity and communication that ICTs facilitate, using wording such as "*interconnected and networked teachers*" (City of Gothenburg 2012, p. 3) and:

> Teachers who connect and network facilitate cooperation and collaboration and provide opportunities for the development of educational work and is a prerequisite for the development of the professional role. (City of Gothenburg 2012, p. 9)

Connectivity is not only related to teachers and students, but also to resources and information:

> All teachers are working individually and in teams with technology that connects them to information, content and resources that lead to stimulating and relevant learning for all children, pupils and students. (City of Gothenburg 2012, p. 3)

> With modern information and communication technologies, teachers and students meet in new learning situations with continuous access to data, content, resources, skills and experience. (City of Gothenburg 2012, p. 9)

Connectivity is a central concept and persuasive discourse used by cloud providers (compare Lindh & Nolin 2017). Another important discourse that legitimises ICTs in education or any type of system are references to the concept of *quality*. The ICT strategy also includes these arguments: "*For increased quality, modern technologies are used in the work of monitoring, evaluation and analysis of education*" (City of Gothenburg 2012, p. 4). In the next quotation, the means for improving quality are enumerated. Apart from an improved economic situation, arguments focus on issues related to monitoring and control – from "*single units*" to the entire school system. By using adverbs such as "*easily, smoothly, efficiently and clearly*", rationalisation of ICTs is legitimised by shielding these tools from criticism:

> The city of Gothenburg is striving for the continuous quality improvement of pre-schools and schools. A basis for this work is to easily, smoothly, efficiently and clearly use ICT in the processes of analysing quality, from single units … to the entire organisation. IT support is therefore used systematically to monitor goal achievement, through the review of examination dossiers and financial goals etc. In addition, IT support is used for quick feedback and evaluation in learning situations as well as in relation to users. Evidence collected is then used as a basis for analysis with the aim of developing education. (City of Gothenburg 2012, p. 10)

In the strategy, there is a noticeable lack of references to ICT use and pupils' privacy. This absence resonates with a de-emphasis of the complexities of technologies, such as free public cloud services, as will be discussed next.

Legitimation of free public cloud services and its implications

The aim of this article was to discuss the legitimation of free public cloud services in the Swedish public educational system in order to reveal the power structures that have shaped discourses about their implementation. The following questions were discussed: How have ICTs in education been depicted and legitimised, and how can this legitimation be understood? What are the implications of ICT legitimation in relation to affordances of free public cloud services?

Overall, the legitimising arguments in the policies reflect an overreliance on what technology affords and ICTs are explained in simple terms, avoiding complexity. In line with Selwyn's (2013) exploration of discourses around digital education, the images of technology as transformative for education, together with values such as its intrinsic qualities, are prevalent. Notions such as 'modern' and 'up-to-date' underline the importance of

development and change within education, rather than arguments related to the overarching goal of education – that students learn. Instead, learning is always argued for in relation to technology use, i.e. that technology facilitates learning. Technology is perceived as a remedy, as a powerful solution to the problems of learning in education. In the city of Gothenburg's strategy, ICTs are not just put forward as a complement; it is portrayed as a prerequisite. It is argued for as necessary to education. With the implementation and use of ICTs, education will become 'modern', which is also emphasised in the government agenda. Furthermore, legitimation is achieved by using the discourse of Sweden as an "*IT nation*" and "*knowledge nation*", or Gothenburg as the corollary "*knowledge city*", as in the city of Gothenburg's strategy. Another reflection is that students and teachers are categorised together as 'learners'. This means that the teachers are, more or less, rendered invisible in the material, and their specific skills are not taken into consideration.

Discourses based on values and norms, hidden or explicit, dominate the legitimation of digital technologies, shaping how we perceive and think about digitalisation within education. In accordance with van Leeuwen's (2007) analytical frame, all legitimation strategies excepting *mythopoesis* were identified in the documents studied. Strategies of legitimation through accounts referring to moral rationalisation were predominant in the material. Arguments for implementing ICTs were legitimised through rationalisation. A few accounts used authorisation as a legitimation strategy, emphasising arguments by referring to the authority of institutions.

The legitimation strategies identified above can be understood as a shield protecting these arguments from criticism, as they seem so reasonable in relation to existing values and norms in society. Similar accounts and strategies can be found in cloud providers' legitimation of free public cloud services. The rhetoric of cloud providers draws on ideas of technology's ability to *empower* and *transform*, among other central themes, discussed by Lindh and Nolin (2017). Providers of free cloud services, such as Google, use persuasive power to communicate simply, thus avoiding images that convey the complexities of implementation and use. The findings indicate that the interpretative prerogative appropriated by cloud providers affects how these services are perceived within public institutions, such as Swedish policymaking circles, whose leaders set the agenda for educational development.

Inspired by Berger and Luckmann's (1966) ideas, the process of implementation of new ICTs in education, the 'layer' or 'strata' of legitimation

investigated here, can be understood as copied from the tech industry (compare Lindh & Nolin 2017), with descriptions of ICTs as "*easy to use*" and "effective tools" with "transformative power", despite evidence of both strengths and weaknesses in its implementation and use. Based on Berger and Luckmann's (1966) theory of social construction, one can argue that the tech industry controls the "*conceptual machineries*", meaning that they have the power to continuously legitimise new ICTs. Furthermore, implementers and users legitimise this power structure when they adopt the same "*universe-maintenance*" language of legitimation (e.g. Lindh 2017) to describe technological innovation within the context of education (e.g. Player-Koro et al. 2018).

As 'modern', 'democratic' and 'technology' are equated, it is difficult to oppose any form of ICTs in education. Who does not want more modern and democratic education? The implication of these strategies of argumentation and legitimation is that the specific problems faced by the current educational system are never directly discussed. This approach reduces complexity, limiting any reflection over the suitability of specific technologies in various educational contexts. Instead, technology is legitimised as a "*quick fix*" – a potent actor that will not only solve problems but further new innovations in education and teaching. It is therefore relevant to inquire if this development will also interfere with the status of the teacher, as the policies are detached from questions of how teachers can use ICTs to construct new learning practices.

The documents scrutinised in this analysis do not support a diversified or argumentative approach to various types of ICTs. The crucial issue in this article is not *if* ICTs should be used or not. The argumentation concerns *which* technology, *how* it should be implemented and used, and finally *for what purposes* in relation to their diverse affordances.

Concluding reflections

Digital technology has become embedded in education and has transformed aspects of learning and teacher-student interaction (Lindh et al. 2016). This study does not discuss whether ICTs in education are needed or not. Rather, the article examines how ICTs have been legitimised using assumptions and values, by exploring arguments within government at the national and local level.

It can be debated whether it is appropriate to discuss values in documents that are now over seven years old. This choice has been made because

it allows for an analysis of the processes of legitimation – discussed by Berger and Luckmann (1966) as 'sedimentations' that build up over time – as new requirements and practices must be reconsidered.

There is no doubt that digital technology and ICTs can facilitate the daily work of people and organisations. However, it is not obvious that the effects of digitalisation are entirely positive and straightforward. Therefore, it is in no one's favour to ignore the complexity that new ICTs entail. Identified complexities concerning free cloud services include, for example, their back-end affordances, such as tracking, collecting and processing personal data.

As previous research has discussed, the value of people's data cannot be underestimated in relation to today's technologies, and the new opportunities to innovate, control, predict, affect and effect that these technologies enable. With the utilisation of free cloud services in education – such as Google – it is not known how cloud providers extract, process and use personal data, as privacy policies are opaque and hard to decipher (Lindh & Nolin 2016). Furthermore, cloud services are in constant transformation; it is therefore impossible to foresee how utilization of this personal data will develop.

In the Gothenburg strategy, ICTs are not identified as negotiable. Instead, they seem to be compulsory, as it is stated that they "*cannot be deselected*". This is a rather inflexible statement, an imperative. The effect may be that this wording deflects questions about how ICTs are implemented and used.

In the wake of Snowden's revelations, news of Cambridge Analytica's use of Facebook data, and similar stories, the one-sided positive view of internet-based technology has come into question. Still, it is not easy to question the rationales driving the growth of the digital economy and its incorporation within the public sphere. Therefore, I argue that pupils should be able to use services like these, but without risking control over their personal data.

