



<http://www.diva-portal.org>

## Postprint

This is the accepted version of a paper published in *The Computer Law and Security Report*. This paper has been peer-reviewed but does not include the final publisher proof-corrections or journal pagination.

Citation for the original published paper (version of record):

Naarttijärvi, M. (2018)

Balancing data protection and privacy: The case of information security sensor systems

*The Computer Law and Security Report*

<https://doi.org/10.1016/j.clsr.2018.04.006>

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

Permanent link to this version:

<http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-148079>

## **Balancing data protection and privacy – the case of information security sensor systems**

*Markus Naarttijärvi\**

*Department of Law, Umeå University, Umeå, Sweden*

### **ABSTRACT**

This article analyses government deployment of information security sensor systems from primarily a European human rights perspective. Sensor systems are designed to detect attacks against information networks by analysing network traffic and comparing this traffic to known attack-vectors, suspicious traffic profiles or content, while also recording attacks and providing information for the prevention of future attacks. The article examines how these sensor systems may be one way of ensuring the necessary protection of personal data stored in government IT-systems, helping governments fulfil positive obligations with regards to data protection under the European Convention on Human Rights (ECHR), the EU Charter of Fundamental Rights (The Charter), as well as data protection and IT-security requirements established in EU-secondary law. It concludes that the implementation of sensor systems illustrates the need to balance data protection against the negative privacy obligations of the state under the ECHR and the Charter and the accompanying need to ensure that surveillance of communications and associated metadata reach established principles of legality and proportionality. The article highlights the difficulty in balancing these positive and negative obligations, makes recommendations on the scope of such sensor systems and the legal safeguards surrounding them to ensure compliance with European human rights law and concludes that there is a risk of privatized policymaking in this field barring further guidance in EU-secondary law or case law.

© 2018 Markus Naarttijärvi. Published by Elsevier Ltd. All rights reserved.

*Keywords:* Data protection, privacy, information security, sensor systems, communications monitoring, metadata

## **1 INTRODUCTION**

Maintaining information security in the face of antagonistic security threats is no easy task. While it is difficult to estimate the number and scope of attacks against information systems and associated data breaches – as all breaches might not be detected and those that are may not necessarily be reported – numbers from security companies seem to suggest an increase in the frequency of data breaches with a slight reduction in the number of records exposed over the last three years.<sup>1</sup> In any case, countering the threat to information systems from antagonistic actors is

---

\* LL.D., Senior lecturer, Department of Law, Samhällsvetarhuset, Plan 5, Umeå universitet 901 87 Umeå, Sweden.

Email address: markus.naarttijarvi@umu.se

<sup>1</sup> Internet Society, 'Global Internet Report 2016' (Internet Society 2016)

<<https://www.internetsociety.org/globalinternetreport/2016/>> accessed 19 January 2018; Gemalto, 'Breach

increasingly highlighted as a priority for the European Union,<sup>2</sup> as well as governments in many states around Europe.<sup>3</sup> A recent industry survey by PwC further suggest that a top information security priority for the public sector is adopting continuous monitoring of technical controls and further use of monitoring systems and security intelligence.<sup>4</sup>

One such type of monitoring system will be analysed in this article; the implementation of information security sensor systems in government information architecture.

The term 'information security sensor systems' is used here to describe network monitoring tools which detect attacks (including attempted breaches) against network servers by analysing traffic and comparing this traffic to known attack-vectors, traffic profiles or content, while also recording attacks and thus providing information to sensor databases for the prevention of future attacks. It is not a term that necessarily connotes a specific type of equipment or configurations of such measures as this may depend on the context where it is deployed or the manufacturer of the technology. Instead it refers to technologies, processes and other measures that may include or be described as 'Security Information and Event Management tools (SIEM)',<sup>5</sup> 'New-Generation Cybersecurity Monitoring and Management Systems',<sup>6</sup> 'Network filters',<sup>7</sup> or 'proactive cooperative defense'.<sup>8</sup> Generally speaking though, the type of sensor system discussed here operate by monitoring the attributes of connections to information systems. This includes, for example, the originating IP-address or e-mail address, the requested resources, and may include the content of e-mails and other communications to and from information systems to enable the real-time or retrospective identification of potential malicious code, phishing attempts or DDoS attacks. A more detailed explanation and concrete examples of their function and use is given in section 2 below.

There are several reasons why government implementation of such systems is different from that of private enterprises. Signatory states to the European Convention on Human Rights ('ECHR', 'the Convention') as well as member states of the European Union subject to the EU Charter of Fundamental Rights ('the Charter') are required to uphold the fundamental rights enshrined in those legal instruments. As such, they are legally precluded from monitoring private communications if doing so would violate their obligation to protect privacy under art. 8 of the Convention or art. 7 or 8 of the Charter. On the other hand, a growing doctrine of positive obligations in relation to those same human rights instruments illustrate how states also have a responsibility to take effective measures to protect the privacy of individuals under their

---

Level Index - First Half 2016' (Gemalto 2016) <<http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf>> accessed 19 January 2018.

<sup>2</sup> European Commission, 'Cybersecurity Strategy of The European Union' (European Union 2013).

<sup>3</sup> E.g. Swedish Government Official Reports, 'Informations- och cybersäkerhet i Sverige: Strategi och åtgärder för säker information i staten (SOU 2015:23)' (Swedish Government 2015); Premier Ministre, 'French National Digital Security Strategy' (French Government 2015); .BE, 'Cyber Security Strategy of Belgium' (Belgian Government 2012); Department of Communications, Energy and Natural Resources, 'Irish National Cyber Security Strategy 2015-2017' (Irish Government 2015).

<sup>4</sup> 'Industry Findings: Public Sector' (PwC, 2017)

<<https://web.archive.org/web/20170405225152/http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/public-sector-industry.html>> accessed 19 January 2018.

<sup>5</sup> Kavanagh, Kelly M., Oliver Rochford, and Toby Bussa. 'Magic quadrant for security information and event management' *Gartner, Tech. Rep.* (2015).

<sup>6</sup> Igor Vitalévich Kotenko and Igor Borisovich Saenko, 'Creating New-Generation Cybersecurity Monitoring and Management Systems' (2014) 84 *Herald of the Russian Academy of Sciences*.

<sup>7</sup> Lech J Janczewski, Douglas Reamer and Juergen Brendel, 'Handling Distributed Denial-Of-Service Attacks' (2001) 6 *Information Security Technical Report*.

<sup>8</sup> Hakem Beitollahi and Geert Deconinck, 'Analyzing Well-Known Countermeasures Against Distributed Denial of Service Attacks' (2012) 35 *Computer Communications*.

jurisdiction, if feasible.<sup>9</sup> Consequently, states are obliged by human rights instruments to both act and to refrain from acting, in ways that private actors are not. Meanwhile, the EU General Data Protection Regulation ('GDPR') further highlights the responsibilities of data processors, including government agencies, to implement suitable security measures to prevent unauthorised access to – or disclosure of – personal data.<sup>10</sup>

Also of note is that government agencies in EU member states may also be operators of essential services as defined under the EU NIS-directive.<sup>11</sup> In such cases, they are under a further obligation to report information security incidents to national Computer Emergency Response Teams (CERT:s).<sup>12</sup> The aim of this reporting obligation is to allow national CERT:s to estimate the cross border effects of a security incident within the essential services.<sup>13</sup> Here, monitoring of traffic data may assist both the operators of essential services and the national CERT to estimate the effects of a security incident, while also providing actionable information to prevent such incidents in other systems. However, the role played by monitoring of traffic data by sensor systems has not been without controversy in the run-up to the implementation of notification requirements, as illustrated by a 2011 survey among regulatory agencies conducted by the *European Union Agency for Network and Information Security* (ENISA):

*“Monitoring of traffic data proved to be a contentious issue among regulatory authorities. Out of the regulatory authorities surveyed by ENISA, 41% responded positively when asked if they thought data traffic should be monitored in order to discover data breaches. Those who responded positively, however, indicated that such monitoring should be conducted under strict legal conditions. In other words, the purpose of the monitoring should be clearly defined and relevant authorities should oversee the process. One regulator further suggested that the proportion of data monitored should be restricted only to the data required for the discovery of the data breach.”<sup>14</sup>*

The difficulties involved in balancing security and privacy interests in this context can be illustrated by a recent initiative to implement sensor systems among Swedish government agencies information systems. There, an initial implementation proposal was subject to severe criticism by consultation bodies as it allegedly failed to properly analyse and consider the impact on privacy of communications and the processing of personal data.<sup>15</sup> However, a subsequent revised plan still suggested authorizing the Swedish Civil Contingency Agency to install sensor systems within government agencies through a government ordinance, which would provide a wide mandate of network monitoring.<sup>16</sup>

While the balancing of interests involved may be described as one between security and privacy, which is a familiar tune in the legal debates of later years, it may also be seen in a different light. Given that the information stored in the databases of government agencies to a

---

<sup>9</sup> See section 3 below.

<sup>10</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

<sup>11</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

<sup>12</sup> Ibid. article 1.

<sup>13</sup> Ibid. article 14.

<sup>14</sup> European Network and Information Security Agency, 'Data Breach Notification in The European Union' (ENISA 2011) <<https://www.enisa.europa.eu/publications/dbn>> accessed 19 January 2018.

<sup>15</sup> Justitiedepartementet, 'Tillhandahållandet av Tekniska Sensorsystem - Ett Sätt Att Förbättra Samhällets Informationssäkerhet' (Swedish Government 2017), p. 2-3.

<sup>16</sup> Ibid.

large extent is personal data relating to individual citizens, a loss of such data impacts not only the security of government information systems but privacy of individuals as well. As such, the balance that needs to be struck is also, as previously noted, one between the positive obligations of the state to protect citizens' data on the one hand, and on the other the negative obligation of the state to respect citizens' and public employees' privacy by limiting surveillance of communication systems to what is lawful, necessary and proportional. In other words, fulfilling positive obligations within the legal limits of the fundamental right to privacy. This article will approach the issue of sensor systems from primarily this fundamental rights perspective, but as we will see, there is considerable overlap between the fundamental rights layer and the more detailed data protection rules on a European level.

To describe in terms that are more concrete the type of security measure in question, the implementation of information security sensor systems currently proposed by the Swedish government to secure information systems run by public authorities providing essential services in Sweden will be used.<sup>17</sup> This implementation is chosen as the proposed system illustrates the implicit legal issues and as it is subject to a relatively concrete and detailed description in Swedish preparatory works thus allowing legal analysis and interpretation without access to privileged information. This example serves only as a point of departure for a wider discussion. As such, the legal analysis and conclusions will focus on the European context of privacy and data protection law and is not dependent on the Swedish context or specific implementation; instead, it is likely to apply equally to similar systems in other jurisdictions within the European Union.

The proposed sensor system will be described in section 2 in closer detail. In section 3, the positive obligations of the state stemming from both EU law and the ECHR will be analysed as they extend to information security and data protection, to clarify the potential legal drivers of implementing such systems and to what extent they can be regarded as a way to ensure compliance with European law. In section 4 the focus will turn to the rules and principles in the ECHR and EU law relating to the protection against monitoring of electronic communication of citizens or government employees, or that places restrictions on the processing of personal data in such systems. In other words, legal interests on the European level that may restrict the implementation of sensor systems in certain ways. Finally, in section 5, some conclusions are drawn relating to the balancing of privacy and data protection in this context, certain issues are highlighted, and recommendations are made.

