Offprint of article from

TRANSPARENCY IN THE FUTURE

– *Swedish openness 250 years*

Anna-Sara Lind, Jane Reichel &
Inger Österdahl (eds), Ragulka 2017

Ragulka Press

The Swedish right to freedom of speech, EU data protection law and the question of territoriality

*Jane Reichel**

1. Introduction

Sweden and the EU have quite different traditions when it comes to freedom of the press, freedom of expression and transparency on the one hand, and the protection of privacy and data protection on the other. One way these differences manifest themselves is in the choice of territorial scope of the respective legal framework. The two Swedish basic acts, the Freedom of the Press Act (FPA)[1] and the Fundamental Law on Freedom of Expression (FLFE),[2] have a rather strict national approach; they aim at protecting Swedish freedom of the press, including the right to public documents, and freedom of expression within the borders of Sweden. For example, according to the FPA, all limitations of the right to access to documents must be set out clearly in a Swedish law, the Public Access to Information and Secrecy Act.[3] Any other interest that might deserve an exception from the right to access to documents held by Swedish authorities that is not listed in this act will therefore not be protected. The Swedish freedom of the press act can be contrasted to the EU data protection law[4] which, with its wide

* My warmest thanks to the participants at the Colloquium in Uppsala, 25–26 October 2016, for your valuable input and ideas, and to associate professor of private international law, Marie Linton, for taking the time to read and generously sharing your deep knowledge.

[1] Freedom of the Press Act [Tryckfrihetsförordningen] (1949:105), official English translation.

[2] Fundamental Law on Freedom of Expression [Yttrandefrihetsgrundlag] (1991:1469), official English translation.

[3] Chapter 2, section 2, second para. FPA and Public Access to Information and Secrecy act [offentlighets- och sekretesslagen] (2009:400).

[4] The two main legislative acts are the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of per-

scope of application, may even be described as extraterritorial.[5] The EU data protection law also directs itself to processors outside the sphere of application of the specific EU acts, by only permitting transfer of personal data if one of the mechanisms in the acts are followed; under an adequacy decision of the Commission, with the availability of adequate safeguard, or, if none of the above, closely defined exceptions to the rules.[6] From the *Safe Harbor* verdict of the Court of Justice of the European Union,[7] and the aftermath of the EU-US privacy shield,[8] it is clear that the EU has high demands on those wanting to process EU data in third countries.

The divergence in the underlying philosophy of the Swedish constitutional protection of freedom of speech and the EU data protection law is clearly illustrated by two recent cases; one case from the Swedish Supreme Administrative Court from 2014, HFD 2014 ref. 66, and one case from the European Court of Human rights, the *Arlewin v. Sweden* case.[9] Both cases concerns legal consequences of the limited geographical sphere of application of the FPA and FLFE respectively, the rather strict and inflexible set up within the basic laws for restrictions of the rights guaranteed in the laws, and the connected procedures for allocating responsibility for breaches of the rights.

In the case HFD 2014 ref. 66, a Norwegian company, Accurate Care AS, requested data on all registered nurses in Sweden from the Swedish National Board of Health and Welfare. The Board rejected the request on the grounds of Chapter 21, section 7 of the Public Access to Information

sonal data and on the free movement of such data (hereinafter the Data Protection Directive) and the Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (hereinafter the General Data Protection Regulation). The General Data Protection Regulation thus replaces the Data Protection Directive, but the regulation will not come into force until May 2018 and during this time the directive is still in effect.

[5] See section 2 and Dan Jerker B. Svantesson, The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and its Practical Effect on U.S. Business, 50 Stan. J. Int'l L. 53 2014.

[6] Article 25 and 26 Data Protection Directive and Article 44–49 General Data Protection Regulation.

[7] Case C-362/14 *Schrems v. Data Protection Commissioner*, EU:C:2015:650. The Court of Justice of the European Union will hereinafter be referred to as the Court of Justice.

[8] Commission implementing decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C (2016) 4176 final (EU-US Privacy Shield Decision).

[9] Arlewin v. Sweden, European Court of Human Rights, 1 March 2016, Application no. 22302/10.

and Secrecy Act, referring to the Swedish Personal Data Act.[10] According to the Board, it could be assumed that disclosure may cause personal data to be processed in violation of the Personal Data Act. However, the Supreme Administrative Court found the exception from the right to access public documents in chapter 21, section 7 was not applicable. The Swedish Personal data act is applicable only to those processing data (data controllers) who are established in Sweden, and thus not to Norwegian companies. There was therefore no legal basis for restricting the right to access to documents in Sweden, and the information was thus to be released.

The *Arlewin v. Sweden* case concerned a broadcast where the applicant, Arlewin, had been portrayed as a central figure of organised crime within media and advertising as well as being guilty of several counts of fraud and other economic offences. Arlewin argued that his appearance in the show breached his right to privacy as well as his right to be presumed innocent. Even though the show was broadcasted in Swedish, and the participants, the programme host and the production team were all Swedish, the show was broadcasted from London, UK. Accordingly, due to lack of Swedish jurisdiction, the Swedish FLFE was held not to be applicable and the Swedish courts thus rejected Arlewin's private prosecution against the Chief Executive Officer of the Swedish broadcasting firm, who was also the programme host, for gross defamation.[11] According to the FPA and FLFE and the principle of exclusivity, there is a strict and exclusive chain of legal responsibilities for publication and broadcastings, which may only be assessed in a specific procedure laid down in the basic laws.[12] The Swedish Chief Executive Officer in this case could therefore not be held responsible for the broadcasting. In the Spring of 2016, the European Court of Human Rights found that Sweden had violated Article 6 of the European Convention on Human Rights, by not affording Arlewin any legal remedies and access to courts for the alleged breaches of his right to privacy.[13]

In this chapter I will contrast the nationally-based approach on regulating the Swedish FPA and FLFE to the far-reaching approach in EU data

[10] Personal Data Act [Personuppgiftslag] (1998:204).

[11] Arlewin v. Sweden, paras. 8–17.

