CHAPTER 6

PROTECTING HUMAN RIGHTS THROUGH A GLOBAL ENCRYPTION PROVISION

Danaja Fabčič Povše

1. INTRODUCTION

In a global digital economy, data pass through servers, located in different countries with diverse rules on data protection security. Different standards and requirements lead to the problem of the global system only being as strong (or weak) as cyber-security requirements in the "least trusted country".[1]

Encryption is often put forward by the crypto experts as an effective security measure. At its core, encryption transforms text-information into a seemingly random string of words and letters that can only be deciphered by using another bit of information, called the decryption key. The rules on use of encryption vary and some countries have adopted regimes that may compromise information and conversations despite use of appropriate encryption techniques.[2] Encryption is also an important measure contributing to human rights, especially freedom of expression and the right to privacy. It keeps communications inaccessible and safe from prying eyes, enabling the sharing of opinion, accessing online information and organising with others to counter injustices.[3] In data protection, encryption is a privacy preserving technique, that also contributes to security of processing personal data.[4]

---

1 Peter Swire and Kenesa Ahmad, 'Encryption and Globalization' (2011) 23 Columbia Science and Technology Law Review.

2 An overview of different laws, applicable to encryption, incl. references, is available on two websites:
'Crypto Law Survey – Page 2' <www.cryptolaw.org/cls2.htm> accessed 4 March 2019.
'World Map of Encryption Laws and Policies | Global Partners Digital' <https://www.gp-digital.org/world-map-of-encryption/> accessed 2 July 2019.

3 Amnesty International, 'Encryption: A Matter of Human Rights' (2016) <https://www.amnesty.nl/content/uploads/2016/03/160322_encryption_-_a_matter_of_human_rights_-_def.pdf?x68337> accessed 16 July 2019.

4 Gerald Spindler and Philipp Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 Journal of Intellectual Property, Information

The data protection framework has seen two important changes in 2018 and 2019: the General Data Protection Regulation (GDPR) becoming applicable, and the modernisation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (so-called Convention no. 108+), respectively. Both instruments are oriented toward European states. However, due to their extraterritorial effects, the two instruments can be considered as means of *globalising* the data protection framework to achieve a worldwide adequate level of protection of personal data.[5]

A connected world with international data flows could therefore benefit from globalised data protection rules. However, as discussed in this paper, progress has been slow, and not all instruments explicitly contain a reference to encryption. Nevertheless, if the international community decided to push for an obligation to use encryption under international law, some potentially applicable rules are already in place. Such an obligation would apply globally.[6]

This paper attempts to address the challenge of finding such an obligation by examining provisions, relevant to encryption, that could potentially lead to a worldwide encryption requirement, thus obviating the problem of the least trusted country.[7] More specifically, it poses the question: in the absence of a global encryption treaty, which existing legal documents in the international law on privacy and data protection apply to encryption, and how could a binding legal obligation on states to mandate the use of encryption be imposed?

To answer the question, which is descriptive and normative in its nature, the following steps will be taken. First, encryption is explained from the perspective of concepts of cybersecurity and data protection, and its contribution to protection of human rights is examined. Applicable legal sources from Europe, Western Africa, Asia-Pacific and East Asia regions are analysed in order to find relevant provisions on encryption. Finally, three ways on binding states to impose encryption obligations are suggested: adoption of a relevant new international treaty on data protection or data security, globalisation of existing (European) rules, or keeping the status quo. Traditional desk research model is the most suitable method of choice, including analysis of legal state of the art in

Technology and Electronic Commerce Law [i].

Bruce Schneier, 'Essays: Why We Encrypt' (*Schneier on Security*, June 2015) <https://www.schneier.com/essays/archives/2015/06/why_we_encrypt.html> accessed 17 July 2019.

5 Graham Greenleaf, 'A World Data Privacy Treaty? "Globalisation" and "Modernisation" of Council of Europe Convention 108', *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press 2014); Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' (2012) 2 International Data Privacy Law 68.