## **2 Information security sensor systems**

### **2.1 Outlining an information security sensor system**

The proposed implementation of the Swedish sensor system ('the Proposal') describes a system which in scope and complexity is located in-between simpler commercial systems intended for a specific network and the more advanced cybersecurity sensor systems provided by the Swedish signals intelligence agency to government information systems relating to national security. The new sensor system is intended to be offered to both public and private entities providing essential

---

<sup>17</sup> See generally Justitiedepartementet, 'Tillhandahållandet av tekniska sensorsystem - Ett sätt att förbättra samhällets informationssäkerhet' (Swedish Government 2017).

services,<sup>18</sup> but whose systems are not deemed vital for national security as those would be covered by the system provided by the signals intelligence agency instead.<sup>19</sup>

The system will be provided by The Swedish Civil Contingencies Agency, which is also the designated Swedish national Computer Emergency Response Team ('CERT'). This is a civil agency tasked with civil protection, public safety, emergency management and civil defence as long as no other authority has responsibility. Their responsibility include measures taken before, during and after an emergency or crisis. The Swedish Civil Contingencies Agency has no law enforcement tasks but may assist in the coordination of law enforcement and other agencies in the context of emergencies or crises.<sup>20</sup>

The proposed system consists of five parts: i) a record, ii) detection sensors, iii) alarms, iv) an alarm database, and v) traffic flow sensors and databases.<sup>21</sup>

- i) *The record* consists of information which helps detect attacks, such as previously identified malicious IP-addresses, malicious code, e-mail addresses or other personally identifiable information connected to previous attacks known to the CERT.<sup>22</sup>
- ii) *The detection sensors* are provided by the CERT and are placed outside of the government agency firewall. They search through all incoming and outgoing network traffic looking for, e.g. phishing attacks or attempted network breaches through web traffic. If suspicious traffic is found the CERT and the network owner is notified by the sensors. At this stage, a recording of a few minutes of the suspected traffic is also possible when it is not clear if the alarm is false or not or if further information is necessary to evaluate the incident. This recording may include the sending and receiving IP-addresses, timestamp, traffic size and the content of communications if the suspicious traffic involves e-mail. Since the recording takes place outside of the firewall, where the sensors are deployed, internal communication within the authority is not included. The gathered traffic information is forwarded to the alarm database at the CERT where analysts perform evaluation of recordings.<sup>23</sup>
- iii) *The alarms* sent from the sensors to the CERT includes information about the discovered threat, such as code snippets, time-stamp, receiving and sending IP-address. This data is then stored in the alarm database.<sup>24</sup>
- iv) *The alarm database* at the CERT will store alarms sent to the CERT from every authority where sensor systems have been deployed, along with network recordings connected to each alarm. The CERT decides on the further use of the data in the alarm database and the security surrounding it. The content of the

---

<sup>18</sup> This type of service is defined in section 2 of the Civil Contingency Agency regulation (2016:7) as a service that meets at least one of the following conditions: 1) Where a loss of, or a serious disturbance in the service can, on its own or together with corresponding events in other services, lead to a serious crisis in society. 2) The service is necessary or very essential for managing an already occurred crisis in society so as to minimize harmful effects. Examples of social sectors with important social functions are energy supply, financial services and security.

<sup>19</sup> Justitiedepartementet, 'Tillhandahållandet av tekniska sensorsystem - Ett sätt att förbättra samhällets informationssäkerhet' (Swedish Government 2017) p. 11–13.

<sup>20</sup> Förordning (government regulation) (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

<sup>21</sup> Justitiedepartementet, 'Tillhandahållandet av tekniska sensorsystem - Ett sätt att förbättra samhällets informationssäkerhet' (Swedish Government 2017), pp. 5–7.

<sup>22</sup> Ibid. p. 6.

<sup>23</sup> Ibid. p. 6–7.

<sup>24</sup> Ibid. p. 7–8.

database is used to provide knowledge and information to authorities to assist in countering current and future network attacks.<sup>25</sup>

- v) In *the traffic flow sensors* network traffic is continuously collected and sent to *the traffic flow database*. This includes network traffic not flagged by the detection sensors. This information is used to retrospectively search for attacks not flagged by the detection sensors. This data only includes meta-data such as IP-addresses, data sizes and timestamps but no e-mail content. The traffic flow database allows the CERT to identify attacks in earlier traffic based on information not available in the detection sensors at the time. This is helpful to counter so called Advanced Persistent Threats (APT) where a network intrusion or exploit is not detected until long after it began.<sup>26</sup>

While this example of a sensor system might in certain details, such as the size and scope of the traffic flow database or the information recorded by the sensors vary from other similar systems, the key components of records, sensors, alarms and databases are likely to be similar given the intended functions of sensor systems as such. The main legal issues are also likely to be similar, namely the generalized (though automated) monitoring and storing of communications data. As such, the proposed sensor system will here serve as a functioning point of departure for a legal analysis of public sector sensor systems as such.

## 2.2 Legislative rationales underpinning implementation

The proposal to implement the previously described sensor system in Sweden must be understood in light of severe criticisms that has previously been levelled against the information security of Swedish government entities. In three consecutive reports from 2007 to 2016, The Swedish National Audit Office (SNAO) found serious deficiencies in the information security of the audited government agencies.<sup>27</sup> In the most recent 2016 report, the SNAO concluded, “information security at the agencies audited is at a level that falls considerably short of being adequate”.<sup>28</sup> While the SNAO attributed significant responsibility for these deficiencies on organisational cultures within the agencies, which failed to understand or prioritize information security, some responsibility was also placed at the lack of cross-agency coordination and support from the government, leading the SNAO to recommend a centralized government function for operative support to agencies.<sup>29</sup>

Parallel to this criticism, a government expert inquiry published in 2015 highlighted the lack of sensor systems in Swedish government information infrastructures, while pointing to the existence of such systems in the other Nordic countries. This implied the inquiry found, that many serious IT incidents went undiscovered or was not discovered in time. The establishment of such systems would however warrant further legal analysis of the necessary processing of personal data implied, and the potential need for further secrecy rules to exempt such systems from the

---

<sup>25</sup> Ibid. p. 8.

<sup>26</sup> Ibid. p. 8–9.

<sup>27</sup> Swedish National Audit Office, 'Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen – RiR 2007:10' (Riksrevisionsverket 2007); Swedish National Audit Office, 'Informationssäkerheten i den civila statsförvaltningen – RiR 2014:23' (Riksrevisionsverket 2014); Swedish National Audit Office, 'Informationssäkerhetsarbete vid nio myndigheter - RiR 2016:8' (Riksrevisionsverket 2016).

<sup>28</sup> Swedish National Audit Office, 'Informationssäkerhetsarbete vid nio myndigheter - RiR 2016:8' (Riksrevisionsverket 2016), p. 6.

<sup>29</sup> Ibid. p. 7–9.

principle of public access to government records.<sup>30</sup> The expert inquiry was a response to the upcoming requirements of the NIS-directive,<sup>31</sup> and the need for sensor systems was framed in the context of the need for a national situational awareness and a proposed incident notification requirement following from the directive.<sup>32</sup>

As such, while it is likely that the NIS-directive has been a driver of implementation of the Swedish sensor system, it is one that must be seen in the light of already established weaknesses in the legislative and institutional framework surrounding government information security.

### 2.3 Domestic criticism

While the importance of information security in government IT-systems is largely uncontested, the suggested legal implementation of the earlier described sensor system in Sweden was subject to substantial criticism in the consultation process that followed the proposal.<sup>33</sup> This criticism serve to highlight some of the implicit legal issues surrounding sensor systems. As noted by the Swedish Data Protection Authority, the sensor system could imply a limitation of privacy that would be subject to the constitutional requirement of parliamentary statute in the Swedish instrument of government. As such, it was questionable that the legislative basis of the proposed system was intended to be a government regulation rather than statutory law.<sup>34</sup> Furthermore, the proposed system's compatibility with, *inter alia*, the purpose limitation requirement and the responsibility to inform data subjects provided by the EU Data Protection Directive<sup>35</sup> and its Swedish implementation was questioned by, among others, the Swedish Data Protection Authority,<sup>36</sup> the Swedish Bar Association,<sup>37</sup> and the Swedish National Courts Administration.<sup>38</sup> From a different perspective, the Swedish Union of Journalists questioned the analysis of e-mail content given the constitutional protection of journalistic sources.<sup>39</sup> Finally, from a technical standpoint, the Swedish Prosecution Authority questioned the usability of the system given that the sensors would be placed outside of the government agencies firewalls and presumably without access to the agencies encryption keys. As most communication to and from government agency networks was now encrypted, the Prosecution Authority deemed it unlikely that the sensor system would be able to analyse the traffic as intended.<sup>40</sup> Worth noting, however is that several other

---

<sup>30</sup> Swedish Government Official Reports, 'Informations- och cybersäkerhet i Sverige: Strategi och åtgärder för säker information i staten (SOU 2015:23)' (Swedish Government 2015), p. 250–251.

<sup>31</sup> Directive (EU) 2016/1148.

<sup>32</sup> Swedish Government Official Reports, 'Informations- och cybersäkerhet i Sverige: Strategi och åtgärder för säker information i staten (SOU 2015:23)' (Swedish Government 2015), p. 250, 259–261.

<sup>33</sup> This process, where Swedish government agencies and other relevant organisations are asked to comment on legislative proposals is well established in the Swedish legislative process.

<sup>34</sup> Datainspektionen, 'Remiss av promemorian Tillhandahållande av tekniska sensorsystem – Ett sätt att förbättra samhällets informationssäkerhet' (Datainspektionen 2017).

<sup>35</sup> Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data' (1995).

<sup>36</sup> Datainspektionen, 'Remiss av promemorian Tillhandahållande av tekniska sensorsystem – Ett sätt att förbättra samhällets informationssäkerhet' (Datainspektionen 2017).

<sup>37</sup> Sveriges advokatsamfund, 'R-2017/0444' (Sveriges advokatsamfund 2017).

<sup>38</sup> Domstolsverket, 'Remissyttrande över promemorian Tillhandahållande av tekniska sensorsystem – Ett sätt att förbättra samhällets informationssäkerhet' (Domstolsverket 2017).

<sup>39</sup> Svenska Journalistförbundet, 'Promemorian Tillhandahållande av tekniska sensorsystem – Ett sätt att förbättra samhällets informationssäkerhet' (Svenska journalistförbundet 2017).

<sup>40</sup> Åklagarmyndigheten, 'Yttrande över promemorian Tillhandahållande av tekniska sensorsystem - Ett sätt att förbättra samhällets informationssäkerhet' (Åklagarmyndigheten 2017).

consulted agencies either left no comments or left generally positive comments about the proposed sensor system.

## 2.4 Sensor systems and law enforcement

While the deployment of the proposed sensor system was not as such tied to the investigation or prevention of crimes, but rather to maintain information security, there are certain implicit connections between the two. An attempted breach of, or antagonistic attack on a government network is in many states, including Sweden, a criminal act. Consequently, the sensor system will contain information pertaining to possible criminal activity. There is thus *prima facie* a law enforcement relevance and potential to the information collected by a sensor system such as the one proposed. This connection becomes more apparent through another proposed Swedish government regulation that will require the Civil Contingencies Agency (who will deploy and monitor the sensor systems as the national CERT) to forward any incidents reported to them that could have their basis in a criminal act to the police.<sup>41</sup> This would in effect have the potential of turning the sensor system into an indirect proactive law enforcement interception system. Currently, the Civil Contingencies Agency is only obliged to *encourage* those public agencies reporting incidents with a potential basis in a criminal act to report them to the police.<sup>42</sup> This is in line with the requirements of the NIS-directive establishing that when incidents are suspected to be related to serious criminal activities under national or Union law member states should encourage operators of essential services to report such incidents to the relevant law enforcement authorities.<sup>43</sup> However, so far not a single report has actually been filed with the police since information security incident notifications to the Civil Contingencies Agency were made mandatory in Sweden. The Civil Contingencies Agency also made it clear that it had no intention of voluntarily reporting incidents to the police. This position was based on the concern that such reporting might undermine the willingness of public agencies to report incidents to the agency, or make reports less detailed as technical details surrounding information architecture or security measures would be at risk of becoming exposed in a criminal inquiry or court case.<sup>44</sup> As Swedish government authorities enjoy a certain constitutionally enforced independence from the executive government in their day-to-day operations, this led the government to propose a requirement through government regulation instead.<sup>45</sup>

The resulting requirement on the Civil Contingencies Agency to report incidents to the police would be tied to incident notifications received from public authorities and not the proposed sensor system as such. However, given that the sensor system would be one key source of information relating to incidents based on criminal acts, the information collected by the sensor system could directly or indirectly be subject to the requirement to report incidents to the police.

---

<sup>41</sup> Department of Justice, 'Polisens tillgång till information om vissa IT-incidenter (DS 2016:22)' (Swedish Government 2016).

<sup>42</sup> Swedish government regulation (2015:1052), § 20, 'Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap'.

<sup>43</sup> Recital 62 NIS-directive.

<sup>44</sup> Department of Justice, 'Polisens tillgång till information om vissa IT-incidenter (DS 2016:22)' (Swedish Government 2016), p. 112.