[12] See Chapter 7–12 FPA and Chapters 5–10 FLFE and Johan Hirschfeld's and Vilhelm Persson's chapters in this book, Free access to public documents – a heritage from 1766 and Publications Based on Crimes respectively.

[13] Arlewin v. Sweden, paras. 73–74.

protection law, where the main goal seems to be the protection of EU personal data according to an EU standard wherever it is processed in the world. The question posed is how to understand the territorial restrictions of a legal order, and lawmakers wishes to protect the individuals within this territory.

This chapter is structured as follows. In the following section 2, central concepts such as globalization, territoriality and jurisdiction are discussed. In section 3 the reach of EU data protection law is analysed, followed by the equivalent rules and practices regarding Swedish freedom of speech, in chapter 4. In section 5, some conclusions are drawn.

2. Globalisation, territoriality and jurisdiction

The effects of globalisation on law and legal systems are today a well-known phenomenon that hardly needs any justification in legal analysis. One of the questions raised in connection with globalisation is how to allocate legal responsibilities to states in cross-border situations. The more individuals, goods, services, information and ideas move cross-border, the bigger the need for adapted legal tools that can address legal affairs and connect them to a relevant legal order, to define the relevant jurisdiction and the applicable law. These issues are the focus of private international law, which, as the name of the legal area suggests, traditionally has been mostly oriented towards private law matters. The equivalent question in administrative law has been discussed within the field of international administrative law, namely the application of public law of one jurisdiction in another jurisdiction.[14] In contrast to private international law, this an area of law that seldom reaches the curriculum of general legal education or administrative law textbooks. The need to have public or administrative law solutions for identifying the applicable law to a cross-border situation was for a long period of time not particularly relevant. Traditionally, there has been a strong link between the public administration and the state, with the

[14] Herwig C.H. Hofmann, Dealing with trans-Territorial Executive Rule-Making, *Missouri Law Review*, Spring 2103, 423–442, p. 427 and Henrik Wenander, Recognition of Foreign Administrative. Decisions Balancing International Cooperation, National Self-Determination, and Individual Rights, *ZaöRV* 71 (2011), 755–785, p. 760. See further, Lena Marcusson, The internationalization of administrative law, in Anna-Sara Lind & Jane Reichel (eds) *Administrative Law beyond the State – Nordic Perspectives*, Liber, 2013s. 22.

words of Cassesse and D'Alterio, "public administrations were conceived as belonging to national communities, and thus being dependent upon national governments".[15] Today, the situation is different. There is a vivid academic debate regarding the processes of internationalisation of administrative law within the developing field of global administrative law[16] and transnational, or as referred to by Hofmann, trans-territorial administrative law.[17] However, unresolved issues still remain.

When defining the applicable legal framework in a cross-border situation, the principle of territoriality has traditionally been recognized as the predominant guiding principle.[18] As discussed by Svantesson, the highly influential Harvard Research Draft Convention on Jurisdiction with Respect to Crime ("Harvard Draft") published in 1935, describes the principle of territoriality as of "primary importance and of fundamental character" to establish jurisdiction.[19] According to this understanding, each state has jurisdiction over all legal matters occurring within their territory. The laws of jurisdiction recognized in public international law, as well as international administrative law, are thereby used to ensure that states do not assert jurisdiction over affairs that are the domain of another state.[20] States may, however, want to impact rules beyond this area, giving their legislation what can be called extraterritorial application.[21]

This can be done for several reason.[22] Benvenisti has analyzed the practice of states to unilaterally attempt to prevent or remedy collective action failures that produce global "bads" under the notion of "legislating for

[15] Sabino Cassesse with Elisa D'Alterio, Introduction: the development of Global Administrative Law, in Sabino Cassesse (ed), Research Handbook on Global Administrative Law, Elgar, 2016, p. 1.
[16] Benedict Kingsbury, Nico Krisch and Richard B.Stewart, The Emergence of Global Administrative Law, *68 Law and Contemporary Problems* 15(2005), pp. 15–61.
[17] Hofmann, (n 14) p. 425.
[18] Ibid., p. 427.
[19] Dan Jerker B. Svantesson, A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, *AJIL Unbound*, 109, 69–74, p. 69, with further reference to Draft Convention on Jurisdiction with Respect to Crime, 29 AJIL 439 (1935).
[20] Cedric Ryngaert, Jurisdiction in International Law, 2nd ed. Oxford University Press, 2015, p. 6.
[21] For a discussion on the definition on the extraterritorial concept, see Svantesson (n 5) pp. 520.
[22] Hofmann refers to anti-trust rules, and rules relating to telecommunication and the internet, (n 14), p. 428. See for an analysis on provisions determining the area of application of law from a private international law perspective, Marie Linton, S.k. tillämpningsområdesbestämmelser och Rom I-förordnigen – internationellt privaträttsliga perspektiv på sjötransporträtten [On rules determining the area of application and Rome I statute – private international law perspective on maritime law], Marius, Scandinavian Institute of Maritime Law, 2012.

humanity".[23] Benvenisti refers to examples such as the early 19th century unilateral UK action ban of the slave trade and the US sanction of today on public, private and even foreign actors who do not comply with US rules on human trafficking.[24] I will return to the question of connecting a legal order to a specific territory in section 5.

With regard to legal issues relating to the Internet, central concepts of sovereignty, territoriality and jurisdiction have been placed under severe pressure.[25] As information flows freely over the internet and over national jurisdictions, the effective protection of citizens within each and every one of these jurisdictions involved becomes difficult. As will be seen in the following two sections, the EU and Sweden have taken two rather different paths in relation to questions of territoriality and jurisdiction in regulating the use of information and personal data. Whereas the EU has taken an all-encompassing approach, Sweden has chosen to restrict the sphere of application of its rules.