It is significant that the use of ICTs such as Google's free public cloud services are legitimised by central institutions, not the IT sector but government agencies and academia as well. This study concerns pupils in the lower levels of the educational system. However, these services are used within all educational levels as well as in society at large, both in private and employment sectors. van Dijck (2014) argues that institutional structures support the extensive use and processing of information via online services, because they encourage users to rely on them. To build substantive trust in digital technology, O'Neill (2017) advocates integrating human values into algo-

rithmic models, instead of values of efficiency and profit or default rates (p. 206). Giant actors like Google and Facebook need to become transparent, especially because the public is learning more about these devices and how personal data is utilised in today's Big Data economy. O'Neill argues that the choices regarding which data to utilise and to build models around, are "*fundamentally moral*" (2017, p. 218).

To paraphrase van Leeuwen (2007), recalling this text's introductory quotation, the increasing "*slippage between the rule of law and the rule of conformity*" (p. 97), as I understand it, means that a common practice is generally not questioned. Therefore, the widely distributed use and acceptance of ICT's affordances, allowing questionable back end practices, are not extensively questioned within our institutions, such as the school system. Importantly, these services are developed today principally for other purposes than educational, such as the exploitation of "*data exhaust*" (Zuboff 2019). Central to this line of argumentation is the success the ed-tech industry has had with these legitimation strategies. Consequently, there is an increasing need to discuss the substance and implications of digitalisation, not just within the educational system, but in other public and private institutions as well.

References

Andrejevic, M. (2014). The big data divide. *International Journal of Communication*, 8: 1673–89.

Andrejevic, M. (2013). *Infoghut: How too much information is changing the way we think and know*. New York, NY: Routledge.

Ball, Stephen J. (2018). Commercialising education: profiting from reform! *Journal of Education Policy*, 33(5): 587–589. DOI: 10.1080/02680939.2018.1467599

Behandling av personuppgifter påutbildningsområdet: regeringens proposition 2017/18: 218. (2018). Stockholm. [Government Bill]

Berger, P. L. & Luckmann, T. (1966). *The social construction of reality: a treatise in the sociology of knowledge*. London: Penguin books.

Cheney-Lippold, J. (2011). A new algorithmic identity: Soft biopolitics and the modulation of control. *Theory, Culture and Society,* 28(6): 164–181.

City of Gothenburg (2012). *Göteborgsskolor ITiden – IKT-program Göteborgs stad.* [Report] Available at: https://docplayer.se/789755-Goteborgsskolor-itiden.html [2021-01-12]

Digitaliseringskommissionen (2013). *En digital agenda i människans tjänst – Sveriges digitala ekosystem, dess aktörer och drivkrafter* (SOU 2013:31). Stockholm: Fritzes Offentliga Publikationer.

Edwards, R. (2015). Software and the hidden curriculum of digital education. *Pedagogy, Culture and Society* 23(2): 265–279.

Edwards, R. & Carmichael P. (2012). Secret codes: the hidden curriculum of semantic web technologies. *Discourse: Studies in the Cultural Politics of Education*, 33(4): 575–590.

Franklin, M. (2013). *Digital dilemmas: Power, resistance, and the Internet*. Oxford: Oxford University Press.

Fuchs, C. (2011). A contribution to the critique of the political economy of Google. *Fast Capitalism*, 8(1): 1–24.

Fuchs, C. (2012). Google capitalism, tripleC: Communication, capitalism & critique. *Open Access Journal for a Global Sustainable Information Society*, 10(1): 42–48.

Integritetskommittén (2016). *Hur står det till med den personliga integriteten? – en kartläggning av Integritetskommittén* (SOU 2016:41). Stockholm. Official report.

Johansson, M. (1997). *Smart, fast and beautiful: on rhetoric of technology and computing discourse in Sweden 1955–1995*. Diss. Linköping: Univ. Linköping.

Jonason, P. (2018). The Swedish measures accompanying the GDPR. E-conférence, National Adaptations of the GDPR. Available at: https://blogdroiteuropeen.files.wordpress.com/2018/06/sweden.pdf [2021-01-12]

Jones, C. (2015). Openness, technologies, business models and austerity. *Learning, Media and Technology*, 40(3): 328–349.

Keen, A. (2015). *The Internet is Not the Answer*. New York: Atlantic Monthly Press.

Kitchin, Rob (2014). *The data revolution: Big data, open data, data infrastructures and their consequences*. London: SAGE.

Lindh, M. (2017). *Cloudy talks [Electronic resource]: exploring accounts about cloud computing*. Diss. Borås: Högskolan i Borås. Available at: urn:nbn:se:hb:diva-11178

Lindh, M. (2016). As a utility: Metaphors of information technologies. *Human IT*, 13(2): 47-80. Available at: urn:nbn:se:hb:diva-10679

Lindh, M. & Nolin, J. (2017). GAFA speaks: Metaphors in the promotion of cloud technology. *Journal of Documentation*, 73(1): 1–22. Available at: urn:nbn:se:hb:diva-10712

Lindh, M. & Nolin, J. (2016). Information we collect: Surveillance and privacy in the imple…mentation of Google Apps for Education. *European Educational Research Journal*, 15(6): 644–663. Available at: DOI: 10.1177/1474904116654917

Lindh, M., Nolin, J. & Nowé Hedvall, K. (2016). Pupils in the clouds: Implementation of Google Apps for Education. *First Monday*, 21(4). Available at: DOI: 10.5210/fm.v21i4.6185

Livingstone, S. (2016). Reframing media effects in terms of children's rights in the digital age. *Journal of Children and Media*, 10(1): 4–12.

Lupton, D. (2015). Data assemblages, sentient schools and digitised health and physical education (response to Gard). *Sport, Education and Society*, 20(1): 122–32.

Lupton, D. & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, 19(5): 780-794.

Ny dataskyddslag: regeringens proposition 2017/18:105. (2018). Stockholm. [Government Bill]

Näringsdepartementet (2011). *It i människans tjänst – en digital agenda för Sverige*. Report. Available at: https://www.regeringen.se/informationsmaterial/2011/09/it-i-manniskans-tjanst--en-digital-agenda-for-sverige/ [2021-01-12]

O'Neil, C. (2017[2016]). *Weapons of math destruction: How big data increases inequality and threatens democracy*. London: Penguin Books.

Player-Koro, C. (2013). Hype, hope and ICT in teacher education. A Bernsteinian perspective. *Learning, Media and Technology*, 38(1): 26–40. Available at: http://dx.doi.org/10.1080/17439884.2011.637503

Player-Koro, C. & Beach, D. (2014). 'Roll-out neoliberalism' through one-to-one laptop investments in Swedish schools. In Landri, P.; Maccarini, A. & De Rosa, R. (eds.). *Networked together: designing participatory research in online ethnography*. CNR-IRPPS. doi:10.14600/978-88-98822-02-7-8

Player-Koro, C.; Bergviken Rensfeldt, A. & Selwyn, N. (2018). Selling tech to teachers: Education trade shows as policy events. *Journal of Education Policy*, 33(5): 682–703. DOI: 10.1080/02680939.2017.1380232

Regeringskansliet (2017). *Stärkt digital kompetens i skolans styrdokument*. Memorandum 2017-03-09.

Roberts-Mahoney, H.; Means, Alexander J. & Garrison, M. J. (2016). Netflixing human capital development: Personalized learning technology and the corporatization of K-12 education. *Journal of Education Policy*, 31(4): 405-420. doi: 10.1080/02680939.2015.1132774

Rosengren, A. (2017). The Swedish Black Box. On the Principle of Public Access to Official Documents in Sweden. In Jonason, P & Rosengren, A (Eds.). *The Right of Access to Information and the Right to Privacy: A Democratic Balancing Act*. Working paper 2017:2. Södertörns högskola. Available at: https://www.diva-portal.org/smash/get/diva2:1166661/FULLTEXT01.pdf [2021-01-12]

Selwyn, Neil (2013). Discourses of digital 'disruption' in education: a critical analysis. *Fifth International Roundtable on Discourse Analysis*, City University, Hong Kong, 23–25.

Sullivan, J. L. (2014). Uncovering the Data Panopticon: the urgent need for critical scholarship in an era of corporate and government surveillance. *The Political Economy of Communication*, 1(2). Available at: http://polecom.org/index.php/polecom/article/view/23/192 [2021-01-12]

Utbildningsdatautredningen (2017). *EU:s dataskyddsförordning och utbildningsområdet* (SOU 2017:49). Stockholm. Official report.