<sup>45</sup> The constitutional rule in chapter 12, section 2 of the Swedish Instrument of Government (1974:152) prohibits the government (including individual ministers) from interfering in individual decisions or the exercise of public power by public agencies. Government control of its agencies is instead supposed to take place primarily through appointment of agency heads, budget-steering and laws and regulations, see Derlén, Mattias, Johan Lindholm & Markus Naarttijärvi, *Konstitutionell rätt* (1st edn, Wolters Kluwer 2016), p. 236.

### 3 Positive obligations and data protection under European law

#### 3.1 Introduction

As illustrated above, the deployment of sensor system is described as a way of maintaining information security in the face of increasing antagonistic threats. This is of course closely linked to both the security of IT-systems as such, as lacking IT-security will endanger information stored in them as well. A lack of information security further implies deficiencies in data protection. In light of this, it is worth posing the question if, and to what extent, sensor systems may be a necessary part of ensuring the protection of personal data stored in public information systems. A further question is to what extent such measures are a necessary part of reaching the positive obligations implied by data protection as a fundamental right. To arrive there, the concept of positive obligations in relation to data protection must first be analysed.

#### 3.2 Positive obligations as a concept of human rights law

The doctrine of positive obligations is most commonly associated with the ECHR. However, it represents at its core the idea that ‘states have responsibilities to safeguard certain individual rights from interference by other private parties, who’s casual relation to the violation complained of requires an effective response from the state’.<sup>46</sup> While data protection rules in Europe developed independently from the ECHR and its growing doctrine of positive obligations,<sup>47</sup> and the fundamental right to data protection in the Charter was established after the development of substantive secondary law protection of personal data, they are conceptually similar. Data protection rules establish the necessary legal framework to protect individuals against violations of privacy and data protection by other private parties (as well as public bodies). As such, they may be regarded as a more concrete expression of the positive obligations of the state in relation to privacy and data protection. The close connection between positive obligations and the protection of ‘private life’ as a conceptual holistic centre of the ECHR has been acknowledged,<sup>48</sup> indeed the first cases establishing the positive obligations of the state under the convention concerned article 8 of the ECHR.<sup>49</sup>

#### 3.3 Information security as a positive obligation of the state under the ECHR

While most of the case law on data protection issues is concerned with either the initial storing of personal data by contracting states,<sup>50</sup> or by the subsequent disclosure of such data to third parties,<sup>51</sup> there are cases implying a positive obligation to ensure an adequate level of information security as well.

In the case of *I v. Finland*, the ECtHR made the role of information security for maintaining the protection of private life under the ECHR explicit. The case concerned the

---

<sup>46</sup> Dimitris Xenos, *The Positive Obligations of the State under the European Convention of Human Rights* (1st edn, Routledge 2013), p. 22.

<sup>47</sup> E.g. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, which entered into force in 1985.

<sup>48</sup> Dimitris Xenos, *The Positive Obligations of the State under the European Convention of Human Rights* (1st edn, Routledge 2013), p. 12-13.

<sup>49</sup> See *Marckx v Belgium* (6833/74) [Plenary] (1979) HUDOC; *Airey v Ireland* (6289/73) (1979) HUDOC; *X and Y v the Netherlands* (8978/80) (1985) HUDOC. See also Dimitris Xenos, *The Positive Obligations of the State under the European Convention of Human Rights* (1st edn, Routledge 2013), p. 22-27.

<sup>50</sup> E.g. *S and Marper v the United Kingdom* (30562/04; 30566/04) [GC] (2008) Reports of Judgments and Decisions.

<sup>51</sup> E.g. *Peck v the United Kingdom* (44647/98) (2003) Reports of Judgments and Decisions 2003-I.

protection of information about the applicant's HIV-positive status in a hospital's patient files. The applicant, who worked at a hospital where she was also a patient, became suspicious of unauthorized access to her medical file when colleagues alluded to her HIV-positive status. The ECtHR approached the case as a matter of whether the state-owned hospital had failed to guarantee the security of her data from unauthorised access, or as the ECtHR restated the issue in Convention terms; if there had been "a breach of the State's positive obligation to secure respect for her private life by means of a system of data protection rules and safeguards".<sup>52</sup> As the hospital had not limited access to patient medical files to only relevant staff, nor maintained a log of all persons who had accessed the applicant's medical file, the ECtHR found it had failed to ensure adequate security against unauthorised access.<sup>53</sup>

Importantly, while positive obligations under the ECHR primarily entail a responsibility to provide a legal framework and procedures whereby individuals may either secure their rights against encroachments by other individuals,<sup>54</sup> or possibilities to claim compensation from parties responsible for violations,<sup>55</sup> the ECtHR held in *I v. Finland* that this was not sufficient in this context. Instead, the Court noted that:

*"the mere fact that the domestic legislation provided the applicant with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place".*<sup>56</sup>

In the case, The ECtHR reviewed the existing data protection arrangements in light of domestic law, which in turn was an implementation of the EU Data Protection Directive. Essentially, the standard applied by the Court boiled down to whether the state had taken necessary technical and organisational measures to protect the sensitive data in question. As such, the Court did not have to elaborate on the status under the ECHR of the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.<sup>57</sup> The link between this convention and article 8 of the ECHR had already been acknowledged by the ECtHR in the earlier case of *Z v. Finland*, a case that also related to the disclosure of sensitive health information although within the context of a judicial procedure.<sup>58</sup> It is also worth noting the similarities of Convention 108 and the EU data protection regime, where the CoE convention has formed a basis for both the EU Data Protection Directive and article 8 of the Charter.<sup>59</sup>

While the possible conclusions of the two Finnish cases must be tempered by the sensitivity of the medical data they deal with,<sup>60</sup> the implication of these cases is that a failure by

<sup>52</sup> *I v Finland* (20511/03) (2008) HUDOC, § 37.

<sup>53</sup> *Ibid.* §§ 44–46.

<sup>54</sup> *Söderman v. Sweden* (5786/08) (2013) HUDOC §§ 80-84; *KU v. Finland* (2872/02) (2008) HUDOC §§ 45-49; *X and Y v. the Netherlands*, (1985), Series A no. 91, § 27.

<sup>55</sup> *Söderman v. Sweden* (5786/08) (2013) HUDOC § 85.

<sup>56</sup> *I v Finland* (20511/03) (2008) HUDOC, §§ 47.

<sup>57</sup> ETS No. 108.

<sup>58</sup> *Z v Finland* (22009/93) (1997) Reports 1997-I, § 95. See also Herke Kranenborg, 'Article 8 – Protection of Personal Data', *The EU Charter of Fundamental Rights – A Commentary* (1st edn, Hart Publishing 2014), p. 228.

<sup>59</sup> European Union, 'Explanations Relating to The Charter of Fundamental Rights of the European Union (2007/C 303/02)' (2007); see also Herke Kranenborg, 'Article 8 – Protection of Personal Data', *The EU Charter of Fundamental Rights – A Commentary* (1st edn, Hart Publishing 2014), p. 229.

<sup>60</sup> Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of The EU* (1st edn, Springer International Publishing 2014), p. 101.

the state to uphold a suitable level of information security when storing sensitive personal data may imply a violation of the positive obligations flowing from the rights of the data subject under article 8 of the ECHR.

The boundaries of this positive obligation are however drawn by the reasonable and the possible. For example, the ECtHR has held that preventing individuals from receiving sexual spam e-mail did not fall under the positive obligation of the state given the inherent difficulty of combating this issue on a systematic level, combined with the possibility for individuals to filter such e-mail themselves.<sup>61</sup> Relevant factors in deciding the extent of positive obligations in this context are consequently whether positive action from the state is reasonable following a balancing against opposing values and if the passivity of the state has actually resulted in the violation of a right by a private party.

Within the scope of EU-law, the protection of personal data under the ECHR may have become secondary to the stand-alone right to protection of personal data under the EU-Charter of Fundamental Rights (the Charter).<sup>62</sup> Still, it is important to note that the positive obligations of the state in relation to data protection from a human rights perspective predate the Charter and is relevant beyond the scope of EU-law.

### 3.4 Charter of Fundamental Rights: Data protection constitutionalized

The establishment of data protection as a fundamental right of the European Union through article 8 of the Charter solidified the status of data protection as a fundamental right in Europe. While it is clear from the explanations of the Charter that article 8 was intended to reaffirm a right that already existed in EU-law,<sup>63</sup> the nature of that right *as independent from privacy* before the Charter had been questioned.<sup>64</sup> As such, codifying data protection as an independent right at a European constitutional level was a significant recognition of its importance and positions data protection principles, to a certain extent, beyond the reach of politics barring significant future reforms of EU primary law.

The fact that the right to data protection under article 8 of the Charter affirms previously existing EU-law principles makes it rather difficult to assess the scope of the Charter provision independent of the data protection principles established in secondary law and the case law of the CJEU. For example, both Convention 108 and the Data Protection Directive, which forms a basis for article 8 of the Charter, includes explicit mentions of security measures surrounding the processing of personal data.<sup>65</sup> The Charter, including the explanations, do not however explicitly mention security. It is however likely that reasonable technical and organisational measures are included in the general wording 'right to the protection of personal data' in article 8.1, and

---

<sup>61</sup> *Muscio v. Italy*, (31358/03) (2007) HUDOC.

<sup>62</sup> See Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] Judgment of the Court (Grand Chamber) of 9 November 2010, ECLI:EU:C:2010:662; Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] Judgment of the Court (Third Chamber) of 24 November 2011, ECLI:EU:C:2011:771. See also Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer International Publishing 2014), p. 236-237.

<sup>63</sup> Praesidium of the European Convention, 'Explanations Relating to The Charter of Fundamental Rights (2007/C 303/02)' (2007).

<sup>64</sup> Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer International Publishing 2014), p. 206.

<sup>65</sup> Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (1981), art. 7; Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data' (1995), recital 46 & art. 17.

through the references to the Data Protection Directive. However, given the lack of CJEU case law relating explicitly to the issue of technical and organisational measures, the exact scope of those principles as a fundamental right under EU-law is still somewhat uncertain.

What is less uncertain is the implicit positive obligations that stem from the Charter. To the extent that a right to security of data is included in the scope of protection of article 8 of the Charter, and again – it is likely so, this implies positive obligations for member states to ensure the practical protection of this right.<sup>66</sup> Under EU-law, there is however generally less need to elaborate on the positive obligations stemming from the Charter in relation to data protection given that the applicability of the Charter is practically synonymous with the applicability of the secondary EU-law on data protection as read in the light of the Charter provisions.<sup>67</sup> Indeed, the natural habitats of positive obligations as a concept are those human rights instruments where active measures must be read as implicit in the negative obligations included in the convention text to ensure that individuals may effectively enjoy the rights in question. In contrast, under EU-law positive obligations are less problematic as active responsibilities for both public and private parties can be elaborated in secondary law. Still, it is worth noting that EU secondary law read in conjunction with the charter may be regarded as largely synonymous with the positive obligations of member states (and the EU) in relation to data protection as a fundamental right within the EU.

The relationship between the upcoming GDPR and the Charter is however more uncertain insofar as the GDPR expands on the rights of the data subject compared to the Data Protection Directive, as the directive but not the GDPR forms a basis for the Charter provision.

### **3.5 GDPR – technical and organisational safeguards of personal data**

The primary source of union law obligations relating to security of personal data has long been the Data Protection Directive. As this directive is superseded by the GDPR the data protection requirements in the union is further harmonised and expanded in terms of the responsibilities of data processors. In relation to security of data, the technical and organisational measures to secure such data are put forth with further emphasis in the regulation and connected to more stringent enforcement mechanisms.<sup>68</sup>

While it is difficult to specify the exact level of technical and organisational measures required by the GDPR, as this depends on the available technology and the risk for data subjects of the data processed, recital 78 of the GDPR provides a few examples. Among them are measures such as pseudonymising data, data minimisation and transparency of processing. Given the focus on data protection over IT-security, it is perhaps not surprising that the GDPR does not mention or refer to monitoring or sensor systems. The issue of whether such measures may be part of technical and organisational measures under the GDPR must instead be determined by analysing the best practices within the industry and the risk for the data subjects involved. Provided such technical solutions are established as part of an industry standard or certification guidelines they may become a factor in determining whether the technical and organisational measures under the GDPR have been met as well.<sup>69</sup>

---

<sup>66</sup> See Mistale Taylor, 'The EU's Human Rights Obligations in Relation to its Data Protection Laws with Extraterritorial Effect' (2015) 5 International Data Privacy Law, p. 252-253.