3. The long reach of EU data protection law

Within its data protection law, the EU has taken as a general standpoint that the rights of EU data subjects should be protected regardless of which state the data is processed in.[26] The EU has thus established two different paths to ensuring that EU data subjects' rights to data protection are not undermined by free-flowing information routes on the internet. First, the scope of application of the EU data protection law is very wide and could even be described as extraterritorial (3.1). Secondly, EU data protection law sets up far-reaching requirements on the recipient of EU data in order for a transfer of data outside the scope of application of EU data protection law to be considered legal. If these requirements are not at hand, a data controller under obligation to apply EU data protection law is prohibited

[23] Eyal Benvenisti, The future of sovereignty: the nation state in the global governance space, in Research Handbook on Global Administrative Law, Sabino Cassesse (ed), Elgar, 2016, p. 492–3, with further references.

[24] Ibid.

[25] Svantesson, (n 5), p. 55.

[26] This section draws on research previously published in Jane Reichel, Oversight of EU medical data transfers – A bedside approach to the cross-border medical research administration, forthcoming, Health & Technology.

from transferring the data (3.2). These rules have stirred some controversy, especially in relation to the US (3.3).

3.1 The territorial scope of application of EU data protection rules

The Data Protection Directive already had an unusually broad definition of territorial scope,[27] and the General Data Protection Regulation expands it a bit further. Article 3.1-2 of the Regulation states:

> "1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
>
> 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

According to the first paragraph, all situations where a person who is established in the EU processes personal data, either on one's own behalf (con-

[27] Article 4 of the Data Protection Directive containing the equivalent rule on territorial scope, is drafted somewhat differently since EU directives (but regulations) are to be implemented into national law. That article states: 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

troller) or on behalf of another (processor),[28] must follow the rules in the regulation. Where the data is actually processed is irrelevant. With a cloud service provider, this may in any case vary. This means, for example, that if a person processing personal data in Japan (the controller) uses a data storage service established in the EU, (a processor established in the EU), the Japanese controller must adhere to EU law in regards to the data stored with the European service provider.

The second paragraph defines certain situations in which it is the EU data subject him or herself that renders the regulation applicable, even when the controller and processor is established outside of the EU. This is the case where the controller or processor targets the EU data subject, either by offering goods or services, or by monitoring their behaviour, if the behaviour takes place within the EU. There are countless providers of services and goods all over the world who may fall under this category, requiring them to uphold EU data protection law.[29]

3.2 The requirements for transferring data to third countries

Both the Data Protection Directive and the General Data Protection Regulation contain rules setting out the requirements and conditions for the transfer of personal data outside the EU. Content-wise, the differences between the directive and regulation are not significant although the rules in the regulation are more detailed.

Article 44 of the General Data Protection Regulation sets out the general principles for allowing transfers to third countries, including any onward transfer:

> "Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation."

[28] For definitions of the terms "controller" and "processor", see Article 4 (7) and (8) in the General Data Protection Regulation.

[29] See for a critical analysis, see Svantesson, (n 5), p. 71.

All transfers outside the EU must first comply – as always – with the principles in the regulation, meaning that there has to be a legal basis for the processing of the personal data that includes a transfer outside the EU.[30] Secondly, there have to be mechanisms in place to ensure that the rights of the EU data subjects will be upheld, including when the data is transferred outside of the EU.

The regulation provides a number of set procedures that can be divided into three main categories. These can be seen as hierarchical, with the first category offering the most efficient and thorough protection. First, transfer may take place if the Commission has enacted an *adequacy decision*, meaning that the Commission has found that "a country, a territory or one or more specified sectors within that country… ensures an adequate level of protection" (Article 45).[31] The Safe Harbor Agreement, further discussed below (3.2.3), is an example of this.[32] Secondly, in the absence of such decision, data may be transferred if *appropriate safeguards* are available, on the condition that enforceable data subject rights and effective legal remedies for data subjects are available (Article 46).[33] These safeguards, for example, may be legally binding and enforceable instruments between public authorities, binding corporate rules (the latter further regulated in Article 47), standard data protection clauses adopted by the Commission or on the basis especially approved of codes of conduct. Contractual clauses between the sender and recipient subject to the authorization of a competent supervisory authority also fall within this category. Thirdly, in the absence of either an adequacy decision or appropriate safeguards, there is a list of *derogations* in Article 49.[34] These derogations are narrowly construed and seem primarily to be targeting data transfers that occur on an occasional or even singular basis.

[30] Article 6.1(a) General Data Protection Regulation, corresponding to Article 7 Data Protection Directive.

[31] Corresponding to Article 25 in the Data Protection Directive.

[32] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (C (2016) 4176 final) (Safe Harbor Decision).

[33] Previously regulated in Article 26.2 in the Data Protection Directive, however the requirement to ensure that the rights of the data subject are enforceable was not explicitly mentioned. See further section 3.3.

[34] Corresponding to Article 26.1 Data Protection Directive.

A fourth and final procedure is mentioned only briefly here; the transfer of judgments and official decisions, requiring a controller or processor to disclose personal data, is permitted if based on an international agreement, such as a mutual legal assistance treaty (Article 48). If none of the above-mentioned grounds are available, the transfer of EU data outside the Union is not allowed.

3.3 The Safe Harbor-agreement, Schrems and the EU-US Privacy Shield

The Safe Harbor-agreement between the EU and US is an example of an *adequacy decision*, enacted under Article 25.6 of the Data Protection Directive, the predecessor of Article 45 in the General Data Protection Regulation.[35] The agreement itself is annexed to the actual decision enacted by the Commission, ensuring that entities within the US adhered to the principles laid down in the agreement. Thereby, the entities could be considered trustworthy recipients of EU data. EU controllers could transfer personal data to these entities without further ado. As stated above, the Court of Justice in *Schrems* found that the Commission's decision was invalid, since the Safe Harbor-agreement did not sufficiently ensure an adequate level of protection for EU data rights.[36]

The *Schrems* case was brought to court by an Austrian law student, Maximilian Schrems. He argued that his personal data on his Facebook account was not properly protected, a fact made apparent following the revelations made by Edward Snowden concerning the activities of the US intelligence services.[37] The Court held that while the term "adequate level of protection" in Article 25(6) of Directive 95/46/EC does not mean a level of protection identical to that guaranteed in the EU legal order, it must be understood as requiring a third country to ensure a level of protection of fundamental rights and freedoms "essentially equivalent" to that guaranteed within the Union by virtue of the Data Protection Directive, read in light of the EU Charter of Fundamental Rights.[38]

[35] Safe Harbor Decision, (n 32).
[36] C-362/14 *Schrems*, (n 7).
[37] Ibid., para. 28.
[38] Ibid., para. 73.