Utbildningsdepartementet (2015). *Uppdrag att föreslå nationella it-strategier för skolväsendet*. Government decision 1:2 2015-09-24, U2015/04666/S

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2): 197–208.

van Leeuwen, T. (2007). Legitimation in discourse and communication. *Discourse & Communication*, 1(1): 91–112.

Williamson, B. (2016a). Digital education governance: Data visualization, predictive analytics, and 'real-time' policy instruments. *Journal of Education Policy*, 31(2): 123–141. DOI: 10.1080/02680939.2015.1035758

Williamson, B. (2016b). Political computational thinking: Policy networks, digital governance and 'learning to code'. *Critical Policy Studies*, 10(1): 39–58.

World Economic Forum (2016). *Global information technology report 2015*. Available at: http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf [2021-01-12]

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: Hachette Audio.

Discussions in social media regarding the implementation of the General Data Protection Regulation

RIKARD FRIBERG VON SYDOW[1]

In May 2018 the European Union General Data Protection Regulation (GDPR) was implemented in Sweden. The new legislation changes some of the premises for using personal information in business and government. During 2017 and 2018 these new premises were discussed by professionals and others in different social media settings. This research focuses on these discussions using three Facebook groups representing three different professions affected by the GDPR. What was seen as positive with the new legislation? What fears and worries can be identified among the professionals? What questions are more often discussed than others? These are the types of questions that will be asked to the material. The GDPR itself and its consequences will not be the focus of the discussion. The goal is to describe an online discourse and identify levels of awareness and preparedness among different groups of professionals that were (and are) affected by the new law.

Background: The implementation of the GDPR

The GDPR aims to harmonize the rules regarding data protection in the different EU member states. The regulation was implemented in the member states on 25th of May 2018. The GDPR is a continuation of the Directive 95/46/EC, which was an earlier directive regulating parts of the protection of personal data in the European Union member states. A difference between the Directive 95/46/EC and the GDPR is that the latter applies directly to the states – it does not have to be transferred to a national law (Voigt et al 2017, p. 1f). In Sweden, the GDPR, translated into "Dataskyddsförordningen", is supplemented with a new national law ("Lag 2018:218 med kompletterande bestämmelser till EU:s dataskyddsförordning"). As we will see, in the further analysis, the implementation of the new legislation was widely discussed, and considered problematic by several professions.

[1] Rikard Friberg von Sydow, SeniorLecturer in Archival Science, Södertörn University.

The general opinion seemed to be that a lot was about to change in respect of personal data.

A number of studies deal with work-related change in connection with the GDPR implementation. In the medical field, for instance, it was regarded as a major change. It was considered that medical professionals had to have some kind of guidance if they were to comply with the new law. One major discussion concerned the considerable fines that could be imposed on organizations not complying with the law (McCall 2018, Cornock 2018). Discussions and analysis of how the GDPR will affect other professsions have also been carried out. From the perspective of business in general the GDPR has been described as an "Y2K for business" (Bihari 2018). Research has also been performed regarding different agents in the information sector such as data brokers (Bui 2017) and librarians (Bailey 2018).

The social media setting: Facebook groups

Most studies that have used Facebook as a source have focused on psychological and social concerns regarding Facebook use. Examples are Childs et al. (2015) "Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management" and Cionea et al. (2017) "A profile of arguing behaviours on Facebook" that examine user behaviours. A few studies have been connected to students' and workers' (private) use of Facebook: Manasijević et al. (2016) "Exploring students' purposes of usage and educational usage of Facebook" observed students using Facebook for communication, collaboration and resource sharing, while Robertson et al. (2016) "Social media at work: The roles of job satisfaction, employment status, and Facebook use with co-workers" examined Facebook usage in relation to workplace satisfaction, finding that people who interacted more with their co-workers over Facebook had a higher workplace satisfaction. Yet another study is about work-related change, comparable to the GDPR but in a much smaller area – a change in school politics in Slovakia. This study (Kascak et al. 2016) focused on emotional expressions in discussions regarding work-related change. There are also studies of how social media are used as a substitute for other news sources. Müller et al. (2016) "Appetizer or main dish? Explaining the use of Facebook news posts as a substitute for other news sources" indicates that Facebook users feel informed by just seeing (not really reading) news posts. This, the authors argue, might be something we have to discuss in a more social media dense future.

Method, technique and ethical concerns

This study focuses on posts and threads – not users as most of the studies above. The method used is a hermeneutic case-study. Searches on "GDPR" were made within three groups of professionals. From the first analysis of the identified posts and threads, preliminary categories were created. Subsequently, these categories were used in the second analysis to identify the various discourses on the GDPR by measuring the amounts of different types of posts. Alison Pickard discusses a method called "Online focus group" in her book "Research Methods in Information". An online focus group is a group discussing a topic online. The researcher monitors the group and takes notes of how the discussion evolves (Pickard 2013, p. 47). The method used here is similar to online focus groups, but with the essential difference that discussions that had already taken place were used in this study. Furthermore, I was not involved in the discussion; the conversations were already concluded when I analyzed them.

To understand the discussions that will be analyzed in this text we need to have a common understanding of what a Facebook group is and how it works. Facebook groups:

> are the place for small group communication and for people to share their common interests and express their opinion. Groups allow people to come together around a common cause, issue or activity to organize, express objectives, discuss issues, post photos and share related content (Hicks 2010).

Any content posted can be discussed/answered by other groups members. I choose to call the first post (from which I make the distinctions of the categories in analysis 1) "Post". The person posting the material is usually called "original poster" or "thread starter". There is also an opportunity to start a sub-thread (an answer to another user's answer to a post).

We might also need to have a common understanding of group administration. Any Facebook user can start a group, and the user then becomes the administrator of that group. An administrator can create his or her own rules for the members to comply to. The administrator can add or remove members, add new administrators (or "moderators" – an administrator with lesser authorizations). The administrator is the user who controls the discussion area which a Facebook group deals with (Facebook 2018).

The study was performed on three Facebook groups connected to professions affected by the implementation of the GDPR. The names of the groups have been changed to keep the discussions anonymous. All groups are directed towards a Swedish audience and discussions, posting et cetera

is usually done in Swedish. The group I call "The Archivists", is a group aimed at archivists. Archivists are responsible for large amounts of information in both the public and private sector. In Sweden today, an archivist in the public sector is responsible for information not only in archives but also in the organization in general and the title archivist therefore refers both to employees working in historical archives and to employees working with record management. The group I choose to call "The Programmers", is a group for programmers, system administrators and other IT-professionals. IT-professionals are affected by the GDPR in many ways, both in their task of constructing and administrating data bases, and in their role as entrepreneurs and business owners. Finally, the group I choose to call "The Communicators", is a group for professionals who use social media in their work in the public sector. The members hold positions as public information officers or other similar positions in the public sector, that use social media to communicate with the public. There are other groups on Facebook that were created to discuss GDPR. I have chosen not to include such groups, as they usually have no connection to specific professions. The aim of this study is to investigate how different professions discussed the effects of the new law. Using groups that focus on professions is thus more adequate. The professionals have sought membership in these groups to have a possibility to participate in discussions and to gain insight about subjects close to their professions. In these sense, social media is here considered a participatory culture (Fuchs 2017, p. 65).

Ethical implications must be discussed when dealing with discussions on the Internet. The persons taking part in the discussion behind the accounts need to be treated fairly. In the case of Facebook, most of the people in the discussions analyzed use their real names, making it necessary for anonymization of all used content. This has been done by changing the names of the groups. But there is also a need to anonymize the posts used in the analysis. To do this a special plug-in for the Chrome web browser was used to perform screen shots and anonymizing. The plug-in makes it possible to carry out the analysis without knowing the names of the people involved. The routines I have used comply with those that are generally used in research regarding social media (Fuchs 2017, p. 59). There are many different opinions regarding how to carry out research examinations of online forum content, in an ethical manner. There seem to be a paradigmatic shift that has moved concerns regarding ethical treatment of online content from being virtually none to a paradigm where online content is treated the same as any other personal information (Pickard 2013, p. 94f). One of the ethical

discussions that can be applied to how the online content is treated in this investigation is what is usually called "information obligation" or "informed consent" (Vetenskapsrådet 2002, p. 7). These aspects are usually applied to personal information used in an investigation, but all such information is anonymized here. What is interesting and also the focus of the study is the discourse – not the persons. No personal information has been compared – I have not traced Facebook profiles into other groups or other social media platforms. The research is focused on statements within a certain profession – not on the persons that express them. This investigation could be compared to an investigation where different "Letters to the editor" and similar written statements are used. But in those cases, both the names of the persons that have written the statements – and the platform where the statements have been published – are known to the reader.