<sup>67</sup> See Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2017] Judgment of the Court (Grand Chamber) of 21 December 2016, ECLI:EU:C:2016:970, p. 122-125.

<sup>68</sup> See Art. 83(4) GDPR, allowing for fines of up to EUR 10,000,000.00 or 2% of total worldwide annual turnover for failures of meeting the technical and organizational measures requirement.

<sup>69</sup> See recital 77 GDPR in this regard.

### 3.6 NIS-directive – From security of data to security of systems and networks

In July 2016, the *NIS-directive*<sup>70</sup> was adopted by the European Parliament and the Council. It is to be implemented by member states by May 2018, thus aligning itself temporally with the entry into force of the GDPR. The purpose of the directive is to improve the functioning of the inner market by achieving a high common level of security of network and information systems within the EU.<sup>71</sup> It establishes a number of organisational and strategic responsibilities of member states, such as the adoption of national strategies and the establishment of national competent authorities, single point of contacts and Computer Security Incident Response Teams (CSIRTs).<sup>72</sup> The directive also imposes security requirements on operators of essential services, including risk management measures to “identify any risk of incidents, to prevent, detect and handle incidents and to mitigate their impact”.<sup>73</sup>

The NIS-directive applies to operators of essential services as well as digital service providers. In this context, it is the operators of essential services that are most likely to be government entities. The directive lists a number of sectors in annex II including energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution and digital infrastructure. Entities within these sectors who fulfil three criteria identified in Article 5(2) of the directive operate ‘essential services’ within the meaning of the directive. The criteria are; (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service. It is however possible for member states to supplement this list according to recital 22 of the directive.

The protection required by the GDPR is interconnected with the protections mandated under the NIS-directive, as a high level of IT-security is necessary to maintain a high level of data protection.<sup>74</sup> There is also a considerable overlap in the terminology used in the NIS-directive and the GDPR. For example, under Art. 14(1), the directive places a responsibility on Member States to ensure that

*“[...] operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.”*

Under article 14(2) Member States should also ensure that operators of essential services; *“take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.”*

Through article 14(3) the directive further requires that Member States establish notification requirements on operators of essential services, to provide the national CERT or

---

<sup>70</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

<sup>71</sup> See article 1.1 NIS-directive.

<sup>72</sup> See article 1.2 NIS-directive.

<sup>73</sup> Recital 46 NIS-directive.

<sup>74</sup> Voigt, Paul & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) – A Practical Guide* (1st edn, Springer International Publishing 2017), p. 42.

Computer Security Incident Response Team ('CSIRT') with information in order for them to determine any cross-border impact of the incident.

While these operators of essential services may be government agencies in certain cases, certain further responsibilities of member states beyond the legislative responsibility to enact binding rules of such operators are put forth in Article 9 and Annex I of the directive, which relates to the establishment, requirements and tasks of CSIRTs. The CSIRTs should cover at least the sectors identified by annex II of the directive as well as digital services such as online marketplaces, search engines and cloud computing services as defined in Annex III of the directive, but their role extends beyond this. They are to be responsible for both risk and incident handling,<sup>75</sup> which, among other things, implies a responsibility of all procedures supporting the detection, analysis and containment of an incident (having an actual adverse effect on the security of network and information systems) and the response thereto.<sup>76</sup> Together with the requirements in Annex I of the directive of *inter alia* 'monitoring incidents at a national level', 'providing dynamic risk and incident analysis and situational awareness' and 'responding to incidents', this implies an operative and active role for CSIRTs, acting as a potential driver for the adoption of sensor systems.

As mentioned in the outset of this article, the issue of monitoring of communications as part of such measures has been contentious within ENISA – the EU organisation tasked to advise Member States on the application of the NIS-directive.<sup>77</sup> ENISA does include the implementation of SIEM tools, which are broadly speaking similar to the proposed sensor systems in function though not in scope, as a security measure on “sophistication level 2” (of 3) in its technical guideline for implementation of minimum security measures for Digital Service Providers.<sup>78</sup> In practice, it is likely that ENISA does consider retention and monitoring tools a key aspect of the requirements under the NIS-directive. In the ENISA report on gaps in standardisation of Member States responses to the NIS-directive, the agency describes data retention and auditing as well as real-time data availability to provide data for forensic analysis as a focus of the NIS-directive.<sup>79</sup> Furthermore, the monitoring and defence of information systems is described as a required part of essential service providers' responsibilities under the NIS-directive. In an earlier report, ENISA encouraged “data-consuming” CERTs, i.e. those not providing data helping other CERTs, but rather consuming data, to deploy sensor networks to allow them to verify external threat data and improve detection rate. The report did however note the privacy invasive nature of sensors that monitor production level traffic or use existing network device infrastructure, and points to less intrusive means such as honeypots as an alternative sensor possibility.<sup>80</sup>

---

<sup>75</sup> Article 9, NIS-directive.

<sup>76</sup> Article 4(8).

<sup>77</sup> See section 1 above.

<sup>78</sup> European Network and Information Security Agency, Technical Guidelines for the implementation of minimum security measures for Digital Service Providers' (ENISA 2016) <<https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers>> accessed 19 January 2018. The wording in Art. 14 of the NIS-directive on the responsibility of operators of essential services to take appropriate and proportionate technological measures is similar to that of Art. 16 referring to digital service providers. However, unlike in Art. 14, the security measures mentioned in Art. 16(1)(d) specifically includes “monitoring, auditing and testing”.

<sup>79</sup> European Network and Information Security Agency, 'Gaps in NIS standardisation Recommendations for improving NIS in EU standardisation policy' (ENISA 2016) <<https://www.enisa.europa.eu/publications/gaps-eu-standardisation>> accessed 19 January 2019.

<sup>80</sup> European Network and Information Security Agency, 'Proactive detection of network security incidents' (ENISA 2011) <<https://www.enisa.europa.eu/publications/proactive-detection-report>> accessed 19 January 2018. p. 138.

Importantly, the NIS-directive, as well as the ENISA standards are explicitly tied to a wider set of security standardisation taking place through standardisation bodies such as ISO and ETSI. As the NIS-directive explains in recital 66, standardisation of security requirements is a market-driven process. While industry standards as well as ENISA reports cannot be regarded as sources of law applicable to a positive responsibility under the NIS-directive, they become relevant through the reference to technical and organisational measures in the NIS-directive. This has the effect of essentially outsourcing the normative definition of legal responsibilities to sector agencies such as ENISA and standardisation bodies such as ISO and ETSI. It is worth noting that this also outsources, and to a degree privatizes, the normative drivers of installing potentially privacy invasive technologies in public information systems. The final recital of the directive states that the directive respects fundamental rights and the principles recognised by the Charter, “in particular the right to respect for private life and communications [...]”.<sup>81</sup> The directive should, the recital further states, be implemented in accordance with those rights and principles.<sup>82</sup> However, it is worth noting that the level of interference with this right to private communications will in the end be subject to a market driven process, which may be less mindful of such fundamental rights and principles.

## **4 Negative obligations and privacy of communications under European law**

### **4.1 The relationship between positive and negative obligations**

The positive obligations discussed above do not exist in a vacuum but are rather measures that exist within the legal limits established by the obligation not to violate fundamental rights. As the ECtHR has found, the positive obligation of the state must be understood as operating within the boundaries of the state’s negative obligations.<sup>83</sup> While the interests underpinning positive obligations can be balanced against and thus affect the scope of negative obligations,<sup>84</sup> positive obligations are not free passes to disregard the primary negative responsibilities flowing from fundamental rights. As such, in a context where positive obligations can be located in EU directives and regulations, those obligations must thus be construed in harmony with obligations established in EU primary law such as the Charter, and the rights under the European Convention on Human Rights as fundamental principles of EU law. Where on the other hand positive obligations flow from the Charter or the Convention as such, they must instead be balanced against the negative obligation not to interfere with fundamental rights following from those same instruments. Understanding these negative obligations thus helps us interpret the extent and limits of EU secondary law in this area.

## **4.2 ECHR**

### **4.2.1 Applicability of the ECHR on the proposed sensor systems**

The negative obligations under article 8 of the ECHR must be analysed from the viewpoint of the three distinct types of possible interferences with fundamental rights that sensor systems imply. First, there is the monitoring of communications as such which implies an interference with the

---

<sup>81</sup> Recital 75 NIS-directive.

<sup>82</sup> Ibid.

<sup>83</sup> See *Osman v. the United Kingdom* (23452/94) (1998) HUDOC, § 116; *K.U. v. Finland* (2872/02) (2008) HUDOC, § 49.

<sup>84</sup> See *K.U. v. Finland* (2872/02) (2008) HUDOC, § 49.

right to respect for private life and correspondence of individuals contacting the public agencies where sensor systems are deployed or visiting their websites. Second is the connected issue of the right to respect for private life and correspondence of the employees of those same public agencies as they communicate with people outside of the agency where they work. Third, it is the interference with private life implied by the storing of network traffic and associated personal data in the alarm database and the traffic flow database.

As a point of departure, it is worth noting that the ECtHR has held that:

*In establishing the right of “everyone” to respect for his “correspondence”, Article 8 of the Convention protects the confidentiality of “private communications” [...] whatever the content of the correspondence concerned [...] and whatever form it may take. This means that what Article 8 protects is the confidentiality of all the exchanges in which individuals may engage for the purposes of communication.*<sup>85</sup>

As the proposed sensor systems would be installed in information systems belonging to public agencies, it is unquestionable that the state is responsible for any potential interferences with article 8 they imply. It is worth noting that the outsourcing of this task (or information security related tasks relating to public information systems in general) to private entities, or the installation of government sensor systems within the information systems of private entities would not preclude the applicability of the ECHR. The ECtHR has consistently held that the delegation of tasks to private entities does not absolve the state from responsibility *ratione personae*.<sup>86</sup>

The requirement in article 8(2) that any interference must have a legitimate aim does not present a problem for the proposed sensor system. The state may reasonably claim that it is implemented in the interest of national security, public safety, economic well-being of the country, prevention of disorder or crime as well as for the protection of the rights and freedoms of others, thus checking off almost every interest enumerated in article 8(2). The issue at hand will instead be whether the proposed sensor system is ‘in accordance with the law’ and ‘necessary in a democratic society’; the other two requirements following from article 8(2).

#### **4.2.2 General requirements relating to the interception of communications**

The proposed sensor systems will primarily monitor metadata, information such as the originating and destination IP-addresses. However, as the systems will process – through automated means – all incoming traffic, and specifically monitor the content of e-mail traffic and to a certain extent retain this content if flagged by alarms and recorded, the ECtHR case-law relating to interception of communications content will become applicable as well. This brings with it a stricter standard of legality and proportionality. Perhaps unsurprisingly, the case law on interception of content is primarily developed in relation to law enforcement or intelligence interception. As such, the standard applied by the ECtHR is difficult to apply directly in the context of information security sensor systems. It may however still give an indication as to the necessary detail of any statutory regime allowing for monitoring of communications content.

---

<sup>85</sup> *Michaud v. France* (12323/11) (2012) HUDOC, p. 90 [internal citations omitted], with reference to *Frerot v. France* (70204/01) (2007) HUDOC, p. 53-54.

<sup>86</sup> *Wos v. Poland* (22860/02) (2006) HUDOC, p. 51-54; *Sychev v. Ukraine* (4773/02) (2005) HUDOC, p. 53; *Costello-Roberts v. The United Kingdom* (13134/87) (1993) HUDOC, p. 25-28.