The main criticism of the Court focused on the obligation for entities within the US to disregard the Safe Harbor-principles, in the event "national security, public interest, or law enforcement requirements" within the US legal system so required.[39] As the Court rather laconically stated, since US legislation permitted public authorities such as the NSA "to have access on a generalised basis to the content of electronic communications", this constituted a breach of the EU right to privacy as guaranteed by Article 7 of the Charter.[40] There is no legal basis in EU data protection law that would render such indiscriminate surveillance of personal data lawful. Further, the fact that the US legal system did not provide for any effective remedy for EU data subjects was contrary to Article 47 of the EU Charter and the right to effective judicial protection.[41]

Negotiations between the Commission and the US on different aspects of data protection had been going on already since 2010[42] and after the verdict of the Court was delivered in 2015 they were intensified. A political agreement between the EU and US was reached in early in 2016,[43] and the Commission presented a communication to the EU legislators at the end of February, explaining the agreement in detail.[44] A new adequacy decision, the EU-US Privacy Shield, was enacted in July 2016.[45] However, some uncertainty in regards to the intentions of the Trump administration has followed on the Executive Order issued by president Trump on January 25, 2017, "Enhancing Public Safety in the Interior of the United States". Section 14 of the Executive Order reads:

[39] Ibid., paras. 85–86, referring to Safe Harbor Decision, Part B of Annex IV, (n 32).

[40] Ibid., para. 94.

[41] Ibid., para. 95.

[42] MEMO 10/1661 of the European Commission, published on 3 December 2010, available at: europa.eu/rapid/press-release_IP-10-1661_en.htm; MEMO 11/203 of the European Commission, published on 29 March 2011, available at: europa.eu/rapid/press-release_MEMO-11-203_en.htm and Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU U.S. Data Flows, COM(2013) 846 final and Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies established in the EU, COM(2013) 847 final.

[43] See press release from the Commission; europa.eu/rapid/press-release_IP-16-216_en.htm?locale=en.

[44] Communication from the Commission to the European Parliament and the Council, Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM (2016) 117 final.

[45] EU/US Privacy Shield Decision (n. 8).

> "Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."

Even though the EU-US Privacy Shield does not refer to the US Privacy Act, but affords self-standing protection for European data subjects in the US, the underlying argumentation of the Executive Decree caused some political debate within the EU.[46] The Executive Order was eventually revoked by US courts[47] and later replaced by a second Executive Order, "Protecting The Nation From Foreign Terrorists Entry into the United States". The second order did not contain any provisions on privacy.

The EU-US Privacy Shield is drafted as a general decision on the transfer of data, but is mainly directed to commercial activities and businesses. The Privacy Principles comprise thirteen Framework Principles similar to those in the Safe Harbor-agreement. Further there are Supplemental Principles, including specifications and exceptions to the framework principles as well as informational and institutional rules for the American data controllers to follow. The principles are found in Annex II to the draft decision.[48]

The EU-US Privacy shield is built on a system of self-certification by which US organizations commit to the Privacy Principle.[49] The US Department of Commerce maintains a list of all participating US organizations that have committed to the principles. In order to remain on the list, organizations will have to re-certify annually.[50] Further, under the Recourse, Enforcement and Liability Principle, all participating listed organizations must provide "robust mechanisms to ensure compliance with the other Principles and recourse for EU data subjects whose personal data have been processed in a noncompliant manner, including effective remedies".[51]

[46] See for example Nikolaj Nielsen, Trump's anti-privacy order stirs EU angst, EUobserver.com, published January 27, 2017.

[47] Washington v. Trump, 847 F.3d 1151, 1169 (9th Cir. 2017).

[48] EU-US Privacy Shield Decision, (n 8), Annex II. The Principles are: Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access and Recourse and Enforcement and Liability.

[49] Ibid., recital 31, Annex I and Annex II (Sec. I.3, Sec. I.4, III.6.d, and Sec. III.11.g)

[50] Ibid.

[51] Ibid., Recital 26 and supplemental principle "Dispute Resolution and Enforcement", Annex II, Sec. III.11.

This can be done in three alternative ways. First, EU data subjects may pursue cases of non-compliance with the principles through direct contacts with the US self-certified company. The company must respond within 45 days.[52] Second, individuals can also bring a complaint directly to the independent dispute resolution body (either in the United States or in the Union) designated by an organization to investigate and resolve individual complaints (unless they are obviously unfounded or frivolous), and to provide appropriate recourse free of charge to the individual.[53] Third, individuals may also bring their complaints to a national Data Protection Authority within a Member State of the EU. Organizations are obliged to cooperate in the investigation and the resolution of a complaint by a Data Protection Authority either when it concerns the processing of human resources data collected in the context of an employment relationship or when the respective organization has voluntarily submitted to the oversight by Data Protection Authorities.[54] Notably, organizations have to respond to inquiries, comply with the advice given by the Data Protection Authority, including for remedial or compensatory measures, and provide the authority with written confirmation that such action has been taken.[55] This also affects the choice of applicable law, since EU law will be relevant for interpretation of the compliance of a US organization:[56]

> "US law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have committed to cooperate with European data protection authorities."