6 For the purposes of this article, the term 'globalisation' is understood in wider than by Greenleaf, i.e. applicable on an international scale to all states bound by the relevant instrument, instead of solely meaning accession by non-European countries.

7 Swire and Ahmad (n 1).

existing academic literature, legislation and soft law guidance. Due to its scarcity, relevant case law will be examined to a smaller extent.

This chapter will focus on analysis of encryption in the international human rights legal framework. More specifically, (1) general human rights framework on the right to privacy, especially confidentiality of communications, and/or data protection, (2) legal instruments specific to data protection, and (3) soft law, i.e. experts' and policy-makers' non-binding opinions and recommendations, will be analysed.

2. ENCRYPTION, (CYBER)SECURITY AND HUMAN RIGHTS

Encryption is the process of obscuring information to make it unreadable without special knowledge. It renders the original information, called plaintext, into unintelligible cyphertext. Typically, this is done in order to ensure secrecy, confidentiality and authenticity.[8] Encryption is a crucial factor in ensuring reliable communication through ICTs, since it enables sending and receiving information without exposure to prying eyes of third parties, as well as enabling the receiver to verify that the information had really been sent by the intended sender.

Encryption enables security of information since algorithms, upon which encryption is based, make data unreadable to anyone without the appropriate decryption key. Therefore, the data are virtually inaccessible to third parties without the decryption key to see the plaintext.[9]

There are different types of encryption based on who has access to the decryption (different key management systems). Cryptographic research talks about *public (asymmetric) key cryptography* and *private (symmetric) key cryptography*. The difference between the two is that with private cryptography, one can use the same private key to encrypt and decrypt the message, whereas in public cryptography always a key pair (two keys) exist, whereby what one key encrypts only the other can decrypt the private key encrypts the message, and the public one decrypts it.[10] For example, this is how digital signatures work.

Traditionally, encryption is at the heart of the privacy or security trade-off.[11] On the one hand, cryptographic research is clear on the need for strong

8 Kostas Zotos and Andreas Litke, 'Cryptography and Encryption' [2005] arXiv <http://arxiv.org/abs/math/0510057> accessed 4 March 2019.

9 Hal Abelson and others, 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' (1997) 2 World Wide Web J. 241.

10 Steve Lloyd and Carlisle Adams, 'Key Management' in Henk CA van Tilborg and Sushil Jajodia (eds), *Encyclopedia of Cryptography and Security* (Springer US 2011) <https://doi.org/10.1007/978–1–4419–5906–5_85> accessed 6 June 2019.

11 See for example, Section 3.D, pp.320–329 of Marc Rotenberg, Paul M Schwartz and Daniel J Solove, *Information Privacy Law* (2nd ed., Aspen 2006); or Herbert S Lin, 'Cryptography and

encryption to protect against access by unauthorised third parties. Strong encryption is defined as encryption that is difficult to break[12] or unbreakable,[13] i.e. a "strong algorithm with keys properly secured, and not compromised through back doors, front doors or exceptional access",[14] without the law imposing measures, which render the algorithm less secure, and therefore weaker.[15] If the encryption method does not meet these criteria, the encryption itself cannot be considered strong and it may not provide good security.

Walking the tightrope between privacy and security is a difficult exercise. Recently, the issue has resurfaced as the law enforcement agencies re-iterate their fear of "going dark"[16] – sometimes, suspects use encrypted (or otherwise masked) communications, whose contents are inaccessible to law enforcement. Accordingly, they fear that by going dark and being unable to listen in, crime may not be prevented and public security could not be maintained. To solve the problem, governments have proposed ideas, such as using backdoors (secret access to plaintext),[17] key escrow (access to keys),[18] [19] or simply mandating actors to adopt weaker algorithms or keys.[20]

However, as cryptographic research has shown,[21] the tightrope is not only a question of privacy versus security, it is also a problem of more security

---

Public Policy' (1998) 25 Journal of Government Information 135.