The minimum safeguards that should be set out in law, as currently articulated by the ECtHR in relation to telephone communication include:

- 1) the nature of offences which may give rise to an interception order;
- 2) a definition of the categories of people liable to have their telephones tapped;
- 3) a limit on the duration of telephone tapping;
- 4) the procedure to be followed for examining, using and storing the data obtained;
- 5) the precautions to be taken when communicating the data to other parties; and
- 6) the circumstances in which recordings may or must be erased or destroyed.<sup>87</sup>

While this case law developed in relation to the content of telephone calls, the ECtHR found in *Copland v. United Kingdom* that e-mail content and internet usage should enjoy similar protection as telephone calls, as the same reasonable expectation of privacy is applicable.<sup>88</sup>

At first, these minimum criteria may seem difficult to translate to a context where communications are not ‘tapped’ to investigate crimes. The connection between sensor systems and law enforcement mentioned above, such as the possibility of information gathered by sensor systems being used in criminal proceedings, imply however that the logic underpinning these requirements may still be valid.<sup>89</sup> To the extent that it is, there must be sufficiently clear rules to give the public an adequate indication of when their communications are liable to be intercepted. Furthermore, the power vested in the executive must not be unfettered or arbitrary, but subject to clear limits and safeguards.<sup>90</sup>

The criteria developed in relation to metadata is somewhat less stringent. While most aspects of legality that apply to metadata are the same as those the court has established in relation to content of communication, there are some differences. In relation to information about numbers called the Court has reduced the requirement to “essentially [...] considerations of foreseeability and lack of arbitrariness”.<sup>91</sup> As such, certain legal safeguards applicable to interception of content such as the six requirements from *Klass*, may not apply as strictly to metadata. This approach by the Court has been regarded as a failure to take into account the type of information that can be gathered through metadata.<sup>92</sup> However, this distinction may be revised by the ECtHR given the influence of CJEU case law relating to metadata in the data retention cases.<sup>93</sup> In the case of *Roman Zakharov v. Russia*, the ECtHR noted the development of the view on metadata by the CJEU,<sup>94</sup> but unfortunately did not elaborate on the distinction between content and metadata surveillance under the convention, as the surveillance by the Russian authorities subject to analysis in the case included both. The ECtHR did however restate the need for any system of surveillance to minimize discretion of authorities and provide adequate and effective

---

<sup>87</sup> See *Roman Zakharov v. Russia* (47143/06) (2015) HUDOC, p. 231. See also *Valenzuelas Contreras v. Spain* (27671/95) (1998) HUDOC, p. 46; *Szabó and Vissy v. Hungary* (37138/14) (2016) HUDOC, p. 56.

<sup>88</sup> *Copland v. the United Kingdom* (62617/00) (2007) HUDOC, p. 41-42.

<sup>89</sup> See by analogy the analysis of the CJEU in case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, judgment of the court, second chamber, 19 October 2016, ECLI:EU:C:2016:779, p. 47, where the CJEU noted the possibility of obtaining identifying information relating to dynamic IP addresses to bring criminal proceedings in the event of cyber-attacks, thereby connecting information security arrangement to a wider legal framework surrounding law enforcement.

<sup>90</sup> Cf. *Roman Zakharov v. Russia* (47143/06) (2015) HUDOC, p. 228-230; *Malone v. The United Kingdom* (8691/79) (1984) HUDOC, p. 79–80.

<sup>91</sup> See *P.G. and J.H. v. The United Kingdom* no. 44787/98, 25 September 2001, §§ 46-47, contrasting the case in question to *Kopp v. Switzerland*, no. 23224/94, 25 March 1998, which concerned the tapping of a lawyer’s phone-line, including the content of communications.

<sup>92</sup> See Iain Cameron in Swedish Government Official Reports, 'SOU 2010:103 - Särskilda spaningsmetoder, betänkande av Polismetodutredningen' (Swedish Government 2010), p. 477.

<sup>93</sup> See further below section 4.3.

<sup>94</sup> *Roman Zakharov v. Russia* (47143/06) (2015) HUDOC, p. 147.

guarantees against abuse. This latter requirement will entail an assessment of all the circumstances of the case “such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law”.<sup>95</sup>

The requirements of foreseeability and lack of arbitrariness thus imply more specific components, primarily in relation to specificity of rules, routines and procedures when surveilling metadata. These requirements will become more stringent as a system of surveillance moves towards “indiscriminate capturing of vast amounts of communications”, as the development of such surveillance will need to be surrounded by a simultaneous development of appropriate legal safeguards.<sup>96</sup>

#### **4.2.3 Sensor system monitoring of public employee communications**

A sensor system deployed at a public authority would not only monitor the communications of individuals contacting authorities or accessing information on government systems, it would also monitor network traffic of public employees such as incoming and outgoing e-mail. It is well established in the case law of the ECtHR that even when monitoring of communication takes place at work, it will interfere with both the right to respect for correspondence and private life. As such, the scope of article 8 is not limited to ‘personal’ communication in the narrow sense but also covers communication in the workplace.<sup>97</sup> The ECtHR noted in the case of *Copland* that it ‘would not exclude that the monitoring of an employee’s telephone, e-mail or Internet usage at the place of work may be considered “necessary in a democratic society” in certain situations in pursuit of a legitimate aim’.<sup>98</sup> However, in *Copland*, the court found that no domestic legal rules existed at the time that gave the public employer a mandate to monitor communications, and the requirement that an interference with article 8 had to be ‘in accordance with the law’ was therefore not met. Beyond its mere existence, such a legal mandate must also reach the quality of law (rule of law) criteria established in the Courts jurisprudence on secret surveillance, mentioned above.<sup>99</sup>

When the ECtHR was recently asked to review the monitoring of internet messaging communications in a private workplace in the case of *Bărbulescu*, the Court in a chamber judgment initially found such monitoring proportional under the circumstances, given that the employer thought the communication in question would be work-related and as the access to communication was limited in scope.<sup>100</sup> The case was however referred to the Grand Chamber of the ECtHR who found a violation of article 8. In particular, the Grand Chamber found that an employer restricting the use of the internet in the workplace might not reduce the private social life in the workplace to zero. While necessary limitations may be made to further, for example, the security of IT-systems, the right to respect for privacy of communication continue to exist. The Grand Chamber pointed to the need for prior information to employees regarding monitoring but pointed out that even with such prior notice the balance between privacy and the needs of the employer must be fair. As the national courts had failed to examine whether the aim pursued by

---

<sup>95</sup> Ibid. p. 231-232.

<sup>96</sup> See *Szabó and Vissy v. Hungary* (37138/14) (2016) HUDOC §§ 68-69.

<sup>97</sup> See *Copland v. the United Kingdom* (62617/00) (2007) HUDOC, p. 41; *Amann v. Switzerland* (27798/95) (2000) HUDOC, p. 65-67; *Halford v. the United Kingdom* (20605/92) (1997) HUDOC, p. 44.

<sup>98</sup> *Copland v. the United Kingdom* (62617/00) (2007) HUDOC, p. 48.

<sup>99</sup> *Copland v. the United Kingdom* (62617/00) (2007) HUDOC, p. 46.

<sup>100</sup> *Bărbulescu v. Romania* (61496/08) [Chamber judgment] (2016) HUDOC, p. 60. The chamber judgment contrasted this case with the search and seizure of computers and data belonging to lawyers which could include privileged information.

the employer could be reached by less intrusive methods and failed to take into account the severity of the sanction (as Mr. Bărbulescu had been terminated), domestic courts had failed to afford adequate protection of the applicant's rights under article 8.<sup>101</sup>

This case is not directly comparable to *Copland* and other previous cases concerning monitoring of public employees as it only concerned the positive obligations of the state to protect the applicant from interference from other private parties (the private employer). Consequently, the domestic authorities in *Bărbulescu* only had to strike a fair balance, within the margin of appreciation of the state, between the applicant's right to respect for his private life under Article 8 and his employer's interests. The Grand Chamber did however indicate that the applicable principles are nonetheless similar.<sup>102</sup>

The sensor system serving as an example in this article is intended to be placed outside of the government agency firewall, which according to the government means that IP-traffic will be traceable only to the joint outward-facing IP of the government agency in question, not individual employee IP's.<sup>103</sup> In practice, the placement of sensors is thus likely to have a large bearing on the degree of interference with employee privacy in this regard. In any case, the alarm databases and traffic recordings may include the content of e-mail to or from a specific employee, which would potentially result in the identification of individual employees and their communications.

In contrast with the case of *Bărbulescu*, recordings in the alarm database may be regarded as justifiable due to the similarities of the traffic with existing alarm profiles. It implies at least a *prima facie* connection with a suspected communication pattern, with the exception for false alarms. While the traffic flow sensors retain metadata on a general basis without any connection to a suspicion or existing alarm profile, they are less problematic in the specific context of employee monitoring, as they would not store the individual IP address of a particular employee.

In conclusion, while the legal framework surrounding the monitoring of public employees' communication may not have to reach the same standard as the interception of communications content of individuals in general, it still must have a statutory basis; respect the rule of law requirements of foreseeability and precision as established by *Copland*. Furthermore, prior information to the employee and a reasonable balance between the interest of the employer and the employee must be reached as established in *Bărbulescu*.

#### 4.3 The Charter and the CJEU: Taking Metadata Seriously

The ECtHR is of course not the only legal limit surrounding the implementation of sensor systems. As mentioned above, the Charter will be applicable when states act within the scope of EU-law. Storing and monitoring of (dynamic as well as static) IP addresses by government agencies has been regarded as falling under the scope of the Data Protection Directive as it involves the processing of personal data, if there are legal means to identify the data subject with additional data which an internet service provider has about that person.<sup>104</sup> There is nothing to suggest that sensor systems would fall outside of the scope of the Charter nor that the

---

<sup>101</sup> *Bărbulescu v. Romania* (61496/08) [GC] (2017) HUDOC, p. 124-141.

<sup>102</sup> *Bărbulescu v. Romania* (61496/08) [GC] (2017) HUDOC, p. 112.

<sup>103</sup> Justitiedepartementet, 'Tillhandahållandet av Tekniska Sensorsystem - Ett Sätt Att Förbättra Samhällets Informationssäkerhet' (Swedish Government 2017), p. 11.

<sup>104</sup> C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, judgment of the court, second chamber, 19 October 2016, ECLI:EU:C:2016:779, p. 47.

interpretation would be different under the GDPR given the extensive interpretation of the material scope of EU-law within the area of fundamental rights.<sup>105</sup>

The Court of Justice of the European Union ('CJEU') has been quite forceful in the application of the Charter in cases relating to communications monitoring in different contexts. The tone was set early on in *Scarlet Extended*, a case dealing with the compatibility with EU-law of an injunction on a Belgian internet service provider (ISP) to implement 'deep-packet inspection'<sup>106</sup> in order to block copyright infringement by their customers.<sup>107</sup> The CJEU approached the balancing exercise between the interests of the intellectual property rights holders and the ISP and its customers by taking into account the effects on 1) the freedom to conduct business of ISP:s, 2) the data protection rights of ISP customers under article 8 of the Charter, and 3) the effects on freedom of information under article 11 of the Charter. It concluded that considering these three interests, an injunction requiring the monitoring of all the electronic communications made through the network of the ISP concerned in the interests of right holders, unlimited in time and directed at all future infringements, did not strike a fair balance between the involved interests.<sup>108</sup> A similar approach was used in *Netlog*, another case concerning intellectual property rights and filtering of network content, this time concerning an injunction on a social network operator, with a similar outcome.<sup>109</sup> The three-pronged approach used by the CJEU makes it difficult to sort out the weight attributed to the right to data protection as such and the outcome of an analysis of sensor systems, which would not affect the freedom to conduct business.

Despite certain important differences, the CJEU case law surrounding the invalidated Data Retention Directive (DRD)<sup>110</sup> and its member state equivalences and their compatibility with fundamental rights should also be mentioned in this regard. While the DRD was significantly wider in its scope, requiring the retention of communications metadata connected to the communications of virtually every person living or working within the EU, it did not collect any communications content. This distinction is important but should not be overstated, as traffic and location data allow for a comprehensive mapping of the individual, as acknowledged by the CJEU in its landmark ruling in *Digital Rights Ireland*.<sup>111</sup> The sensor system on the other hand will only collect metadata relating to internet traffic to and from government systems providing essential services but will include scanning of all incoming traffic and the retention of content of e-mail messages flagged by the alarms. The sensor system proposed in Sweden may also come to

---

<sup>105</sup> See Derlén, Mattias & Johan Lindholm, 'Three Ideas: The Scope of EU Law Protecting Against Discrimination', in Derlén & Lindholm (ed.), *Volume in Honor of Per Hallström* (Iustus förlag, 2012), p. 86-90.

<sup>106</sup> *Deep Packet Inspection* refers to technology allowing the operators of network to monitor not only the header of IP-packets, but also the content or payload of the packet - the text, images, files or applications transmitted by the user. It allows for real-time searching for patterns of interest in network data streams and classification and control of traffic based on content, applications and subscribers. See Bendrath, Ralf & Milton Mueller, 'The end of the net as we know it? Deep packet inspection and internet governance', *New Media & Society*, 13(7) 1142-1160, p. 1144.