European data protection authorities are to establish a specific pan-EU panel to resolve these complaints.[57] When US organizations are cooperating with EU data protection authorities, the US actors will accordingly have to abide by the EU interpretation of the Privacy Shield and its principles and will further be bound by the decisions of a pan-EU panel.[58]

[52] Ibid., Recital 43–44.
[53] Ibid., Recital 45.
[54] Ibid., Annex II, Supplementary Principles, III.5.
[55] Ibid., Recital 48 and Annex II (Sec. I.3, Sec. I.4, III.6.d, and Sec. III.11.g)
[56] Ibid., Annex II, Overview, I.7.
[57] Ibid., Annex II, Supplementary Principles, III.5.c.
[58] Ibid., Annex II, Supplementary Principles, III.5.c. ii.

Non-Compliance with any remedies provided by a dispute resolution body is to be notified to the governmental bodies or to the courts, as appropriate, and to the Derpartment. Also the US Federal Trade Commission may bring cases to the courts.[59] Accordingly, there are several steps to be taken before a person may access a court.

4. The geographically bounded jurisdiction of Swedish Freedom of the Press Act and the Fundamental Law on Freedom of Expression

The FPA has a traditional scope of application; first and foremost it applies to Swedish citizens for publications directed to the Swedish public.[60] Accordingly, in order to rely on the protection for a publication, a printed text or any other media covered, a connection to Sweden and/or the Swedish public should exist. Foreigners in Sweden, or others falling within the material scope of application, do enjoy the equivalent protection, however, these right could be changed by means of an ordinary statutory law enacted by the Swedish parliament.[61] Further, the important role of the responsible editor for periodical, can only be upheld by a person domiciled in Sweden.[62] In regards to the responsible editor for online databases, there is further a specific requirement of Swedish citizenship.[63] In Chapter 13 FPA and Chapter 10 FLFE, specific rules have been laid down addressing publications and recordings published abroad. In the following section, the background to the Swedish approach to territoriality will be briefly commented on above (2.1). In the following two sections, two examples from case law will be presented; the *Arlewin* case and the right to protection of privacy in "Swedish" programs broadcasted from the United Kingdom (2.2), and HFD 2014 ref. 66 and the list of nurses required by Accurate Care (2.3), both mentioned in the introduction.

[59] Ibid., Annex II, Supplementary principles, III, II e.

[60] Chapter 1, section 1 and 6 FPA and Chapter 1, section, 1, 2, 6, 7 and 10 FLFE.

[61] FPA chapter 14 section 5 and FLFE chapter 11 section 1, last paragraph.

[62] Chapter 4 section 2 FPA and Chapter 2, section 6 Lag (1991:1559) med föreskrifter på tryckfrihetsförordningens och yttrandefrihetsgrundlagens områden.

[63] Chapter 4, section 2 YGL. The Chapter 2, section 6 in Statute 1991:1559 does not mention YGL and therefor the requirement of Swedish citizenship for responsible editor is still upheld in regards to online databases.

4.1 Swedish traditions in a Europeanized context

The Swedish legislator is aware of the fact that Swedish traditions differ from those of other countries with regard to freedom of the press and transparency, including the EU and its Member States. As has been discussed by Österdahl, the question of transparency has been sensitive from the very start of Sweden's membership in the EU,[64] and the debate is still ongoing.[65] At first, the Swedish position was to protect and strengthen its tradition on transparency, to safeguard that the membership in the EU would not lead to less or decreased transparency. In line with this, Sweden made a Declaration on open government which was attached to the accession treaty.[66] As the years have gone by, this unequivocal stand in transparency issues has undergone change. Questions relating to transparency have been identified as an area where Swedish tradition most frequently poses problems in negotiating Swedish interest within the EU, together with the Swedish administrative model with its partially independent authorities.[67] Changes in the Public Access to Information and Secrecy Act, where exceptions to

[64] Inger Österdahl, Transparency versus secrecy in an international context: a Swedish dilemma, in Anna-Sara Lind, Jane Reichel & Inger Österdahl, Freedom of Speech, Internet, Privacy and Democracy, Liber 2015.

[65] See Olle Abrahamsson & Henrik Jermsten, Om behovet av en ny tryck- och yttrandefrihetsrättslig regleringsmodell [On the need for a new regulatory model for freedom of the press and speech], *Svensk Juristtidning* 2014 s. 201; Göran Lambertz, "Grundbultarna kan behållas" [The basic structures can remain], *Svensk Juristtidning* 2014 s. 440; Magnus Schmauch, "Tryck- och yttrandefrihetsgrundlagarna och EU-rätten — en kommentar till en kommentar" [Freedom of the press and speech and EU law — comment on a comment], *Svensk Juristtidning* 2014 s. 520; Olle Abrahamsson & Henrik Jermsten, Myter och missförstånd om TF och YGL i ett EU-perspektiv — replik [Myths and missunderstandings on FPA and FLFE in EU law perspective — a reply], *Svensk Juristtidning* 2015 s. 8; Magnus Schmauch, Fler besynnerligheter — slutreplik till Olle Abrahamsson och Henrik Jermsten [Further oddities — final reply to Olle Abrahamsson and Henrik Jermsten], *Svensk Juristtidning* 2015 s. 199; and Inger Österdahl, Offentlighetsprincipen och den svenska tryck- och yttrandefrihetsmodellen — en ytterligare kommentar [Principle of openness and the Swedish model for freedom of the press and speech — a further comment], *Svensk Juristtidning* 2016 s. 503.

[66] Treaty concerning the accession of the Kingdom of Norway, the Republic of Austria, the Republic of Finland and the Kingdom of Sweden to the European Union, Official Journal of the European Communities (O.J.) 94/C 241/07, p 397, Declaration No. 47: Declaration by the Kingdom of Sweden on open government and Declaration made by the Union in response.