12 Joris Van Hoboken and Wolfgang Schulz, *Human Rights and Encryption* (UNESCO Publishing 2016).

13 'The Importance of Strong Encryption to Security – Schneier on Security' (*Schneier on Security* 25 February 2016) <https://www.schneier.com/blog/archives/2016/02/the_importance_.html> accessed 27 March 2019.

14 Susan Landau, *Listening in: Cybersecurity in an Insecure Age* (Yale University press 2017).

15 Stephen Mason, 'Digital Signatures', *Electronic Signatures in Law* (School of Advanced Study, University of London 2016).

16 Famously referenced in the speech by James Comey in 2015, the then-director of the FBI, following terrorist attacks in the US – see: James Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (*Federal Bureau of Investigation,* October 16 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> accessed 4 July 2019.

17 Very recently proposed by the G7 summit in April 2019 – see the Outcome Document at: G7, 'Outcome Document. Combatting the use of the internet for terrorist and violent extremist content' (*elysee.fr*) <https://www.elysee.fr/admin/upload/default/0001/04/287b5bb9a30155452ff7762a9131301284ff6417.pdf> accessed 4 July 2019.

18 Abelson and others (n 9).

19 Glyn Moody, 'Nobody Saw This Coming: Now China Too Wants Company Encryption Keys And Backdoors In Hardware And Software' (*Techdirt.*, 29 January 2015) <https://www.techdirt.com/articles/20150129/06262129848/nobody-saw-this-coming-now-china-too-wants-company-encryption-keys-backdoors-hardware-software.shtml> accessed 4 July 2019.

20 For example, India mandates using keys no longer than 40 bits in certain instances. See: Software Freedom Law Center India, 'FAQ: Legal Position of Encryption in India' (*SFLC.in*) <https://sflc.in/faq-legal-position-encryption-india> accessed 4 July 2019.

21 Susan Landau and Whitfield Diffie, *Privacy on the Line: The Politics of Wiretapping and Encryption* (<https://mitpress.mit.edu/books/privacy-line>, MIT Press 2007); Harold Abelson and others, 'Keys Under Doormats' (2015) 58 Commun. ACM 24.

versus less security.[22] Namely, setting up a system that would enable lawful and exceptional access either to keys or to plaintext would be very costly and technologically very difficult. In fact, such a system would be almost impossible to implement, highly impractical and it would not prevent access by hackers or foreign, unfriendly governments. It would decrease the cybersecurity of *all* communications and transactions.[23] Moreover, backdoors may not be necessary, since arguments have been made by cybersecurity experts and lawyers[24] that law enforcement can take alternative steps to access encrypted text or information.

The advent of the digital society through the internet and associated technologies has been beneficial to businesses, individuals and society at large; however, it has also made state surveillance and mass surveillance much easier. As Amnesty International notes in its report on encryption, tracking and discovering crime used to be a laborious, cost-ineffective exercise that required agents to install wiretaps or intercept communications, has now become "easily achievable through the deployment of inexpensive electronic surveillance technologies that can conduct analyses at a speed and volume that far outpaces the capacity of traditional law enforcement or intelligence services".[25]

Intelligence services globally have made use of the information technologies in order to spy on own and foreign citizens alike. Companies, especially social media networks and technological giants like Google, have had to hand over their customers' data to state agencies without disclosing it properly.[26] After the

---

22 See the 2016 testimony in front of US Congress by Susan Landau, 'The Encryption Tightrope: Balancing Americans' Security and Privacy | Committee Repository | U.S. House of Representatives' (*U.S. House of Representatives*, 1 March 2016) <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=104573> accessed 4 July 2019.