Regarding my own participation in the groups used in this research: I am, and have been, a member of the groups used in the study. Initially for professional reasons, and during the study, of course, to gain insight. Without being a participant, I would not have had access to the content. No discussions I have participated in earlier have been used in this study.

Technically, what has been done to collect the empirical material (the threads), is to search in each group for GDPR. The searches were sorted chronologically. Then each thread has been downloaded using "Screenshots for Chrome", named chronologically (1, 2, 3 etcetera) and anonymized using the same plug-in. Only posts that mention GDPR were analyzed – not posts which start with a post about some other subject that later lead to a discussion about the GDPR. Although these kinds of posts appear in the type of searches described above, only posts where the thread starter's intention was to discuss GDPR were chosen. The posts were created between 2018-01-01 and 2018-06-13 an interval that thus constitutes the investigation period of the study. The GDPR was brought into force in Sweden on May the 25th, so most of the discussions about preparation for the implementation will naturally appear in 2018. 2018-06-13 is the date I started to collect the empirical material – it is also during the summer that a great deal of those employed in the public and private sectors start their summer vacation. All posts were named after their respective professional group (A - "The Archivists", P - "The Programmers", C - "The Communicators") and with a number starting with the post closest to the end date 2018-06-13 (A1, P33 et cetera). The other way around (with number 1 for the first post of 2018) would have been more convenient, but was impossible due to the lack of sorting possibilities in the Facebook search application.

First analysis: Examining the material and creating the categories

After all threads had been downloaded and anonymized the empirical material consists of 104 threads, 50 from "The Archivists", 31 from "The Programmers" and 23 from "The Communicators". When referring to a thread the number of the thread will be used together with the first letter of the profession (A1, P15, C22 et cetera). After reading each thread-start, several categories have been identified, and are presented in the sub-headings below. Some threads have been sorted into more than one category. The categories will be described in order to be used in further analysis. Some simple statistics is performed on each thread-type and category. This is done to give the researcher, and later, the readers of this paper, an insight into the number of posts in each discussion. The statistics are not a final goal for the study but rather a way of creating an understanding of the proportions of the discourse. These statistics have been calculated using a flat database file usually called a CSV or comma-separated-value-file. In this file the categories are columns and the threads are rows. To do calculations the "grep" command in the GNU/Linux Command line has been used. The full command to calculate the number of times one category has been used in each group is formulated as:

```
grep "A" raster.csv | grep "L" | wc -l
```

In the example above all "A" (threads from "The Archivists") in the file raster.csv are picked out. Subsequently all of these threads that contain "L" ("Links to external content") have been choosen through piping (with the command |). The number of rows is then counted ("wc -l" – word count – line). The result in this case is that 25 threads from "The Archivists" have been sorted into the category "Links to external content".

Links to external content (L)

Threads that have been categorized as "Links to external content" (37 threads in total) are threads that in the original (first) post contain a link to external content. External content is digital material outside Facebook that is linked into the platform from an external source. It could be news regarding the new law from the news media. It can also be invitations to courses regarding GDPR or statements and instructions from "The Swedish Data Protection Authority" (Datainspektionen). "The Swedish Data Protection

Authority" is the governmental agency that is responsible for instructions regarding the practical implementation and compliance to the GDPR.

Links to external content constitute 50% of the threads from "The Archivists" (25/50), a little less than 30% of "The Programmers" (9/31) and around 13% of the threads in "The Communicators" (3/23)

Direct questions (D)

A direct question, in this case, is when a person asks the group a question about the GDPR-implementation to the group. Why is this a specific category? Because a question in these professional contexts seems to have a little more thought behind it than just a posting of external content. The questions are often connected to administrative and technical problems an organization faces in the process of implementing the new law.

Direct questions are much more common in "The Programmers" (~67%, 21/31) and "The Communicators" (~78%, 18/23) than in "The Archivists" (22%, 11/50) even though it is hard to draw any direct conclusions from this. It might be related to how much work the new law demands of each profession. It might also relate to group culture – if direct questions regarding other problems are more common in the group in general.

Technical Solutions (T)

Technical solutions are posts in which technical solutions connected to the GDPR are discussed or presented. It can be a commercial product or a solutions that members of a group have constructed themselves.

The fact that discussions around different technical solutions are more common in "The Programmers"-group in which IT-professionals are active – is not that surprising. Around 26% (8/31) of the threads are about different technical solutions to GDPR-related problems. In "The Communicators" these posts consist of around 13% (3/23) of the number of threads, while no threads at all relate to technical solutions in "The Archivists".

Administrative Solutions (M)

Administrative solutions are very much alike the earlier category technical solutions, but this time more closely related to administrative work. The discussions might for instance deal with solutions regarding how to document consent of the use of personal data from a user of a service – a routine connected to the GDPR. Solutions regarding documentation prompted by the new law might also be discussed.

Administrative solutions are less discussed in "The Archivists" (4% or 2/50) and "The Programmers" (~6% or 2/31) and more common in "The Communicators" (~57% or 13/23).

What should we do about our... (W)
"What should we do about our..." is a category focused on direct questions regarding certain functions. "What should we do about the photos on our social media account?" is an example of a typical question. The category overlaps with "Direct question". It is also related to the category "Disaster!" below.

The category "What should we do about our..." is very uncommon in "The Archivists" (2%, 1/50) and quite uncommon in "The Programmers" (~6%, 2/31) and "The Communicators" (~22%, 5/23). In general, an existing but uncommon discussion in the three different groups.

Disaster! (I)
Sometimes the transition into a GDPR-ready organization is described in less favorable terms. I have used the category "Disaster!" for two kinds of subjects that have been identified in the material. Ideas that a business is ruined because of the new law as well as descriptions of the new law in media et cetera that are considered dangerous/disastrous. Sometimes these two kinds of threads are combined, such as when bad descriptions lead to views of an upcoming disaster.

The disaster-category is not common in any of the groups. In "The Archivists" it consists of eight out of fifty posts (16%), while "The Programmers" and "The Communicators" contain one post each (1/31 – ~3% and 1/23 ~4%).

Jokes et cetera about the GDPR (J)
The last category is jokes and other content of social character regarding the GDPR. Memes, advertisement with references to the new law and posts regarding social gatherings connected to the implementation are included in this category. Examples are photos of "GDPR-cakes" and photos from "GDPR-parties".

Jokes and social posts are much more common among "The Archivists" (12/50, 24%) than in "The Programmers" (2/31 ~6%) and "The Communicators" (3/23 ~13%). There is a possibility that the lack of this kind of content could be due to harder rules against off-topic posts in the two latter groups.

As mentioned earlier, categories can, of course be combined in the same post. Something can both be a joke and a serious question at the same time. We will now turn to the actual discussions in the quest for finding the online discourse of GDPR-discussion. In this second analysis, the categories constructed above will be used to analyze the posts users have created in each group.

Second analysis: The online discourse of the GDPR-discussion

In the second analysis the entryway in to the analysis will be through each group. In this analysis I will focus on the specific categories that are more common in each of the three Facebook groups. In the final part of the article I will focus on the difference between the three groups and discuss why these differences occur. But first a word on discourse – and what I choose to call online discourse. Online discourse, as a concept, is very close to what often is called public discourse. Public discourse, in relation to a subject such as the GDPR would be what media, the press, television, newspapers etcetera chose to discuss regarding that subject. Online discourse is similar but here we must add the possibilities of an online discussion (Sommer 2012, p. 2). An elemental description would be that online discourse is public discourse + the possibilities to discuss online. The main difference is that online discussions are more open and offer more opportunities of participation than the discussion in the public debate section of a newspaper, for instance.