[67] Jane Reichel, Den svenska förvaltningsmodellen i det europeiska samarbetsprojektet, Statskontoret och Sieps, *Statsförvaltningen efter 20 år i EU*, om offentlig sektor, [The Swedish Administrative Model in European Cooperation, in *Public administration after 20 years in the EU*], 2016.

the right of access to public documents are found, have subsequently been enacted in order to allow for more secrecy in relation to EU documents.[68]

Furthermore, the question of territorial application of the FPA has been addressed in connection to Swedish involvement in the EU and other international collaborations. The territorial scope was diminished in 2014, in order for the far-reaching regulations in the Swedish FPA not to place obstacles for Swedish international cooperation.[69] Problems had arisen for Sweden to engage in international judicial cooperation, in situations where the criminal act committed abroad was protected under the Swedish FPA and FLFE. As stated in the preparatory works, it was not considered "justified that the scope of application of the basic laws were to be so widespread. It also threatens to hinder Sweden's ability to participate in international judicial cooperation, without being motivated by strong freedom of expression interests."[70] A more limited scope of application to the FPA has therefore been considered as motivated. It was further clarified that the sphere of application for the freedom to communicate information (meddelarskydd) in connection to correspondence received was limited to situations where the information was given in Sweden, to foreign journalists.[71] In this context the clarification was also motivated by the interest of partaking in international judicial cooperation.[72]

In the following analysis, two situations in which the limited scope of application of the Swedish FPA and FLFE has caused some problems – in particular with connection to the right to an effective remedy for privacy and data protection – will be studied more closely.

4.2 HFD 2014 ref. 66

The first case to be discussed more thoroughly is the 2014 case from the Supreme Administrative Court in Sweden, on the right to access to public documents and data protection. As briefly stated in the introduction, the case concerned a Norwegian company, Accurate Care AS, who requested

[68] Inger Österdahl, Transparency versus secrecy in an international context: a Swedish dilemma, (n 64), p. 90.

[69] Changes were made in Chapter 1, section 6 and 9 FPL and chapter 1, section 10 FLFE.

[70] Regeringens proposition 2013/14:47 Några ändringar på tryck- och yttrandefrihetens område, p. 17. [Some changes in the arena of freedom of the press and speech]. Translation by the author.

[71] Chapter 13 section 6 §, second paragraph, FPA and Chapter 10 section 2 FLFE.

[72] Regeringens proposition 2013/14:47 (n 70), p. 18.

data on all registered nurses in Sweden from the Swedish National Board of Health and Welfare. The Board rejected the request on the grounds of chapter 21, section 7 of the Public Access to Information and Secrecy Act[73] which refers to the Swedish Personal Data Act.[74] According to the Board, it could be assumed that disclosure would cause personal data to be processed in violation of the Personal Data Act. However, the Supreme Administrative Court found that there was no applicable legal basis for refusing to release the documents. According to the FPA, all documents are to be public, unless otherwise clearly stated in a special act of law:[75]

> "Any restriction of the right to access to official documents shall be scrupulously specified in a provision of a special act of law, or, if deemed more appropriate in a particular case, in another act of law to which the special act refers."

The act of law referred to is the abovementioned Public Access to Information and Secrecy Act, chapter 21, section 7, which states that secrecy shall apply to personal data, if it can be assumed that disclosure would cause the data to be processed in violation of the Personal Data Act. Since Accurate Care AS was a Norwegian company established in Norway, where the Swedish Personal Data Act is not applicable, the Supreme Administrative Court found that there were no grounds for refusing access to public documents. The assessment of the Court is very short and can be cited.[76]

> "According to Chapter 21, section 7 Personal Data Act, secrecy applies to personal data, if it can be assumed that disclosure would cause the data to be processed in violation of the Personal Data Act. The assessment refers to any processing to be carried out after the release of the data (compare RÅ 2001 ref. 68 and RÅ 2002 ref. 54). Accurate Care AS is established in Norway. The Personal Data Act is therefore not applicable to the company (section 4 Personal Data Act). The company's treatment of the data in question can therefore not be in conflict with the law. Secrecy under Chapter 21, section 7 Public Access to Information and Secrecy Act does not apply to the company. Nothing in the case gives reason to believe that secrecy should apply on any other basis. The appeal is to be upheld."

[73] Public Access to Information and Secrecy Act (2009:400).
[74] Personal Data Act [Personuppgiftslag] (1998:204).
[75] Chapter 2, Section 2, second paragraph FPA.
[76] Translation by the author.

It may therefore be concluded that the right of access to documents is given priority over the right to data protection, in the Swedish constitutional tradition. The structure of the rules can further be described as inflexible; all grounds for denying the release of a document must be clearly stated in a specific act of law in order to be taken into account, no matter how relevant the interest of secrecy may be.

In the following section, another case where the limited scope of application of the FLFE meant that an individual whose privacy had been overstepped could not have the matter reviewed by Swedish courts. The matter will be discussed in the light of a verdict from the European Court of Human Rights.

4.3 *Arlewin v. Sweden*

In the case *Arlewin v. Sweden*, the European Court of Human Rights reviewed the Swedish rules on territoriality of the FLFE and the question of right to an effective remedy for breaches of a person's right to privacy.[77] The matter of the case concerned a TV programme called "Insider" aired in Sweden in April 2004, but transmitted by the Swedish company Strix from London, UK. As described in the case, the applicant, who was unknown to the broader public, appeared in the show in pictures and was mentioned by name, being singled out as the central figure of organised crime within media and advertising and as being guilty of several counts of fraud and other economic offences. However, at this time, no criminal investigation had been initiated against the applicant.[78]

To recall what was mentioned in the introduction, Swedish courts rejected Arlewin's private prosecution against the Chief Executive Officer of the broadcasting company for gross defamation, since the FLFE was not applicable to the broadcasting.[79] Almost identical questions had already been assessed by the Swedish Supreme Court in its previous case law, NJA 2002 p. 314 and NJA 2005 p. 884, where the Supreme Court had found that the broadcasts fell outside of the scope of application of the FLFE, further than what followed from Chapter 1 section 7. According to this rule, only a minor part of the FLFE was to be applied to "simultaneous and unmodified

[77] European Court of Human Rights, 1 March 2016, Application no. 22302/10.
[78] Ibid., para. 7.
[79] Arlewin v. Sweden, paras. 8–16.

onward transmission in this country of radio programmes under Article 6 that is emanating from abroad or transmitted to Sweden by satellite but not emanating from Sweden", and not, for example, rules on freedom of expression offences.[80] The Swedish basic laws rests on the premise that there is an exclusive chain of responsibility for all broadcasts and publications covered by the basic laws. This entails, in cases like the present where the basic laws were not applicable, that there was no one to be held responsible in Sweden.