23 Abelson and others (n 21).

24 For techno-legal analyses, see:
Orin S Kerr and Bruce Schneier, 'Encryption Workarounds' (2018) 106 Georgetown Law Journal;
Matt Olsen, Bruce Schneier and Jonathan Zittrain, 'Don't Panic: Making Progress on the "Going Dark" Debate' (The Berkman Centre for Internet & Society 2016) <https://dash.harvard.edu/handle/1/28552576 > accessed 28 June 2019.
Justin Gus Hurwitz, 'Encryption.Congress Mod (Apple + CALEA).(Communications Assistance for Law Enforcement Act of 1994)' (2017) 30 Harvard Journal of Law & Technology.

25 Amnesty International (n 3).

26 Google provides an interesting overview of its own compliance with user data request warrants at: Google, 'Requests for User Information – Google Transparency Report' (*Google*) <https://transparencyreport.google.com/user-data/overview> accessed 4 July 2019; A comparative analysis of other 'big tech' companies was compiled by Wong at: Joon Ian Wong, 'Here's How Often Apple, Google, and Others Handed over Data When the US Government Asked for It' (*Quartz*, 19 February 2016) <https://qz.com/620423/heres-how-often-apple-google-and-others-handed-over-data-when-the-us-government-asked-for-it/> accessed 4 July 2019. However, this does not take into account secret and undisclosed warrants whose scale was leaked by Snowden – see footnote 27.

revelation of NSA's secret programmes, the pervasiveness of surveillance is has gained traction and awareness.[27]

Encryption contributes to genuine enjoyment of the right to expression online by providing the opportunity to communicate confidentially. Together with anonymity, encryption creates a 'zone of privacy to protect opinion and belief'. This is especially important in environments, which are politically, socially or religiously hostile to members of certain communities – for example, artists in countries with strong censorship, or people who wish to explore their gender identity in socially conservative places. Confidential communication is also important for human rights defenders, lawyers and journalists, who wish to protect their sources or clients from societal or governmental repercussions. Nevertheless, like many other technologies, encryption can also be abused – for examples, when it is used to mask comprehensible behaviour of criminals, terrorists or cowardly cyberbullies. However, whenever states impose limitations on encryption they inadvertently affect both beneficent and maleficent users of encryption. Therefore, encryption deserves special protection.[28]

Human rights law traditionally reins in governments' powers by mandating negative obligations – i.e. the state must not interfere with the exercise of the right. Nonetheless, sometimes it is necessary to implement certain measures in order to ensure effective exercise of human rights, leading to the notion of positive obligations. Positive obligations are implied the International Covenant on Political and Civil Rights, whose Article 17(2) grants the right to the protection of the law against interferences with one's privacy rights. The European Court of Human Rights views positive obligations as necessary for the exercise of human rights in general[29] and in order to ensure private communications are not disclosed publically.[30] Accordingly, in a cyber-insecure world, where encryption has been proposed as the best line of defence against cyber-attacks,[31] positive state obligations on ensuring secure encryption is used, could be considered justifiable. Such obligations can include, but are not limited to, ensuring security of online communications, spreading awareness of internet security, encouraging vulnerability disclosure practices and facilitating the use of encryption.[32]

In a global digital economy, data traverse the globe easily and with relatively low costs. Data may pass through servers, located in different countries with

---

27 See: Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (Vintage Books 2014).

28 David Kaye, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (*United Nations Human Rights Council* 2015) <www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc> accessed 28 June 2019.

29 *Airey v Ireland*, App. no. 6289/73 (ECtHR, 9 October 1979), para. 25: "…hindrance in fact can contravene the Convention just like a legal impediment…"

30 *Craxi v. Italy*, App. no. 25337/94 (ECtHR, 17 July 2003), paras. 68–76.

31 Peter Swire and Kenesa Ahmad (n 1).

32 Amnesty International (n 3).

diverse rules on data or general IT security. As Swire and Ahmad[33] point out, different standards and requirements on strength of encryption, lead to the problem of the global system only being as strong as cyber-security requirements in the "least trusted country" mandate. For example, if a country imposes secret backdoors for law enforcement and intelligence purposes, it creates the risk that another, potentially hostile, country could access seemingly secure encrypted data as well by exploiting the decreased strength of encryption.[34] Security holes multiply when more and more governments impose limitations on strong encryption and when data pass through such territories, there is a risk that important communications end up in the hands of the least trusted country, potentially unencrypted for unauthorised eyes to see.