<sup>107</sup> Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] Judgment of the Court (Third Chamber) of 24 November 2011, ECLI:EU:C:2011:771.

<sup>108</sup> Ibid. p. 46-54.

<sup>109</sup> Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] Judgment of the Court (Third Chamber) of 16 February 2012, ECLI:EU:C:2012:85.

<sup>110</sup> Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

<sup>111</sup> Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014], Judgment of the Court (Grand Chamber), 8 April 2014 (ECLI:EU:C:2014:238), p. 27.

retain, through the alarm and network flow databases, information relating to the communications of large portions of Swedish internet users. Sweden has largely deployed internet systems to allow citizens to handle their interactions with public agencies, making communication with government agencies through their services and network more or less a ubiquitous part of the Swedish society. Sweden ranked 8<sup>th</sup> in the EU in the European Commission's Digital Economy and Society scorecard on 'digital public services', with 50% of internet users categorized as 'eGovernment users' (the EU-average being 34%).<sup>112</sup> To further increase this figure Sweden has implemented a 'digital first' strategy whereby as far as possible and relevant digital services should be the default in the public sectors contacts with people and companies.<sup>113</sup> As such, the impact of sensor systems on the privacy of average Swedish internet users is likely to increase over time.

As mentioned above, the CJEU in *Digital Rights Ireland* showed that it took communications metadata (including *inter alia* location data, identifying information, IP addresses and numbers called)<sup>114</sup> seriously and elaborated somewhat on the sensitivity of the data itself, finding that:

*“Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.”*<sup>115</sup>

As the CJEU subsequently pointed out in the *Tele2 & Watson* judgment, where it gave a preliminary ruling on the Swedish and British data retention rules still in place after the invalidation of the DRD, this is “information that is no less sensitive, having regard to the right to privacy, than the actual content of communications”.<sup>116</sup> In its ruling the CJEU discussed traffic and location data subject to retention as a collected whole and as a consequence it is difficult to assess the degree of sensitivity of individual categories of data, or the relevance of the case in relation to retention of data which is less comprehensive in terms of its possible use in the mapping of the individual. In a CJEU analysis of generalized collection and transfer of airline passenger data to Canada, the court seemed to take a more generous view given the limited slice of the personal life (travels to Canada) the information related to, and provided sensitive information was not subject to transfer and appropriate safeguard existed for access to the transferred information.<sup>117</sup> In any case, the CJEU case law on data retention highlights the danger of disregarding meta-data as something harmless or something that is by default less sensitive than communications content.<sup>118</sup> Should the data processed and retained by sensor systems be deemed similar, for example through the combination of metadata and e-mail content, it is worth

<sup>112</sup> European Commission, 'Digital Economy and Society Index 2017' (European Commission 2017) <<https://ec.europa.eu/digital-single-market/en/scoreboard/sweden>>

<sup>113</sup> Swedish Government, 'Digitalisering av Offentlig Sektor' (Swedish Government 2017) <<http://www.regeringen.se/regeringens-politik/digitalisering/digital-forvaltning/>>

<sup>114</sup> Ibid. p. 26.

<sup>115</sup> Ibid. p. 27.

<sup>116</sup> Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (2016), Judgment of the Court (Grand Chamber) of 21 December 2016, ECLI:EU:C:2016:970.

<sup>117</sup> Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, ECLI:EU:C:2017:592.

<sup>118</sup> For a similar analysis, see United Nations General Assembly (2013), 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue', A/HCR/23/40, 17 April 2013.

noting that the further principles established by the CJEU in *Tele2 & Watson* would significantly limit the permitted use of sensor systems. It is likely that retention of data would then only be able to be justified by the fighting of *serious crime*.<sup>119</sup> To ensure that retention would be the exception and not the rule, the CJEU also points to the need for the national legislation to be based on “*objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security*”.<sup>120</sup> A further implication is the need to limit the access and use of this data by defining the circumstances where relevant national authorities may access data. As the CJEU puts it, access “should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body”.<sup>121</sup> Importantly, the need for notification of affected individuals when authorities have accessed their data is also stressed, as this is key to allowing them to exercise the right to a legal remedy.<sup>122</sup>

The data in question in terms of communications meta-data retained by sensor systems such as the one proposed in Sweden is less comprehensive than that of the data retention systems evaluated by the CJEU. For example, it does not necessarily retain the names and addresses of individuals communicating with the public agency unless an alarm has triggered the recording of communications content. Such information may however be possible to retrieve based on the data in the system, or through legal means of accessing further information about the users of a certain IP address from internet service providers. Furthermore, the retained data only relates to the communication of the individual with the authority where the sensor system is deployed as such, not communication in general, which must be seen as an important limitation. The retained data also does not necessarily contain location data beyond that associated with the IP-number of the individual communicating with the authority. However, the data retained will include data from all authorities where sensor systems are deployed, collecting them into a larger whole. It is therefore reasonable to argue that the deployment of sensor systems may, as the CJEU observed with regards to the DRD in *Digital Rights Ireland*, have an effect on the exercise of freedom of expression as protected under article 11 of the Charter. Furthermore, it may affect the rights under article 7 and 8 of the Charter as retention of data affects private life and implies processing of personal data.<sup>123</sup>

#### 4.4 The GDPR and ePrivacy regulation: a shifting legal basis

##### 4.4.1 Communications data as personal data

It is clear that the processing and retention of data relating to communications with government information systems implies the processing of personal data, bringing with it the application of EU data protection law.

In the case of *Patrick Breyer v. Bundesrepublik Deutschland* (*‘Breyer’*), the CJEU specifically approached issues relating to the storing of IP addresses belonging to the users of government information systems. The Bundesgerichtshof in a request for a preliminary ruling put

---

<sup>119</sup> Ibid. § 102.

<sup>120</sup> Ibid. § 111.

<sup>121</sup> Ibid. §§ 119-120.

<sup>122</sup> Ibid. § 121.

<sup>123</sup> Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014], Judgment of the Court (Grand Chamber), 8 April 2014 (ECLI:EU:C:2014:238), § 28-29.

two questions to the CJEU. First if dynamic IP addresses could be considered personal data under the Data Protection Directive if a third party (an access provider) has the additional knowledge required to identify the data subject, and secondly, put more simply, if the storing of such addresses without the users consent for purposes beyond the facilitation, and charging for, the specific use of the government information system was acceptable under the Data Protection Directive. This second question also included considerations of the storing of such data beyond the users visit to the information system to ensure the functioning of these systems in the future.<sup>124</sup> Both these issues are pertinent to sensor systems.

In *Breyer* the CJEU noted that dynamic IP addresses did not directly reveal the identity of internet users, but the indirect information that could legally be obtained from an internet access provider meant that it was personal data under the Data Protection Directive. Here, the link between access logs, kept for information security purposes, and the possibility of a criminal investigation into cyber-attacks were specifically mentioned as a relevant factor.<sup>125</sup>

Under the proposed new ePrivacy regulation,<sup>126</sup> there is a general presumption expressed in recital 4 that any electronic communications data is personal data as defined in the GDPR, which has been regarded as an extension of the scope of the ePrivacy regulation in comparison with the directive.<sup>127</sup> This presumption should apply to IP addresses as well, but in any case, IP-addresses is clearly included in the category of communications metadata under article 4 (3) (c) of the ePrivacy regulation. In summary, the application of both the GDPR and the ePrivacy regulation on the type of data processed by sensor systems should be clear, and more so under the new regulations.

#### 4.4.2 A caveat: Prevention and detection of criminal offences?

Given that communications data is, following the reasoning above, personal data, the applicable instruments are primarily the GDPR, and where applicable, the proposed new ePrivacy regulation. These will both be discussed further soon. First however it is worth analysing a certain caveat, as both the GDPR and the ePrivacy regulation are not, according to article 2 (1) (d) of the respective regulations, applicable to “*activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*”. Such activity will instead be governed by the new directive 2016/680.<sup>128</sup> As mentioned above, sensor systems may, in certain respects, be tied to certain ancillary responsibilities of public authorities to report incidents suspected to be based on criminal acts to law enforcement authorities.<sup>129</sup> Sensor systems are also likely to both prevent and detect criminal certain criminal acts, such as hacking-attempts, as a result of their main objective of ensuring security and

<sup>124</sup> C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, judgment of the court, second chamber, 19 October 2016, ECLI:EU:C:2016:779, p. 30.

<sup>125</sup> Ibid. p. 47-49.

<sup>126</sup> Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). (2017/0003 (COD))

<sup>127</sup> Burden, Kit, *EU update*, Computer Law and Security Review, 34 (2018), p. 171.

<sup>128</sup> Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

<sup>129</sup> See section 2.4, above.

continuity of government information systems and maintaining information security. The question is whether this will put their use under the regulations or the new directive.

Two separate arguments can be made for placing them under the scope of the regulations. First, the language in recital 12 of the new directive suggests that the intended scope of the directive is aimed at prevention and detections of threats against – primarily but not exclusively – physical security. In contrast, information security may be regarded as a general requirement of safeguarding integrity of data, which flows from the processing of personal data as such, rather than having the specific aim of detecting or preventing crime.<sup>130</sup> Second, the scope of the directive is aimed at “competent authorities”. While this is not necessarily restricted to law enforcement agencies or agencies in the justice sector as such, it does imply that competent authorities are those whose tasks are aimed at the prevention, investigation, detection or prosecution of criminal offences, etc., or that exercise public authority and public powers for this purpose.<sup>131</sup> Insofar as a sensor system is mainly deployed for information security purposes, they are more likely to fall under the scope of the GDPR and the upcoming ePrivacy regulation. However, this is likely to vary depending on the intended role of the sensor systems and the role of the responsible authorities. In the case of the proposed Swedish system, it would be deployed and run by the Swedish Civil Contingencies Agency, which does not have a law enforcement role. It is however worth noting that a higher emphasis on detecting crime and informing law enforcement authorities may shift the applicable legal framework towards directive 2016/680.

#### **4.4.3 The legal basis for processing personal data in sensor systems**

Once we have established that sensor systems imply the processing of personal data, and that the law enforcement context of directive 2016/680 is likely not applicable, the next question is locating the relevant legal basis for processing relevant for sensor systems.

In the case of *Breyer*, the CJEU found that the use of IP-addresses without the users consent and beyond what is needed to facilitate or charge for the service was allowed subject to a balancing of interest. In fact, the German law in question did not allow for such a balancing and thus precluded the use of IP addresses to ensure the future functioning of the information systems. The CJEU found that this restricted article 7(f) of the Data Protection Directive in a way that EU-law did not allow and held that German Federal institutions could have a legitimate interest in ensuring, in addition to the specific use of their publicly accessible websites, the continued functioning of those websites.<sup>132</sup> These findings in *Breyer* must however be viewed considering certain changes following the adoption of the GDPR. Under article 6 sec. 1(f), GDPR the processing of personal data is still lawful following a balancing of interest. This explicitly includes the interest of information security through recital 49. However, in the GDPR this legal basis for processing is not available for “processing carried out by public authorities in the performance of their tasks” according to art. 6 sec. 1 para. 2. The wording of this implies that public authorities would instead have to rely on art. 6 sec. 1(e), processing necessary for the performance of a task in the public interest or in the exercise of public authority vested in the controller. This would imply a departure from the legal ground for processing in *Breyer*, and

---

<sup>130</sup> This is in line with the analysis of the Swedish government on the scope of the new directive, see Swedish Government Official Reports, ‘Brottsdatalog – Delbetänkande av Utredningen om 2016 års dataskyddsdirektiv (SOU 2017:29)’ (Swedish Government 2017), pp. 168–169.

<sup>131</sup> Article 3 (7) (a–b).

<sup>132</sup> Ibid. p. 60-64.

further implies that the processing by public authorities should have a basis in Union or Member State law.<sup>133</sup>

It may be argued that the processing performed for information security purposes is not directly related to the tasks of public authorities, which would allow for the use of the balancing of interest basis.<sup>134</sup> It is somewhat difficult to draw a clear conclusion in this regard and is likely to depend on the role and responsibilities of the public authority. In the context of the proposed Swedish system, the maintenance of sufficient information security to enable a satisfactory level of operation is a specific responsibility of public authorities through government regulation.<sup>135</sup> Relying on a balancing of interest is also a less viable position in terms of the Swedish Civil Contingencies Agency who would operate the sensor system, as this it would be a part of their official tasks and powers.