The European Court of Human Rights described the problem as "Sweden did not have a regulatory framework in place that made it possible for the applicant to hold anybody civilly or criminally responsible in court for alleged infringements of his privacy rights".[81] The Swedish government held that the case should be tried before UK courts, which would have jurisdiction to try the applicant's claims for damages.[82] The European Court of Human Rights did not agree.[83]

> "Under Article 1 of the Convention, Sweden "shall secure to everyone within [its] jurisdiction the rights and freedoms" set out in the Convention. In this regard, the Court reiterates that both the applicant and X, the person against whom he brought the defamation proceedings [the Chief Executive Officer of the broadcasting company], are Swedish nationals. Moreover, as will be further described in the following, there were strong connections between Sweden, on the one hand, and the television programme and the UK company responsible for the programme contents and involved in its broadcasts, on the other. These circumstances are sufficient to conclude that there was a prima facie obligation on the Swedish State to secure the applicant's rights, including the right of access to court. Consequently, the possible access of the applicant to a court in a different country, namely the United Kingdom, does not affect Sweden's responsibility as such under Article 1, but is rather a factor

[80] The rules to be applied are the following: Chapter 1, Article 3, paragraph one, prohibiting prior scrutiny and other restrictions; Chapter 1 Article 3, paragraph three, on the possession of technical aids and the construction of landline networks; Chapter 1, Article 4, prohibiting interventions except by virtue of this Fundamental Law; Chapter 1, Article 5, on the attitude to be adopted in applying this Fundamental Law; Chapter 3, Article 1, on the right to transmit radio programmes by landline; and Chapter 3, Articles 3 and 5, on special legislative procedures and examination before a court of law. If the Riksdag has approved an international agreement concerning radio programmes, provisions under Article 12, paragraph two, may not constitute an obstacle to onward transmission of radio programmes in breach of the agreement. The article further note that Chapter 10, Article 2, contains provisions concerning the right to communicate and procure information and intelligence for publication in radio programmes emanating from abroad.

[81] Arlewin v. Sweden, para. 59.

[82] Arlewin v. Sweden, para. 57.

[83] Ibid., para. 65. See also para. 72, where the relevant connections to Sweden are listed.

> to consider in determining whether the lack of access to a court in Sweden, in the particular circumstances of the case, was proportionate under Article 6."

The European Court of Human Rights further noted that the Chief Executer Officer, who also functioned as the programme host, could rely on the freedom of communication in Chapter 10 section 2 FLFE, regardless of the fact that no individual could be held responsible for the programme content under the law.[84] Under these circumstances, the Court found that Sweden was in breach of Article 6 of the European Convention of Human Rights.[85]

5. Territorial scope and the question of a higher standard of protection

With globalization and technical development, states are forced to adjust their (perhaps natural) aspirations to apply their own constitutional rules to all situations around the world where their nationals' fundamental rights may be affected. Other states whose nationals, or even territory, is involved in the matter may also want to enforce their version of fundamental rights. The situation is not in itself new, as seen from the examples given by Benvenisti on the practice of states to unilaterally attempt to prevent or remedy collective action failures that produce global "bads" under the notion of "legislating for humanity" referred to in section 2; the UK action ban of the slave trade and the US rules on human trafficking.[86] If this reasoning would be applied to the situation discussed here, regulating freedom of speech v. data protection in cross-border situations, an immediate problem arises in finding a common understanding of what is bad. As further held by Benvenisti, "when states 'legislate for humanity' or otherwise form policies that seek global standards, it is rather evident that they should bear in mind the impact of their policies on others, and that they should balance the other's interest against their own".[87] In this connection it is also relevant to ask what states are in a position to uphold their own view on what is bad in relation to others.

[84] Ibid., para. 70.
[85] Ibid., paras. 73–74.
[86] Benvenisti, (n 23) 492-3.
[87] Ibid., p. 498.

States finding themselves in a minority opinion in regards to what can be defined as bad will have to choose their battles. As shown in the foregoing, Sweden traditionally gives precedence to the right to transparency, access to documents, freedom of press and expression in a situation where these rights are to be balanced against other rights, for example privacy and data protection. Freedom of press and expression is considered to be of higher constitutional value. However, Sweden seems to have accepted that this standpoint is not shared with the rest of the EU, or the world for that matter. Sweden has accordingly accepted to diminish the territorial scope of its basic laws in the area, the FPA and the FLFE. Better to protect what can be protected within core areas of application of Swedish law, than to accept a diminished standard all over.

It is easy to see that the Swedish regulatory approach to balancing freedom of press and expression against privacy and data protection has its limitations. The system is too rigid, with a far-driven all-or-nothing approach, which is especially vulnerable to cross-border situations. Individuals whose privacy is intruded by some outside of the scope of application of the Swedish basic laws, could often find him or herself in a situation where the responsible parties cannot be held accountable at all within the Swedish system, even if the intrusion to their privacy actually takes place in, or is strongly connected to Sweden. This is clear from the two cases discussed above, HFD 2014 ref 66 and the *Arlewin v. Sweden* case.

In the *Arlewin v. Sweden* case, the European Court of Human Rights found the Swedish regulatory framework insufficient, and found Sweden in breach of Article 6 of the European Convention of Human Rights. To my mind, the same outcome would be very likely, if the situation of the HFD 2014 ref 66 would be reviewed in Strasbourg. In this situation, there was not even the option to turn to Norwegian courts, since they would not have jurisdiction to hear a case regarding access to Swedish documents held by a Swedish authority.