While the problem of least trusted country could have been contained if data never left national borders in any form, that was not possible any more by the late 90s. By 1997, there were already millions of internet users throughout the world, using tens of millions (or more) private and public keys, and there were numerous law enforcement agencies interested in accessing information located in various countries.[35] Since then, while the use of internet has expanded rapidly and the society has become very dependent on the use of networks, the arguments against –or for, from the point of view of law enforcement– imposing either key escrows, backdoors or otherwise decreasing the strength of encryption, have remained the same. Cryptographic experts point out that constructing infrastructure that would satisfy the needs of secure but accessible key escrow or exceptional access to plaintext is technically too costly and too complicated to set up according to the current technical state of the art.[36]

Moreover, the systems would have to be aligned: either all the countries adopted a mandatory key escrow system, or none. A divergence in systems would decrease the usability and security of key escrows significantly.[37]

Adoption of standards has been proposed as a means of bridging the divergence in systems – a collaboration to use cryptography for good of all mankind.[38] Standardisation has a positive effect on innovation, leading to better products and services.[39] Standards, however, are voluntary, and most of the effort has been led by a limited amount of actors, thus risking that potentially

---

33 Peter Swire and Kenesa Ahmad (n 1).

34 Peter Swire and Kenesa Ahmad (n 1).

35 Hal Abelson and others (n 9).

36 Harold Abelson and others (n 21).

37 "And this prohibition would have to be enforced on a global scale, for if this kind of initiative were to be adopted only by a limited number of countries, its usefulness would be greatly undermined. Full international consensus on the matter would have to be achieved, and this is clearly an extremely complex ambition, given the particular interests at stake."
Hassan Aljifri and Diego Sánchez Navarro, 'International Legal Aspects of Cryptography: Understanding Cryptography' (2003) 22 Computers & Security 196.

38 ibid.

39 Knut Blind, 'The Impact of Standardization and Standards on Innovation' (Manchester Institute of Innovation Research 2013) 13/15 <www.innovation-policy.org.uk/compendium/section/Default.aspx?topicid=30> accessed 18 July 2019.

more secure encryption techniques and tools are not taken into consideration out of commercial interests.

Another way to harmonise rules is globalisation-driven regulatory convergence. Governments lay down rules for businesses to follow, and since there is an interest to explore foreign markets, the legal frameworks may start resembling each other. However, in the absence of formal harmonisation, the great powers will lead the effort, and set the rules for everyone else.[40] Since the United States are without doubt a leader in the technological development, the result could be that other legal systems would follow it without allowing for more nuanced frameworks.

Finally, there are rules on an international level. As discussed above, international human rights law could in certain instances bind states to adopt certain measures in order to protect human rights rather than prevent them from doing so, as is traditionally understood. Certain areas of law, such as private international law and commercial law have profited from unification at international or regional level. Traditionally, rules are laid down in a treaty or a convention, open to other countries. However, drafting countries must be careful not to make the text too inflexible lest conventional rules become too difficult to realise in practice.[41]

The benefits of international rules are also stressed by the Council of Europe in its Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).[42] It cites reasons of unresolved jurisdiction issues – though those may not be entirely resolved by international conventions[43] – and facilitated exercise of data subjects' rights.

Adopting uniform rules on encryption – a global obligation on states to mandate the use of encryption – at international level therefore has its benefits and drawbacks. As a uniform flexible standard, it would enhance innovation in order to find a more secure encryption algorithm and other techniques, which would ensure a comparable level of protection of human rights in different legal system. On the other hand, if global superpowers, such as US and EU[44] were the only ones leading the effort, they could skew the rules in their favour, which could prevent better encryption tools being considered, and the decreased level of protection of human rights.