"The Archivists"

In the group "The Archivists" I have found 50 posts with discussions threads related to the GDPR. The biggest category is "Links to external content" (25 posts). The linked content is mostly news related to the new law. This content is very seldom discussed. Most posts only get a few likes (~5), the most likes get a post (A33 – 156 likes), that I have cross-categorized to the category "Jokes" and it will be discussed under that category. I have chosen a few of the posts with more advanced and engaged discussions connected to linked content and will discuss them further. A4 is a discussion regarding posted content from the Swedish Data Protection Authority. It is a post with news regarding a legal dispute between the Swedish Data Protection Authority and the company Google regarding "the right to be forgotten". A right to be forgotten on the internet is part of the GDPR (Bartolini, et al 2016). The participants in the discussion do not agree on

whether this right is part of a positive development or not. One user explains that as a historian (s)he will never agree upon such a principle. Some users agree, while other users are of the opinion that the right to be forgotten is 1) only valid on the internet, 2) a right that is accepted in laws regulating some government archives already. In the end it seems like the participants agree to disagree.

A15 and A20 are two similar posts where posted links lead to a discussion. The reason that I describe them together is that both are posts from the same news site (svt.se) and that the discussions are about the problems two different municipalities think they will face when the GDPR is introduced. A15 is an interview with a politician on the municipal level. The politician is very worried about the new law and fears that public organizations will face numerous problems. That organizations, according to the politician's interpretation of the law will have to delete parts of their archives on request, is directly connected to the work of an archivist (Eiderbrant 2018). The interview was thus directly connected to the users of the group where the item is posted. A20 discusses the news about multiple changes that various municipalities believe they will face when the new law is introduced. Among other things it is believed that the municipalities will have to ban school photos and calculations are made regarding how much the implementation of the law will cost the municipalities (Grill Pettersson 2018). In both discussions the users are quite harsh and angry because in their view the people responsible (politicians et cetera) have not used the competence that exist within the organizations (archivists and others). This lack of use of in-house competence is seen as the reason for bad decisions.

Other linked content that leads to discussions are posts about how "the government wants to ban historical photographs" (A37), linked content from the Swedish Data Protection Authority (A39 – about the GDPR and the use of e-mail) and content from the Swedish government (A43 – about how the new law will be implemented). The discussion regarding the first link, about historical photographs, dies out fast when people discover that it is an article about regulations in Finland. The other discussions are rather short and mostly consist of various concerns that the users have regarding the practical implementation of the GDPR.

The second largest category is "Jokes" (13 posts). Jokes do not generate a lot of discussions, but they get a lot of user reactions (in the form of likes). The posts categorized as jokes get up to over 150 likes, which is a rather high rate for the group in general. The jokes vary a lot. One post (A5) is a link to a meditation application that reads part of the GDPR-law to help

you relax, implying that the text is very boring. Another is a picture (A7) of a well-known Swedish comical actor in one of his roles, a very annoying character. The text connected to the picture says "If the GDPR was a human" in Swedish. Another joke (A9) uses an ad from a Swedish beer brand. A new law is coming, and you must serve your friends beer as soon as you meet them – otherwise you will face expensive fines. The law is called "Ge Dig Pilsner Raskt" (Give You Beer Quickly). Other posts that I have categorized as jokes in a wider sense (social material) is a photo of a GDPR-cake (A10), a photo of a power-point slide with lots of names blurred out (A19) and a discussion regarding photos at a casino where an association of archivists had a meeting (A28). The discussion about the visit to the casino had potential to turn into a serious discussion but ended up discussing what types of drinks the members of the association had been served at the venue. The post with most likes is a short film made by two archivists that shows them throwing away a lot of archival matter (grades, documents about pensions et cetera) because they include personal data. The pun in the end is that you should not do that – archives in public administration are still ruled by the Swedish archive law and do not need to be destroyed because of the GDPR.

The next category is "Direct questions" (11 posts). These are posts where users describe direct problems they want to find a solution to. A1 is a thread where a problem of theoretical and legal nature seeks its solution. The user asks for help with finding the border between when a document is archived or not in a public administration as it is assumed that this will have an impact on rules connected to the GDPR. The other users are not sure if this really is the case, but agree that questions regarding the GDPR and archives are hard to answer and that the question should be forwarded to a public investigation regarding archives.

Post A38 is an interesting discussion emanating from a direct question. One user asks if anybody else remembers how a picture of a horse published by a newspaper, a couple of years earlier (about when a newspaper published a picture of a horse) had been considered a breach of privacy according to Sweden's previous personal data law. Yes, other users remember the story – but it was not about the old privacy law – they say instead it was a breach of press ethics. The user wants to use the story when educating other employees in his or her workplace about the GDPR. How it would be used is not discussed.

In one example, the direct question (like A26) is just answered by another user without further discussion. The question was asked how other

archivists have constructed the data inventory ("registerförteckning") of their archival collections. The first and only answer is a link to the Swedish Data Protection Agency website where at least parts of the question were answered. Four other users react to (like) the answer, indicating that it was a good answer to that question. Another short discussion is A27, where a user asks if there is any suitable way to make references to the GDPR in footnotes. The two users participating in the discussion are of the view that no suitable way to make such references exists. Several other posts (A31, A35, A40 among others) are quite short and start with a direct question and end with an answer to that question. The original questions are asked because the user needs the answer for his/her work and no further "intellectual" discussion is needed. The user just wants to be pointed towards a decent solution to a work-related problem.

"Disaster!" (8 posts) is the last category I will discuss in relation to this group. This category is based on original posts that foresee some kind of organizational disaster when the new law is implemented or regard the current situation as catastrophic. One post (A34) is about the situation for small businesses. According to a newspaper article, small businesses might face harsh fines when the new law is enforced. No users in the group react to this article and no one writes comments. The post seems to be outside of the focus of the group. A little more interesting, but also a bit outside of the group's focus is a post containing a British newspaper article from the Telegraph (A13). The article tells us that the British Data Protector Regulator's web page crashed just days before the implementation of the GDPR. This post leads only to two reactions (likes) from users. Two posts speak of the media not understanding the GDPR (A25), and that the poster does not understand the GDPR (A50). I have put these in the disaster-category because the undertone is stressed and angry. A25 is about the news misnaming the law a couple of days before it was implemented. A50 is posted by a user watching a webcast about the GDPR from the Swedish Association of Local Authorities and Regions. The user tells the group that (s)he now has reached "a higher state of confusion". There are some reactions (12 likes) and users with experience of the work of the Swedish Association of Local Authorities and Regions related to the GDPR agree that it is very confusing and that the association uses a lot of time on theoretical parts of the law, not explaining the consequences it will have.

The other categories ("Administrative solutions", "Technical solutions" and "What should we do about...") have very few categorized posts in this

group. I have chosen not to discuss these posts as these categories causes more discussions in the other two groups.

"The Programmers"

In the group "The Programmers" I have found 31 posts with connection to the GDPR. The posts have been categorized in the same way as the post from "The Archivists". I will now present my findings from the different categories.

The category that has the most posts is the one I name "Direct questions" and consists of examples of work-related questions about the new law. Twenty-one posts relate to that category. P1 starts like this "I am sorry to come to you with a question about the GDPR again...". The threadstarter is a user who needs instruction regarding how to take care of unstructured personal data generated by users of a company's web applications. This can be personal data stored in reviews, message applications et cetera that might be illegal to store due to the GDPR. A number of other users comment and add content to the thread. The general view is that it is impossible to comply with the new law with current work patterns and systems. Users do not solve the problem – instead they add other similar problems to the discussions ("What about e-mails?"). The two last comments in the thread contain an interjection ("this is madness!") and a joke ("We refer all personal information to Skynet" - a reference to an evil computer in the Terminator movies of the 1980s and 1990s. All in all, a discussion about a serious problem ends without any real answers.

Post P4, also categorized in "Direct questions", is about a dilemma the threadstarters have to deal with in relation to the new law. The user starting the thread has in his/her possession a hard drive with a large number of pictures taken during activities with an association that (s)he has been active in. Do these pictures have to be deleted when the GDPR becomes valid? And if so, how does this correspond to the Swedish Archival Act (Arkivlagen 1990:782)? No, other users answer, the archival act does not apply to associations – just to public organizations. Save it as a private person – not as an association – another user argues, citing parts of the GDPR that allow the private preservation of information. Yet another user argues in the same way later in the thread, and it seems like this advice is the most useful. Users in other parts of the thread deal with the possibility of preserving electronic information over long periods of time. Another question with a similar outcome is post P7. In this example a user asks if a company in Thailand would be bound by the GDPR if they process personal informa-

tion about the thread-starter who is a Swedish citizen. First, most of the other users who answer believe the poster to be confused – of course the company would not be bound by the GDPR. Or? Soon other users working in international companies in contact with the American and Chinese markets post privacy policies from companies that seem to regard the GDPR as applicable to their policies, although they are situated outside the European Union. Suddenly none of the users seem to know what a reasonable interpretation of the new law is. One user adds that: there will be a lot of lawsuits before the international use of this law is settled.