Taking an overall perspective on the balancing of access to public documents and data protection, as was the relevant issue of the case HFD 2014 ref 66, it does not seem proportionate to drop all protection of an individual's personal data, simply because the intrusion emanates from a different legal order. The fact that the Norwegian data protection act, which is also based on the EU Data Protection Directive, is not mentioned in the Swedish Public Access to Information and Secrecy Act, the only act that accord-

ing to the FPA may limit the Swedish access to documents, does seem to be a convincing reason for allowing a potentially massive intrusion into the nurses' right to protection for personal data. It would have been reasonable for the Supreme Administrative Court to assess the matter in a somewhat wider perspective, taking into account the interests of the individual nurses concerned and the obligations stemming from both EU law and the European Conventions of Human Rights, and not merely the black letters of the Swedish basic laws.

On the other hand, the EU approach to data protection can be seen to be problematic from the point of view of a common understanding of what is "bad". The EU has adopted a far-reaching interpretation of extraterritoriality and requirements for recipients of EU data to adhere to, in order for a transfer of data to be lawful. One of the architects of the GDPR, Jan Philipp Albrecht, MEP and Vice-Chair of its Civil Liberties, Home Affairs and Justice, recently stated that "it is paramount to understand how the GDPR will change not only the European data protection laws but nothing less than the whole world as we know it."[88]

One may wonder if the world at large is aware of this change and has been given an appropriate opportunity to have a say, or at least a chance to adjust to it. The extraterritorial approach of EU Data Protection Law will render a large number of persons and companies around the world liable to uphold the EU law, on criteria that must be considered difficult to interpret. This is especially true since the Court of Justice has shown a tendency to interpret central concepts in an extensive and perhaps surprising manner, for example the *Google Spain* case.[89] The problems connected to lack of foreseeability and legal certainty should not be underestimated.[90]

[88] Jan Philipp Albrecht, How the GDPR Will Change the Worlds, *European Data Protection Law*, 3/2016, 287–289, p. 287.

[89] Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González ('Google Spain'). In an opinion regarding the case, the Article 29 Working Party Group holds the following; "the judgement makes it clear that the scope of current EU law extends to processing carried out by non-EU entities with a 'relevant' establishment whose activities in the EU are 'inextricably linked' to the processing of data, even where the applicability of EU law would not have been triggered based on more traditional criteria", Update of Opinion 8/2010 on applicable law in light of the Court of Justice of the European Union judgement in Google Spain, 176/16/EN WP 179 update, p. 7.

[90] Dan Jerker B. Svantesson, The Google Spain case: Part of a harmful trend of jurisdictional overreach, EUI Working Paper RSCAS 2015/45.

Further, in the situation where EU data actually leaves the scope of application of EU Data Protection Law, the EU requires that the rights of EU data subjects should be continuously upheld. Foreign oversight bodies will thus have to uphold EU Data Protection Law. Svantesson rightly points out that "the weakness of extraterritoriality is that enforcement typically is tied to territorial limitations".[91] And the main vehicle for enforcement, public administrations, have traditionally been conceived as belonging to national communities.[92] Even if there has been important developments, public administrations as organizations are typically set in national administrative culture that is not easily changed overnight. In order to overcome the territorial limitations, in other words, to achieve the efficient implementation of rules from one legislator in another legislator's territory, something extra is needed. There is an obvious risk of an "over-bureaucratization" of data protection when oversight bodies are to uphold the rules of a legislator different than the one appointed by the constitutional context in which they are embedded. Thus, in order to verify that EU personal data will remain protected after entering US jurisdiction, the EU/US privacy agreement, for example, has introduced a rather complex scheme of annual self-evaluations for companies, requirements of information, together with mechanisms of redress for data subjects. The system is to be under the supervision of either EU or US authorities, where the allocation of the final say in interpretation of the rules may vary.[93] However, even if the system is complex, it does not necessarily mean it is effective. It remains to be seen if the Court of Justice will find that the EU-US Privacy Shield affords an adequate level of protection, if and when the question will be placed before the Court. Further, it remains to be seen if the Trump administration will continue to uphold their side of the agreement.[94] Even if the second Executive Order did not contain provisions on privacy, the whole matter does cast some doubts on how determined the Trump administration is to protect EU subject's data.

[91] Svantesson (n 5), p. 519.

[92] Cassese & D'Alterio, (n 15), p. 1 and Jane Reichel, Oversight of EU medical data transfer – an administrative law perspective on cross-border biomedical research administration, Health Technol, DOI 10.1007/s 12553-017-0182-6.

[93] See above, section 3.3.

[94] See above, section 3.3.

The foreign oversight bodies tasked with supervising the processing of EU data within their jurisdiction will be in a situation where data from individuals in the EU is to be treated differently from other individual's data. The idea has a certain unpleasant ring to it. Why would these foreign oversight bodies want to make an effort to uphold and protect EU data subjects' rights, rights that "their own" nationals may not be afforded? Are EU data subjects worth a higher level of protection? Also within the EU, the rules on transfer may risk different treatments based on the origin of the data. When importing foreign data into the EU, the equivalent protection is to be upheld vis-à-vis data subjects in third countries. However, this question has not rendered much interest from EU policy-makers or academics. What are the mechanisms in place within the EU to ensure that data subjects in third countries have consented to the use of their data, on equal terms as data subjects within the EU? How can their rights to information and access to effective judicial review be upheld? EU law does not provide any convincing answer to these questions.

So, even if Swedish law makers to my mind would benefit from adopting a less rigid regulatory framework for upholding the right of freedom of press and expression in cross-border situations, the EU solution seems to go too far on the other end of the spectrum.[95] When identifying what the applicable law is, geographical borders and territoriality can no longer be considered to be of "primary importance and of fundamental character", as stated in the Harvard Draft, in 1935. As pointed out by Benvenisti, this does not mean that the entire world can be expected to apply one's own standard for the protection of rights.

Jane Reichel is Professor of Administrative Law, Uppsala University, Sweden.

[95] Compare the argument put forward by Cecilia Magnusson Sjöberg on "postmodern transparency" in her chapter, The Swedish Principle of Transparency in the context of E-learning, in this book.