---

40 Daniel W Drezner, 'Globalization, Harmonization, and Competition: The Different Pathways to Policy Convergence' (2005) 12 Journal of European Public Policy 841.

41 Martin Gebauer, 'Unification and Harmonization of Laws', *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2009) <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1123> accessed 4 June 2019.

42 The report is available at 'Convention 108 and Protocols' (*Council of Europe*) <https://www.coe.int/en/web/data-protection/convention108-and-protocol> accessed 4 July 2019.

43 Aljifri and Sánchez Navarro (n 37).

44 US has by far the most encryption products available on the market, with EU member states (as a whole) not far behind it. China is surprisingly lagging behind despite their efforts at creating a home-grown encryption market. See: Bruce Schneier, Kathleen Seidel and Saranya Vijayakumar, 'A Worldwide Survey of Encryption Products' (2016) Social Science Research Network SSRN Scholarly Paper <https://papers.ssrn.com/abstract=2731160> accessed 18 July 2019.

However, the questions remains – is there already a provision obliging states to mandate the use of encryption? This will be explored in the next section.

3. FRAGMENTED PROVISIONS IN INTERNATIONAL HUMAN RIGHTS LAW

On the international law level, cryptography can trigger questions in relation to human rights, law enforcement and jurisdiction, intelligence, trade and economy, as well as export controls.[45] Data gathering as a result of breaking or limiting encryption can be seen as encroachment upon another state's territory, and lead to jurisdiction issues, which are not completely resolved by the existing legal framework.[46]

As the UN special rapporteur David Kaye has noted, encryption and/or anonymity are capable of creating "a zone of privacy to protect opinion and belief", and that any restrictions on encryption must be provided for by the law, can be imposed only if legitimate grounds exist, and such a restriction must meet the tests of necessity and proportionality.[47]

3.1. GENERAL HUMAN RIGHTS FRAMEWORK

The right to privacy is enshrined in several international human rights legal documents.

The Universal Declaration of Human Rights (UDHR),[48] arguably the most important and well-known human rights instrument despite its non-binding character,[49] provides for the right to be free from interference with, inter alia, privacy and communications in its Article 12. Any restrictions placed upon the privacy of communications, incl. restrictions on encryption, must not be arbitrary (as set out in Article 12), nor can they be arbitrary and unlawful (as laid down in Article 17).

The International Covenant on Civil and Political Rights (ICCPR)[50] likewise provides for freedom from arbitrary or unlawful interference with privacy and communications in its Article 17.

---

45 Ashley Deeks, 'The International Legal Dynamics of Encryption' <https://www.hoover.org/sites/default/files/research/docs/deeks_webreadypdf.pdf> accessed 28 June 2019 28.

46 Grant Hodgson, Breaking Encryption and Gathering Data: International Law Applications, 20 J. Tech. L. & Pol'y 39 (2015).

47 Kaye (n 28).

48 Universal Declaration of Human Rights (adopted 10/12/1948 UNGA Res 217 A(III) (UDHR).

49 See esp. pp. 32–38 of Gordon Brown (ed.), *The Universal Declaration of Human Rights in the 21st Century* (Open Book Publishers 2016).

50 International Covenant on Civil and Political Rights (adopted 16/12/1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

On regional European level, the *European Convention on Human Rights*[51] in its Article 8 provides for the right to respect for private and family life, home and correspondence. The provision applies to private and family life, home and correspondence. The European Court of Human Rights has ruled that the notion of correspondence covers not only physical means, such as letters, but also email and internet,[52] as well as instant messaging.[53] Case law has also confirmed that this right extends to interception of communications[54] in a mass surveillance scenario.[55]

The Council of Europe's Convention no. 108[56] protects an individual's right to privacy, with regard to automatic processing of personal data relating to him ("data protection"). Unlike the other human rights international conventions, it specifically applies to protection of personal data, and contains provisions about data security, which will be discussed in the next section.