P8 is a more practical work-related question. One user asks the other members of the group if they have been asked to sign a Non-disclosure agreement for a customer. One user says that (s)he was asked to do this, and that the agreement was a whole pile of papers. The user had refused arguing that signing the agreement would need more legal support than the user had access to. "They have to trust my intentions" the user argued. The customer had solved the issue by separating the user from all personal data in the systems (s)he was working with. The user adds, later in the discussions, by posting that the agreements might be reasonable but that it makes him/her nervous to sign a vast amount of papers filled with "legal mumbo-jumbo".

Post P9 is not work-related as such, but has more of a customer perspective. One user asks other members of the group if they have requested personal data from companies they have a relation to. Some users have done this and share their experience of answers and of (quite often) being ignored. Most users are positive to making such requests – even though some of them might be on both sides – being customers and at the same time working in organizations that could be the recipients of such requests. One user has even constructed a web service to multiply requests and direct them to many different companies. But not everyone is pleased with the discussion regarding such requests. "Use your time more wisely" writes one user, claiming that such requests are a misuse of the rights given by the new law. A discussion follows but leads no further than to creating two sides; those that see all requests as necessary and relevant and those that see most of the requests as made by querulous persons.

It is always interesting when two professions clash over new and advanced rules. In post P17 one user writes that the legal adviser in the company (s)he works for claims that one of their developers working from Ukraine cannot have access to certain databases containing personal data. This leads to problems in the work place and to difficulties when an

employee cannot access certain parts of their resources. The users active in the thread claim that this interpretation of the law is wrong. That it all has to do with an agreement with potential customers. They need to be informed that the data will be accessed from locations outside the European Union. How the law should be interpreted is not discussed in any deeper sense – some links are posted but they do not entirely rule out either interpretation.

Nine links to external content have been identified in the material and I will describe some of the more relevant posts. One of the more active discussions is related to a (linked) episode of the Swedish news program "Rapport" (P3). The episode contains an interview regarding the GDPR with a person who is Chief of Information Security at a Swedish university. During the interview the person logs in to her computer and the camera is held in a way that makes it easy to see what is written on the keyboard – her password. Most of the discussion is regarding how stupid it is to reveal your password in such a way and that the person should be fired from her position as Chief of Information Security. Users see it as ironical that it was during an interview regarding the GDPR that this breach of information security appeared. There is also one user who finds that the university should be sued because according to the GDPR, the organization has a responsibility to work towards secure systems. This discussion is dropped quickly, however.

Post P18 is a link to a letter posted on ICANN.org (ICANN 2018). ICANN (Internet Corporation for Assigned Names and Numbers) is a foundation connected to the administration of the internet. Among other things it provides WHOIS, a protocol for metadata regarding websites that can be used to keep track of website owners. There is a concern that this service (which provides the names of owners among other data) could be considered illegal when the GDPR is implemented. According to the threadstarter, WHOIS can be used to prevent malicious activities on the internet (malware, spam et cetera). The discussion that follows focusses on two questions 1) do WHOIS really prevent malicious activities? 2) is WHOIS threatened by the GDPR? The first question is just answered by one user who holds the opinion that the service cannot be effective as a tool in preventing malicious activities. The data reported to the service has been too easy to forge. But in some cases, WHOIS has been effective, especially when servers have been infected by viruses and you need to contact the owner. The second question regarding whether the service is threatened seems to interest users more. Most of them believe that this is not the case.

By registering a website, you agree to the use of your personal data in the WHOIS-protocol. It would be very easy for those actors that sell web domains to refuse to sell to anyone that would not agree that their personal data would be used in WHOIS, the users argue.

Post P23 is a link to a Twitter-post that describes what kind of data Facebook saves regarding a user-account. The tweeter has requested all information from his/her account, a feature that was added during April 2017, the time the thread was first posted (Matsakis 2018). The discussion evolves around the part of the Facebook data that was considered more controversial during the time that the Facebook application saved information regarding text messages, calls made etcetera. This was considered problematic and related to the same kind of problems that the GDPR was meant to deal with. But the users involved in the discussion download their own information from Facebook and claim not to recognize the types of data mentioned in the Twitter-post or in contemporary media. Their data is much less controversial. According to one of the users, the more controversial data is just saved if the user gives his/her consent. The discussion challenges a more conspiratorial view of how large companies use personal data.

Finding technical solutions to problems is directly related to the work IT-professionals do. The amount of threads regarding technical solutions are thus slightly higher than in the other groups in this investigation (8 post). I will describe two of these posts and the discussions they lead to. The thread P5 starts with a post that describes a possible technical solution to the problem with vast amounts of personal data. The first poster gives the suggestion that organization could encrypt e-mails or user-names using a hash function that would make them possible to identify by a server without being visible as personal data. This could be used if a person asked to be forgotten by a company letting earlier transactions (orders et cetera) still be connected to the earlier account. The solution is not accepted by other users. "This is not anonymizing – it is pseudo-anonymizing" is one of the arguments. Another user describes an analogy to the solution in this way: "Imagine that I have a box of papers which I am supposed to destroy – but instead of destroying them I just hide the box. This is what you do in your suggestion." Other users point out that pseudo-anonymizing is not accepted according to the GDPR. Information that is supposed to be destroyed must be impossible to recreate.

P14 is a post regarding how to technically hinder personal data from being saved to a company server without given documented consent. This post is treated in the same way as P5 above. Especially other users point out

that the GDPR will not affect the possibility of using personal information when this information is needed for a business transaction. Thus, registering for a service or buying a product will not be problematic from the perspective of the GDPR. It will be problematic only if the personal information is preserved against the customer's will or used in a way not included in the original agreement, the user claim.

Four of the categories, "What should we do" (4 posts), "Administrative solutions" (2 posts), "Jokes" (2 posts) and "Disaster" (1 post) have too few posts to form the basis of a more advanced analysis.

In general, the discussions in "The Programmers"-group are longer and more advanced than in "The Archivists". There are many possible reasons for this. "The Programmers" has around 14 000 members while "The Archivists" has around 1500 members and a larger cohort of users could produce more potential participants in a discussion. Another factor could be that most jobs in the sector that "The Programmers" represent are connected to the private sector where the GDPR seems to have a greater impact than in the public sector, where members in "The Archivists" usually work. If this is a reason why users in "The Programmers" group discuss more, then discussions might be driven by work-related stress. This might explain why serious work-related problems are met by uncertain answers and jokes (as in P1, above).

"The Communicators"

In the group "The Communicators" I have found 23 posts connected to the GDPR. I will analyze these posts in the same fashion as the other groups, starting with the category which had the largest amount of posts. As was the case, in "The Programmers" group the category "Direct questions" gathered the largest amount of questions. With some overlaps the category has 18 posts. We will return in the concluding analysis to reasons why posts in this category have been so common in two of the groups.

The first "Direct question", C2, is a post where the user asks other users for possibilities to solve the problem of documenting a person's consent to having his/her name/picture and the like published on websites. No real solutions are presented – but some users claim that they have a solution such as a standardized e-mail they send which includes a link to an online contract. Others claim that the best way to solve consent is to connect the preserving of personal data to another law that overrides the GDPR. The discussion ends without the original poster getting any real solutions to his/her problem, just very vague descriptions of what could be done. C5 is a

very similar discussion concerning consent to pictures and recordings published on the social media application Instagram. In this case one of the users claims to have a solution, namely that registered persons can give consent by using their BankID application. BankID is a Swedish application for secure electronic signatures. Other users seem to be satisfied with this solution. C6 contains a similar question and was posted on the 15th of May, just ten days before the GDPR was brought to force in Sweden. The poster, who works with social media for a university in Sweden, is worried about their social media accounts. Will they need to be cleansed from personal data? The answers given are affected by the late awakening of this organization. "Yes", most of the users answer. "No", some of them answer, not if the personal data is part of editorial content ("redaktionellt material"). It seems as if the users have been given very different answers to some of these questions by their legal advisers, in courses on the GDPR et cetera. This causes many different interpretations and quite a lot of confusion.