While the legal basis required by the GDPR does not have to be a legislative act adopted by parliament – unless the member state constitutional order so demands – Recital 41 requires the legal basis to be clear and precise, and its application should be foreseeable to persons subject to it. In this context, the GDPR explicitly references the case law of the CJEU and the ECtHR.<sup>136</sup> Recital 45 adds that this legal basis ‘could’ specify the conditions of processing under the GDPR as well as specifications regarding, *inter alia*, type of data subject to processing, entities to which the personal data may be disclosed, purpose limitations, storage periods, and ‘other measures to ensure lawful and fair processing’.<sup>137</sup> Given the scope of the sensor systems discussed in this article, and in light of the case law of the ECtHR and the CJEU, the ‘could’ in recital 45 is more likely to be a ‘should’.

Consequently, the GDPR allows entities other than public authorities to process personal data such as IP-addresses following a balancing of interest for information security purposes to ensure the security of their information systems, but also to ensure the security of related services provided by public authorities (among others). Those same public authorities will however in many cases, depending on their delegated tasks, have to rely on a member state or union law to process the same personal data for their own information security purposes.

Arguably, EU data protection rules and their requirement of technical and organisational measures could imply a mandate and perhaps to a certain degree a responsibility to process information for information security purposes. This was the standpoint of the Swedish government in their legal analysis relating to sensor systems and the potential processing of sensitive personal data.<sup>138</sup> As developed in section 3 above, the role of sensor system as a *necessary* part of such information security measures is less than clear. The processing carried out through sensor systems is however not likely to be incompatible with those same responsibilities. The key here is instead that the quality of law requirements of recital 41 and 45 are upheld, which is likely to require more specific rules than a general responsibility can achieve.

---

<sup>133</sup> Recital 45 GDPR.

<sup>134</sup> This is for example the position of the Swedish government, see Government bill (Prop. 2017/18:105) p. 123.

<sup>135</sup> Swedish Government regulation (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

<sup>136</sup> Recital 41 GDPR.

<sup>137</sup> Recital 45 GDPR.

<sup>138</sup> Justitiedepartementet, 'Tillhandahållandet av Tekniska Sensorsystem - Ett Sätt Att Förbättra Samhällets Informationssäkerhet' (Swedish Government 2017), p. 21.

#### 4.4.4 The new ePrivacy regulation – a better legal basis?

The processing of communications data for information security purposes will likely be affected by the proposed new ePrivacy regulation. The regulation is to be considered *lex specialis* to the GDPR, meaning that in the absence of specific rules in the ePrivacy regulation the GDPR will apply. The regulation has currently not reached its final form, but a certain consensus seems to have been reached in most matters relevant for sensor systems. In the following, the discussion will focus on the latest revision by the council of the proposed regulation, dated December 5, 2017.<sup>139</sup>

Judging by the current proposal, the scope of the new ePrivacy regulation would be wide. According to article 3 (1) (c) it applies to ‘the protection of information related to the terminal equipment of end-users located in the Union’. As such, it will apply to sensor systems, regardless of whether or not the government information system where they are deployed may be considered an electronic communication service according to article 3 (1) (a) of the regulation or not.

The ePrivacy regulation contains specific rules relating to the processing of both content and metadata in this context. Recital 16 of the proposed regulation states that:

*“The prohibition of storage of communications is not intended to prohibit [...] the processing of electronic communications data to ensure the security and continuity of the electronic communications services, including checking security threats such as the presence of malware [...].”*

This is mirrored by article 6 (1) (b) which allows for the processing of electronic communications data (defined in article 4 (3) (a) as encompassing both content and metadata) if it is:

*“necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors and/or attacks in the transmission of electronic communications, for the duration necessary for that purpose”.*<sup>140</sup>

The exact scope of these expressions is difficult to ascertain. In article 7, they result in exceptions to the need to erase or anonymize communications content and metadata, but this must be read in conjunction with the requirements of the GDPR, which will govern the subsequent processing of personal data as the ePrivacy regulation only provides a legitimate legal basis for this type of processing. It is also clear that any such exception in the ePrivacy regulation must be construed in harmony with fundamental rights as interpreted by the ECJ. Here, the subsequent release of information to law enforcement agencies may become a potential issue.

Furthermore, while a legal basis may be established through the ePrivacy regulation, solving some of the issues caused by the GDPR in this regard, neither the ePrivacy regulation nor the GDPR establishes clear and precise rules in terms of the use of the information for information security purposes. The foreseeability for the individual can arguably still be low and relying exclusively on the ePrivacy regulation will likely not meet the requirements put forth in recital 45 of the GDPR. As such, more specific rules on disclosure, purpose limitations, storage period and other measures to ensure lawful and fair processing of data collected by sensor

---

<sup>139</sup> Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). (2017/0003 (COD))

<sup>140</sup> The inclusion of “and/or attacks” is one addition proposed by the council presidency compared to the text put forth by the Commission in October 2017.

systems is likely required. This is particularly important in relation to sensitive personal data, which in the case of information security sensor systems could be included in e-mail content.

As such, further requirements follow once this legal basis for the processing of personal data is established, they will not be discussed here in depth, but one point should be mentioned. The possibility of notification and information may be of particular relevance, which the CJEU pointed out in *Tele2 & Watson*, as it is a key factor for individuals to protect their interests.<sup>141</sup> However, the GDPR allows for restrictions of the right to information in light of statutory obligations of secrecy.<sup>142</sup> It is further likely that government sensor systems would be subject to such secrecy rules given the importance of keeping detailed information relating to their capacity confidential.

In the end, it is likely that the GDPR will increase the need for more detailed regulation of government information security processes, but further guidance from the CJEU on the requirements of legislative precision and foreseeability in this context would be helpful.

## 5 Conclusions

### 5.1 Complementary or conflicting rights?

The relationship between privacy and data protection is in many ways symbiotic. Protecting privacy implies the collection of less data, which is in line with data minimisation principles. Conversely, ensuring sufficient data protection protects privacy, as information about the individual is not subject to unauthorized disclosure. Interestingly, sensor systems illustrate a potential for conflict between two competing rights, resulting from the development of data protection as a right separate from privacy in a broader sense. Sensor systems do of course protect additional values beyond data protection, such as the security of public information systems and the integrity of government information resources. However, as this article illustrates, there is a growing momentum of positive data protection obligations acting as a potential driver for the deployment of such systems. In doing so, privacy and data protection may become values that largely need to be balanced against each other.

This further implies a tension within EU-law itself, as the CJEU has proven a watchful guardian of privacy in the face of wide-scale legislative encroachments from the EU through, *inter alia*, the DRD and the Safe Harbor agreement. Meanwhile, EU policy makers continues to push for improved network security through the NIS-directive, which may call for measures such as sensor system to be deployed as industry standards are developed, while simultaneously the entry into force of the GDPR implies an increased need to demonstrate sufficient technical and organisational measures to ensure protection of sensitive data.

### 5.2 The possible privatization of privacy invasive policymaking

Another significant point illustrated by sensor systems is the potential outsourcing of policymaking within the area of network and IT-security. This is due to the previously mentioned importance of *best practices* as part of technical and organisational measures under the NIS-directive and the GDPR. These best practices, as established through market-driven processes may in the end determine the necessity of deploying sensor systems as well as more detailed

---

<sup>141</sup> See section 4.3 above.

<sup>142</sup> Article 14.5(d) GDPR.

aspects regarding their scope and effect. This in turn may extra-legally emphasize measures that will intra-legally interfere with negative privacy rights. It is worth stressing that not all systems designed for enterprise sectors will reach the more stringent demands placed on public authorities under fundamental right instruments and the market driven requirements must be critically examined and translated before they are imported into the public sector.

The establishment of technology neutral rules and concepts such as “technical and organisational measures” is a common occurrence in technology law, and has been described in many contexts as a desirable mode of rulemaking to allow for technological development and flexibility.<sup>143</sup> However, there are implicit risks with such an approach, especially in areas affecting fundamental rights.<sup>144</sup> As has been shown above, the deployment of sensor systems implies such effects on privacy that will necessitate a clear and foreseeable legal framework, which limits government discretion to survive scrutiny under the ECHR and the Charter. As such, both the requirement and authorization to deploy sensor systems as well as clear boundaries of how, when and why should be regulated in law. While any demands implying positive obligations flowing from such industry standards must be interpreted within the boundaries of privacy obligations following from fundamental rights, the intermingling of data protection as a motivation for such systems implies a risk of data protection ambitions overshadowing the broader privacy effects of implementing sensor systems.

### 5.3 Striking the balance

It is clear that sensor systems must be constructed and deployed in a manner mindful of the countervailing privacy rights of the users of information systems. Striking a proper balance between data protection and privacy in this context requires an understanding of the scope and effect of sensor systems on these privacy rights. The analysis in this article can provide certain answers in this regard. While the exact configuration of the sensor systems will in the end determine the concrete effect on privacy, one conclusion is that certain issues can at the very least be minimized at the outset through the legal framework itself. The impact of a sensor system like the one proposed in Sweden would be significantly less privacy invasive than a general retention of data relating to telecommunications. However, the proposed sensor system would still likely cover many government authorities and may over time accumulate a substantial amount of data relating to citizens communication with those authorities. Consequently, the privacy risks should not be underestimated. Four main considerations should be noted when implementing such systems.

*First*, on a general level it is important to establish clear rules of access, disclosure, erasure and information to those subject to surveillance by sensor systems to fulfil requirements of both GDPR and the legal framework required by fundamental rights under the ECHR and the Charter. To a certain extent it may be most difficult to fulfil the requirement of information to those subject to surveillance by sensor systems in practice, the need for information, although in a different context, was highlighted by the CJEU in *Tele2 & Watson* it is a crucial safeguard to enable individuals to assert their legal rights. It is further stressed by the GDPR but subject to exceptions that may undermine the rights of the data subject in this particular context.

---

<sup>143</sup> See Reed, Chris, ‘Taking Sides on Technology Neutrality’, SCriPt-ed, Vol. 4, Nr. 3, September 2007, 263–284.

<sup>144</sup> See Ohm, Paul, ‘The Argument Against Technology-Neutral Surveillance Laws’, Texas Law review, Vol. 88, 2010, 1685–1713; Reed, Chris, *Taking Sides on Technology Neutrality*, SCriPt-ed, Vol. 4, Nr. 3, September 2007, 263–284.

*Secondly*, it is clear that stronger links between information security measures and law enforcement will increase the importance of legal safeguards and a clear and foreseeable legal framework surrounding sensor systems. While such concerns will not entirely be avoided by compartmentalizing sensor systems and their data from law enforcement authorities, the avoidance of a general disclosure obligation on data collected by sensor systems and clear limits and conditions regarding the circumstances when disclosure may take place, will go some way of meeting the requirements of legality and proportionality under the Charter and the ECHR. With the principles established by the CJEU in *Tele 2 & Watson* in mind, the disclosure of traffic data to law enforcement agencies should be limited to circumstances where an objective link to serious crime can be established. The quality of the rules surrounding such disclosures become even more important in relation to communications content intercepted by the sensor system, as the legal principles established by the ECtHR in this regard are more stringent than those relating to metadata.

*Third*, there should be some objective criteria to establish a connection between the data analysed, retained and disclosed, and the objective pursued.<sup>145</sup> Such a criterion may be established through the similarity between data intercepted by the sensor system and that of previously identified malicious data. The continued retention of data in traffic flow databases is the main issue in this regard, as this is not limited to traffic targeted by sensors as suspicious. Instead, the purpose is to be able to retroactively search for newly discovered suspicious traffic fingerprints. In the system proposed in Sweden the retention time of IP-numbers and timestamps in the traffic flow database is not limited in time, instead the government held that it is important that information is not retained for longer than necessary, whatever timeframe that may be.<sup>146</sup> Such an approach is problematic and at the very least, a clear time limit proportional to the objective pursued should be established, as well as strict rules on access and security relating to this data.