Posts C13 and C15 are questions connected to the use of APSIS email solutions. APSIS is a company that provides services for marketing by e-mail (APSIS 2018). A service used by some municipalities in Sweden. With the GDPR the lists that contained the metadata about the e-mail recipients became problematic as they constituted personal data. Discussions in these threads were about the function responsible for the personal data (APSIS or the municipalities) and how any changes should be made regarding the collected e-mails. Most of the contributors to the thread restarted their use of the APSIS e-mail-lists. They contacted all recipients and asked for their consent to store their personal data with the purpose of sending them e-mails with information they might need. As it seems, some of them lost recipients in this process. External content from APSIS contained advice on how to reverse the loss, which was, as it seems, a general problem for many organizations and businesses (Chase 2018).

Another direct question discussed images of models bought from image agencies (C22). The general question is about which function has the responsibility to document the models' consent regarding the picture of them. Some of the users claim that it is included in the activity of being a photo model to consent to having your picture taken and spread. Others claim that this is the responsibility of the image agencies. The discussion contains no clear answers, from a legal perspective, regarding responsibility; but the thread is quite interesting from other perspectives. Firstly, it is interesting how the GDPR causes such confusion. Image agencies and their customers are part of a marketing industry that would potentially lose a

large amount of resources if old pictures with unknown models were considered illegal to use because of the new law. If the customers had to keep a register of persons included in all pictures they use, this would be problematic as it would demand more administration. The second question brought up by one user (gaining some feedback in likes from other users) regarding if this "hysteria" concerning consequences of the GDPR is reacted to in equal manners in other member states of the European Union. The user believes that this might be something typically Swedish, to implement directives from the European Union in a very rigid way, causing problems for citizens and companies. Unfortunately, this very interesting turn in the discussion is not elaborated on further.

Administrative solutions are the second largest category of topics discussed in the "The Communicators" group (13 posts). C3 is one of these discussions. The original poster asks if it will be possible to remove "postlistor" (lists of mail and e-mail sent to an organization) with reference to the GDPR. Other users have difficulty understanding what the original poster wants. Some of them do not understand what kind of list the poster refers to since a "postlista" can take on different meanings in Swedish public administration. Some of them do not understand if the original poster wants it removed from a website or removed generally from the organization where the person works. The poster does not specify his/her original question, but the discussants suggest possible versions of the question. First, some of them propose, there is no legal obligation to post "postlista" on a public organizations website. This is something that an organization chooses to do. If it becomes a problem in relation to the GDPR, the list can be removed or modified in a way that makes it comply with the new law, the users argue. Secondly, the original poster seems to want to use the new law to ban something that (s)he wants to be banned for some other reason. This is not seen as entirely appropriate by the users in the discussion.

Post C10 has been classified as pertaining to both the categories of Administrative solutions and Technical solutions. C10 contains a discussion about how to delete personal data on request from a person, when this data is stored in a location that the organization does not have complete control over. One example is Facebook, where a page-owner (an organization) may delete comments et cetera made by a person on the page. The problem is that in doing this, the page-owner has no real knowledge regarding whether the information is deleted everywhere on the servers of Facebook. Is this problematic in relation to the new law? It seems like every user that participate in the discussion agree about the initial problem: there is no possibility to erase

comments or other personal data from a Facebook-page and be 100% sure that it is not still stored somewhere else on the servers of Facebook. What the users do not agree on is whether this is really a problem for the page-owner/organization or not. There are references to upcoming discussions between the European Union and Facebook and ideas about how the situation might change so that these technical problems might not be an issue in the future. It is furthermore discussed whether a restriction created by the European Union could affect a service distributed by a company outside of the union (similar to that in P7, discussed above). This is not a question any of the participants in the discussion can answer, however.

Four of the categories "What should we do about our..." (5 posts), "Links to external content" (3 posts), "Jokes" (3 posts) and "Disaster" (1 post) had so few active discussions, or so many overlaps with other categories, that they were considered not relevant to analyze further.

Altogether, the Facebook groups of the three professions analysed here demonstrate quite a lot of confusion regarding the implementation of the GDPR in Sweden. Nobody seems to be completely sure of what they should do when the new law comes into force. And if they think they know they are quite often in disagreement. I will continue to analyse this in the upcoming concluding analysis

Concluding analysis

To sum up, the discussions the users from three different professions are involved in contain many questions and a lot of confusion. What we need to remember is that the groups consist of users that are working in professions that are affected by the GDPR in various ways. The new law might considerably change part of their work, and it will affect their work duties.

The discussions in the three groups show somewhat different patterns. This might be due to the difference in their professions, but also due to group rules et cetera. "The Programmers" and "The Communicators" seem to share more traits with each other than either of them do with "The Archivists". "The Programmers" and "The Communicators" have more direct questions – where user asks questions with direct significance for their work – than "The Archivists" where "Direct questions" is only the third biggest category. "The Archivists", on the other hand, have more jokes regarding the GDPR and external links connected to the new legislation than "The Programmers" and "The Communicators". If the difference in direct questions concerning work is connected to the different professions it

might reflect that the professions of "The Programmers" (programmers, system administrators and others employed in the IT-sector) and "The Communicators" (Public information officers and others working with social media in the Public sector) are more involved in the implementation of the GDPR than the profession of archivists which "The Archivists" represent. Of course, this is impossible to prove using this method, but if we look at the types of post being made in the different groups, there are differences that could reflect the level of professional involvement.

In general, there are very few positive voices about the implementation of the GDPR in the analysed material. The majority of the voices are neutral, signaling that "this is my job – I will have to accept this" or negative and arguing for instance that "this is impossible to implement!". The only area where one group of professionals seems to be rather enthusiastic is the IT-professionals in "The Programmers" group regarding the possibilities of requesting information from different companies where the IT-professionals themselves have been customers (P9). One user has even constructed a web service to make it possible to send bulk questions to several companies. But not all discussants are pleased – some of the users in "The Programmers" seem to be of the opinion that only the querulous request information without any other reasons than it being legal. A similar discussion is present in "The Archivists" about the "right to be forgotten" (A4). Some users believe that this should be a right. But one user, a historian, argues that this possibility would be a catastrophe. The other users argue that it is not such a big deal since few individuals would use it, and similar rights already exists on the internet.

There are some concerns about how various services that the professions are working with will be affected by the GDPR. The analysis has shown that most of these concerns were exaggerated. Regarding some services – like WHOIS (P18) – the personal information that might not be publishable in the end seemed, by most of the discussants, to be of no real use anyway. As for the discussion regarding pictures from image agencies (C3), initial concerns that the images would no longer be possible to use seemed in the end to demand less changes than was initially believed. A similar example is presented in post A33 where archivists joke about the concerns of having to throw away a lot of important documents (grades et cetera) because they include personal information.

Concerns might be more common, but some solutions are also presented in the material. Especially in "The Communicators" group discussions regarding technical solutions are found. Two discussions about consent

through the BankID-application (C2, C6), which some municipalities have implemented or are going to implement. Other users are very interested in finding out more about this solution. Two other discussions about technical solution concern the e-mail-list service APSIS. Here, actual changes to routines would have to be made in the users' organizations. Some of these routines might solve their problems, but they would also imply a higher workload.

The analysis has also identified a tendency to voice prejudices against other professions. Legal advisers not being able to understand the new law is one example, visible in post P17. It might have been interesting to investigate discussion group where different legal professions discuss GDPR (if such group exists) to see how questions are discussed in such surroundings. One problem I have identified in the groups that was included in this investigation is that users, not being professionals in legal interpretation can seem quite alone and excluded in their search for lawfulness. Better communications between different professions might be a way to relieve people from stress when an implementation process is at hand. Still in P7 a user shows quite good insight in the confusions of the lawmen – the user states that there will be a lot of court-cases before we know how the new law works. Two other professions that are treated with less respect are politicians (in A15 and A20) and an information security officer at an university (P3) that unfortunately shows a password in national television.

All in all, the analysis shows that the discussion among the information and communication professionals of the analysed groups show proof of uncertainty. If the Facebook-groups are regarded as zones where professionals can speak in a more truthful manner than in their ordinary work, then this might indicate that implementation of the GDPR required more resources. But because of our lack of knowledge of the users, identities we cannot be sure of this. The users might be professionals in a position where they are isolated from the staff that perform the GDPR-preparations, thus having no real insight. It is clear, though, that some of them actually do have quite a good insight. It might be this, together with confusion, that is the distinguishing feature of the online discourse of the General Data Protection Regulation. Confusion and a very varying level of insight. And serious problems with no obvious answers.

Bibliography

APSIS (2018) "Vi är APSIS", https://apsis.se/om-oss/om-oss (viewed online 2018-09-11)

Bailey, J. (2018). "Data Protection in UK Library and Information Services: Are we ready for GDPR". Legal Information Management (18).

Bartolini, C. and Siry, L. (2016). "The right to be forgotten in the light of the consent of the data subject" Computer Law & Security Review. Vol 32.

Bihari, E. (2018). "GDPR – A Y2K-II for business" EDPACS: 57:2

Bui, J. (2017). "Data brokers facing the new GDPR – A legal analysis of the GDPR on the processing of personal data by data brokers" Master Thesis in Law, Oslo University.

Chase, S. (2018). "GDPR-bakfylla? 5 strategier för att vinna tillbaka dina prenumeranter" https://www.apsis.se/blogg/gdpr-5-strategier-vinn-tillbaka-prenumeranter (viewed online 2018-09-11)

Childs, J. T. and Starcher S. C. (2015). "Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management". Computers in Human Behavior. Vol 54.

Cionea, I., Piercy, C. W. and Carpenter, C. J. (2017). "A profile of arguing behaviors on Facebook". Computers in Human behavior. Vol 76.

Cornock, M. (2018). "How the writers of case reports need to consider and address consent and GDPR?" Case Reports in Women's Health. Accepted Manuscript.

Eiderbrant, A. (2018). "Kaos att vänta när nya dataskyddslagen börjar gälla" https://www.svt.se/nyheter/lokalt/stockholm/kommunpolitiker-kaos-att-vanta-nar-nya-dataskyddslagen-borjar-galla (viewed online 2018-08-18)

Facebook (2018) "Group Admin Basics" https://en-gb.facebook.com/help/418065968237061/ (viewed online 2018-08-11)

Fuchs, C. (2017). "Social Media – A critical introduction" London: Sage Publications

Grill Pettersson, M. (2018). "Miljonkostnader, heltidstjänster och artificiell intelligens – men inget förbud för skolfoto med GDPR" https://www.svt.se/nyheter/inrikes/miljonkostnader-heltidstjanster-och-artificiell-intelligens-men-inget-forbud-for-skolfoto-med-gdpr (viewed online 2018-08-18)

Hicks, M. (2010). "Facebook Tips: What's the Difference between a Facebook Page and Group?" https://www.facebook.com/notes/facebook/facebook-tips-whats-the-difference-between-a-facebook-page-and-group/324706977130/ (viewed online 2018-08-11).

ICANN (2018). "Letter from Jelink to Marby". https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf (viewed online 2018-09-06)

Kascak, O., Pupala, B. & Mbugua, T. (2016). "Slovak Preschool Curriculum Reform and Teachers' Emotions: An Analysis of Facebook Posts". *Early Childhood Education Journal*. 44:573–580.

Lag 2018:218 med kompletterande bestämmelser till EU:s dataskyddsförordning.

Manasijević, D., Zivković, D, Arsić, S and Milosević, I (2016). "Exploring students' purposes of usage and educational usage of Facebook", Computers in Human behavior. Vol. 60.

Matsakis, L. (2018). "How to download your Facebook data and what to look for in it", Wired Business. https://www.wired.com/story/download-facebook-data-how-to-read/ (viewed online 2018-09-06)

McCall, B. (2018). "What does the GDPR mean to the medical community?" The Lancet, Vol 391.

Müller, P., Schneiders, P. and Schäfer, S. (2016). "Appetizer or main dish? Explaining the use of Facebook news posts as a substitute for other news sources" Computers in Human behavior. Vol. 65.

Pickard, A. (2013). "Research methods in information", London: Facet Publishing.

Robertson, B. W. and Kee, K. F. (2016) "Social media at work: The roles of job satisfaction, employment status, and Facebook use with co-workers". *Computers in Human behavior*. Vol. 70.

Sommer, V. (2012). "The Online discourse on the Demjanjuk trial. New memory practices on the World Wide Web". *Essachess – Journal for Communication Studies*. Vol. 5 (no. 2).

Voigt, P. and von dem Bussche, A. (2017). "The EU General Data Protection Regulation (GDPR) – A Practical Guide". Cham: Springer Verlag.

Vetenskapsrådet (2002) "Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning"

Facebook-threads from the three anonymized groups were started between 2018-01-01 and 2018-06-13.

Anonymized versions of the threads in .PNG-format are kept in the authors possession.

Chrome web browser plugin used to anonymize users in threads:
"Screenshots for Facebook" by Didrik Nordström

https://chrome.google.com/webstore/detail/screenshots-for-facebook/onahgdjaaijinoflbmnbpfpolmfmeklg [Downloaded 2018-06-13]

Contributors

GORDON ANTHONY is Professor of Public Law at Queen's University, Belfast. He teaches and researches almost exclusively in the field of judicial review, and is the co-author (with Peter Leyland) of *Textbook on Administrative Law* (Oxford University Press, 2016, 8th ed). He is Director of the Academy of European Public Law in Athens, Greece, and a member of the Executive Committee of the UK Constitutional Law Association.

DR. NASREDDINE BOUSMAHA is a Professor of Law at the university of Oran 2 – Algeria. He is currently the Director of the research laboratory "Law, Society and Power". His prominent publications include a book entitled « The Rights of the Victims of International Crimes in International Law", also "Commentary on the Rome Statute of the International Criminal Court". He has written several articles on the themes of international law and constitutional law. He teaches Master and Ph.D. students at the university of Oran 2 (Public international law – international organizations – international responsibility).

Doctor of Laws, WILLIAM GILLES is a tenured associate professor (HDR) at the Sorbonne Law School (University Paris 1 Pantheon-Sorbonne) where he is the director of the Master's degree in Digital Law, and the director of the Chair of the Americas. He is the cofounder and President of IMODEV. He is a former member of the board of the Sorbonne Law School, and a former member of the Academic Board of the University Paris 1 Panthéon-Sorbonne, where he served on the Research Council of the University. William Gilles is also attorney at Law at Paris Bar, and professional mediator accredited by the French National Center for Mediation by Attorneys at Law. He is founder and President of BeRecht Avocats. William Gilles is a former lawyer at the French Constitutional council (2009-2011). He received several awards (2016 1st Prize of the Foundation Jacques Descours Desacres, delivered by the French Senate, 2014 SMBG Prize Trophée de la pédagogie). Between 2014 and 2016, he was heard three times by the French Senate on Governmental Transparency, open data, and digital legal issues. Since 2015, he is one of the two Open Government Partnership (OGP) IRM Researchers for France. He is the director of the *International Journal of Open Government*, and of the *International Journal of Digital and Data Law*.

His research focuses on open government issues (open data, government transparency, citizen participation, government accountability), digital law issues (right to privacy, cybercrime, fundamental rights in the digital society), eGovernement, smart cities, but also mediation and collaborative lawyering that he considers as a need for an open justice.

PATRICIA JONASON, Associate Professor in Public Law, School of Social Sciences, Södertörn University. Patricia Jonason teaches Administrative and Constitutional law as well as Comparative Law and Human Rights. Her current research interests are mainly linked to privacy and the right of access to information, the difficulties in striking a balance between the two and their relationship to democracy and the Rule of Law. A large part of her research is comparative and/or contains an analysis of the process of Europeanisation with imbues Public Law.

MICHAEL GØTZE is a Professor of Administrative Law and his research sheds light on good administration, rule of law and transparency issues. He is the director of Center for Legal Studies in Welfare and Market (WELMA) focusing on digital welfare state

MARIA LINDH, Senior Lecturer at the Swedish School of Library and Information Science, University of Borås. Her research interests are related to the intersection of information management, organisational studies and social studies of information technologies. In her doctoral thesis – Cloudy talks – Exploring accounts about Cloud Computing (2017) – she discusses the legitimation of cloud services. A common conception of information technologies and related services is that they are neutral utilities. To the contrary, her perspective is that information technology is intertwined with the social and therefore has essential social implications.

RIKARD FRIBERG VON SYDOW, Archival scientist and doctor in ethics, is Senior Lecturer at the School of Historical and Contemporary Studies, Södertörn University. He is coordinator of the subject of Archival Science at Södertörn University his research includes the analysis of the historical development of medical records, internet and internet culture, and communication within public administration.