*Fourth*, and finally, while the sensor system is primarily intended to alert when, for example, malicious code is included in communications, it is important to consider the significance of the installation of surveillance infrastructure in government systems as such. Once in place, the configuration of the sensors is what will in the end determine the effects of the sensor systems on the right to privacy and political rights. The possibility of a shift in the purposes or configuration of alarms once the technical infrastructure is in place is not to be ignored. Consequently, it is important to ensure that there are clear rules governing the configuration of the sensors as their potential use for purposes beyond information security cannot be disregarded. Such rules, if established through parliamentary statute, would limit the discretion of government authorities and serve to increase the qualitative legality of the rules governing the sensor system. Lacking such legal safeguards there is a risk of *purpose creep*<sup>147</sup> – the use of data for a different goal than it was collected for – in relation to the sensor system. This also highlights the need for continuous independent oversight of these systems by data protection authorities.

The conclusion of this analysis is not that sensor systems must be avoided, but neither should their privacy invasive nature be disregarded because of their role in upholding data

<sup>145</sup> See in particular Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (2016), Judgment of the Court (Grand Chamber) of 21 December 2016, ECLI:EU:C:2016:970, § 110 in this regard.

<sup>146</sup> Justitiedepartementet, 'Tillhandahållandet av tekniska sensorsystem - Ett sätt att förbättra samhällets informationssäkerhet' (Swedish Government 2017), pp. 17-18.

<sup>147</sup> Regarding the term 'purpose creep', see Wisman, T.H.A., 'Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things', *European Journal of Law and Technology*, Vol. 4, No. 2, 2013.

protection and the integrity of public information systems. While there is a need for states to uphold data protection through sufficient security measures, there is not yet evidence to suggest that sensor systems are a mandatory part of such measures, nor a positive obligation under human rights instruments. However, data protection and positive obligations are considerations that may both fuel the ambition to deploy such systems and to some degree legitimise such deployment within the boundaries of human rights instruments through a balancing of the rights involved. The outcome of such a balancing will however be dependent on the legal framework surrounding their deployment. In this regard, the proposed Swedish system described in this article is hardly a functioning role model but serves at least to illustrate the issues and difficulties surrounding their deployment.

### **Acknowledgements**

The author would like to thank Tom Andersson for initially suggesting that sensor systems would be interesting to look into – it was – and Therese Enarsson for valuable comments and support in the writing of this article. The constructive comments made by anonymous reviewers have helped clarify both law and context in certain areas, making the article better in many ways. All remaining errors, obscurities or deliriums are of course to be blamed on the author. This research has been made possible through the generous support of the Ragnar Söderberg Foundation, grant no: R23/14.

## REFERENCES

- .BE, 'Cyber Security Strategy of Belgium' (Belgian Government 2012).
- Airey v Ireland* (6289/73) (1979) HUDOC
- Amann v. Switzerland* (27798/95) (2000) HUDOC.
- Bărbulescu v. Romania* (61496/08) [Chamber judgment] (2016) HUDOC.
- Bărbulescu v. Romania* (61496/08) [GC] (2017) HUDOC.
- Bendrath, Ralf & Milton Mueller, 'The end of the net as we know it? Deep packet inspection and internet governance', *New Media & Society*, 13(7) 1142-1160.
- Burden, Kit, *EU update*, *Computer Law and Security Review*, 34 (2018) 166–174.
- Cameron Iain, in Swedish Government Official Reports, 'SOU 2010:103 - Särskilda spaningsmetoder, betänkande av Polismetodutredningen' (Swedish Government 2010).
- Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] Judgment of the Court (Third Chamber) of 16 February 2012, ECLI:EU:C:2012:85.
- Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, judgment of the court, second chamber, 19 October 2016, ECLI:EU:C:2016:779.
- Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] Judgment of the Court (Third Chamber) of 24 November 2011, ECLI:EU:C:2011:771.
- Copland v. the United Kingdom* (62617/00) (2007) HUDOC.
- Costello-Roberts v. The United Kingdom* (13134/87) (1993) HUDOC.
- Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (1981).
- Datainspektionen, 'Remiss av promemorian Tillhandahållande av tekniska sensorsystem – Ett sätt att förbättra samhällets informationssäkerhet' (Datainspektionen 2017).
- Datainspektionen, 'Remiss av promemorian Tillhandahållande av tekniska sensorsystem – Ett sätt att förbättra samhällets informationssäkerhet' (Datainspektionen 2017).
- Department of Communications, Energy and Natural Resources, 'Irish National Cyber Security Strategy 2015-2017' (Irish Government 2015).
- Derlén, Mattias & Johan Lindholm, 'Three Ideas: The Scope of EU Law Protecting Against Discrimination', in Derlén & Lindholm (ed.), *Volume in Honor of Per Hallström* (Iustus förlag, 2012).
- Derlén, Mattias, Johan Lindholm & Markus Naarttijärvi, *Konstitutionell rätt* (1st edn, Wolters Kluver 2016).
- Dimitris Xenos, *The Positive Obligations of the State under the European Convention of Human Rights* (1st edn, Routledge 2013).
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
- Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data' (1995)

Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data' (1995).

Domstolsverket, 'Remissyttrande över promemorian Tillhandahållande av tekniska sensorsystem – Ett sätt att förbättra samhällets informationssäkerhet' (Domstolsverket 2017).

European Commission, 'Cybersecurity Strategy of The European Union' (European Union 2013).

European Commission, 'Digital Economy and Society Index 2017' (European Commission 2017) <<https://ec.europa.eu/digital-single-market/en/scoreboard/sweden>>

European Network and Information Security Agency, 'Data Breach Notification in The European Union' (ENISA 2011) <<https://www.enisa.europa.eu/publications/dbn>> accessed 19 January 2018.

European Network and Information Security Agency, 'Gaps in NIS standardisation Recommendations for improving NIS in EU standardisation policy' (ENISA 2016) <<https://www.enisa.europa.eu/publications/gaps-eu-standardisation>> accessed 19 January 2019.

European Network and Information Security Agency, 'Proactive detection of network security incidents' (ENISA 2011) <<https://www.enisa.europa.eu/publications/proactive-detection-report>> accessed 19 January 2018.

European Network and Information Security Agency, Technical Guidelines for the implementation of minimum security measures for Digital Service Providers' (ENISA 2016) <<https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers>> accessed 19 January 2018.

European Union, 'Explanations Relating to The Charter of Fundamental Rights of the European Union (2007/C 303/02)' (2007).

Frerot v. France (70204/01) (2007) HUDOC.

Gemalto, 'Breach Level Index - First Half 2016' (Gemalto 2016) <<http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf>> accessed 19 January 2018.

González Fuster, Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of The EU* (1st edn, Springer International Publishing 2014).

Hakem Beitollahi and Geert Deconinck, 'Analyzing Well-Known Countermeasures Against Distributed Denial of Service Attacks' (2012) 35 Computer Communications.

*Halford v. the United Kingdom* (20605/92) (1997) HUDOC.

*I v Finland* (20511/03) (2008) HUDOC.

Igor Vitalévich Kotenko and Igor Borisovich Saenko, 'Creating New-Generation Cybersecurity Monitoring And Management Systems' (2014) 84 Herald of the Russian Academy of Sciences.

Industry Findings: Public Sector' (PwC, 2017) <<https://web.archive.org/web/20170405225152/http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/public-sector-industry.html>> accessed 19 January 2018.

Internet Society, 'Global Internet Report 2016' (Internet Society 2016) <<https://www.internetsociety.org/globalinternetreport/2016/>> accessed 19 January 2018.

Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2017] Judgment of the Court (Grand Chamber) of 21 December 2016, ECLI:EU:C:2016:970.

Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] Judgment of the Court (Grand Chamber) of 9 November 2010, ECLI:EU:C:2010:662.

Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014], Judgment of the Court (Grand Chamber), 8 April 2014 (ECLI:EU:C:2014:238).

Justitiedepartementet, 'Tillhandahållandet av Tekniska Sensorsystem - Ett Sätt Att Förbättra Samhällets Informationssäkerhet' (Swedish Government 2017), p. 2-3.

Justitiedepartementet, 'Polisens tillgång till information om vissa IT-incidenter (DS 2016:22)' (Swedish Government 2016).

*K.U. v. Finland* (2872/02) (2008) HUDOC.

Kavanagh, Kelly M., Oliver Rochford, and Toby Bussa. "Magic quadrant for security information and event management." *Gartner, Tech. Rep.* (2015).

*Kopp v. Switzerland*, (23224/94) (1998) HUDOC.

Kranenborg, Herke, 'Article 8 – Protection of Personal Data', The EU Charter of Fundamental Rights – A Commentary (1st edn, Hart Publishing 2014).

Lech J Janczewski, Douglas Reamer and Juergen Brendel, 'Handling Distributed Denial-Of-Service Attacks' (2001) 6 Information Security Technical Report.

*Malone v. The United Kingdom* (8691/79) (1984) HUDOC.

*Marckx v Belgium* (6833/74) [Plenary] (1979) HUDOC.

*Michaud v. France* (12323/11) (2012) HUDOC.

*Muscio v. Italy*, (31358/03) (2007) HUDOC.

Ohm, Paul, *The Argument Against Technology-Neutral Surveillance Laws*, Texas Law review, Vol. 88, 2010, 1685–1713.

Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, ECLI:EU:C:2017:592.

*Osman v. the United Kingdom* (23452/94) (1998) HUDOC.

*P.G. and J.H. v. The United Kingdom* (44787/98) (2001) HUDOC.

*Peck v the United Kingdom* (44647/98) (2003) Reports of Judgments and Decisions 2003-I.

Praesidium of the European Convention, 'Explanations Relating to The Charter of Fundamental Rights (2007/C 303/02)' (2007).

Premier Ministre, 'French National Digital Security Strategy' (French Government 2015).

Reed, Chris, *Taking Sides on Technology Neutrality*, SCriPt-ed, Vol. 4, Nr. 3, September 2007, 263–284.

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

*Roman Zakharov v. Russia* (47143/06) (2015) HUDOC.

*S and Marper v the United Kingdom* (30562/04; 30566/04) [GC] (2008) Reports of Judgments and Decisions.

Svenska Journalistförbundet, 'Promemorian Tillhandahållande av tekniska sensorsystem – Ett sätt att förbättra samhällets informationssäkerhet' (Svenska journalistförbundet 2017).

Sveriges advokatsamfund, 'R-2017/0444' (Sveriges advokatsamfund 2017).

Swedish Government Official Reports, 'Informations- och cybersäkerhet i Sverige: Strategi och åtgärder för säker information i staten (SOU 2015:23)' (Swedish Government 2015).

Swedish Government Official Reports, 'Brottsdatalog – Delbetänkande av Utredningen om 2016 års dataskyddsdirektiv (SOU 2017:29)' (Swedish Government 2017).

Swedish government regulation (2015:1052) 'Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap'.

Swedish Government, 'Digitalisering av Offentlig Sektor' (Swedish Government 2017)  
 <<http://www.regeringen.se/regeringens-politik/digitalisering/digital-forvaltning/>>  
 Swedish Instrument of Government (1974:152)  
 Swedish National Audit Office, 'Informationssäkerhetsarbete vid nio myndigheter - RiR 2016:8' (Riksrevisionsverket 2016).  
 Swedish National Audit Office, "Informationssäkerheten i den civila statsförvaltningen – RiR 2014:23" (Riksrevisionsverket 2014).  
 Swedish National Audit Office, "Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen – RiR 2007:10" (Riksrevisionsverket 2007).  
*Sychev v. Ukraine* (4773/02) (2005) HUDOC.  
*Szabó and Vissy v. Hungary* (37138/14) (2016) HUDOC.  
*Söderman v. Sweden* (5786/08) (2013) HUDOC.  
 Taylor, Mistale 'The EU's Human Rights Obligations in Relation to its Data Protection Laws with Extraterritorial Effect' (2015) 5 International Data Privacy Law.  
 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108.  
 United Nations General Assembly (2013), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HCR/23/40, 17 April 2013.  
*Valenzuelas Contreras v. Spain* (27671/95) (1998) HUDOC.  
 Voigt, Paul & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) – A Practical Guide* (1st edn, Springer International Publishing 2017).  
 Wisman, T.H.A., "Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things", *European Journal of Law and Technology*, Vol. 4, No. 2, 2013.  
*Wos v. Poland* (22860/02) (2006) HUDOC.  
*X and Y v the Netherlands* (8978/80) (1985) HUDOC.  
*Z v Finland* (22009/93) (1997) Reports 1997-I.  
 Åklagarmyndigheten, 'Yttrande över promemorian Tillhandahållande av tekniska sensorsystem - Ett sätt att förbättra samhällets informationssäkerhet' (Åklagarmyndigheten 2017).