The European Union legal framework provides for both rights to privacy and data protection in Articles 7 and 8 of the *Charter of Fundamental Rights of the European Union,*[57] respectively.

However, while all of the above provisions provide for either the right to privacy, or the right to data protection, they do not explicitly require the states to mandate adoption of any type of cryptography measures. While most of the provisions require *confidentiality* of communications, encryption is far from the only confidentiality measure. For example, measures such as access controls, integrity checking, intrusion detection systems and non-disclosure agreements can also contribute toward confidentiality.[58]

Since many national security agencies' efforts involve listening in to private communications, and storing information about them (metadata), masking communications through use of encryption has been put forward as a viable solution.[59]

---

51 Council of Europe, 'Convention for the Protection of Human Rights and Fundamental Freedoms' European Treaty Number 005.

52 *Copland v. the United Kingdom*, app no. 62617/00 (ECtHR, 3 March 2007).

53 *Barbulescu v. Romania*, app. no 61496/08 (ECtHR, 12 January 2016).

54 *Halford v. the United Kingdom*, app. no. 20605/92 (ECtHR, 25 June 1997), *Copland v. the United Kingdom* (cited at fn. 52).

55 *Big Brother Watch v. the United Kingdom*, apps. no. 58170/13 62322/14 24960/15 (ECtHR, 13 September 2018).

56 Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' European Treaty Number 108.

57 European Union, 'Charter of Fundamental Rights of the European Union' C326.

58 Matthew Scholl and others, 'An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule' (National institute of standards and technology 2008) <https://csrc.nist.gov/publications/detail/sp/800–66/rev-1/final> accessed 19 July 2019.

59 See, among others, Edward Snowden's 2014 speech reported at Lauren C Williams, 'Edward Snowden Says Encryption Is The Only Way To Counter Mass Surveillance' (*ThinkPogress*, 10 March 2014) <https://thinkprogress.org/edward-snowden-says-encryption-is-the-only-way-to-counter-mass-surveillance-ee450433dca8/> accessed 4 July 2019. See also Joris VJ

An implicit link between mass surveillance and encryption has been made by the European Court of Human Rights (ECtHR) in the Big Brother Watch case.[60] While ruling on the mass surveillance regime in the UK, the court indirectly acknowledged the importance of encryption as a measure against such surveillance, as it blocks intelligence services from accessing the content of a telecommunication, in para. 356 of the judgment. Moreover, as already discussed above in the introductory section, the UN Special Rapporteur's reports have explicitly linked encryption to the right to privacy and freedom of expression; however, unlike the judgment, which is binding for the country addressed, and may become a precedent in the court's case law, the reports are non-binding and recommendatory in their nature.

The Court of Justice of the EU (CJEU) has a wide-ranging jurisprudence on privacy and data protection.[61] The case law has set high standards to protect the rights and interests of individuals in mass surveillance scenarios in cases such as Digital Rights Ireland, Schrems, Tele2 Sverige and in its Opinion 1/15, having ruled on data retention rules and transfer of personal data to the United States. According to Directive 2006/24/EC (Data Retention Directive), telecom providers were required to keep metadata of their users from 6 months to 2 years, which was justified by the blanket provision of "investigating, detecting and prosecuting serious crime". Metadata retention in itself falls under the "private life" provision of Article 7 of the Charter of Fundamental Rights, as it makes people feel that their private lives are the subject of constant surveillance.[62] In principle, general-blanket-data retention is incompatible with European data protection rules, while targeted data retention may be permissible if Tele2 Sverige criteria are met.[63] The need for data retention is assessed upon the strict necessity and proportionality test. As the CJEU reiterates in its Opinion 1/15 on the EU-Canada Agreement on the transfer of Passenger Name Record data (PNR), general data retention and processing is not strictly necessary and does not meet the threshold of the test.[64] Further, in the Maximillian Schrems case on transfer of data to the US under its PRISM surveillance program, the CJEU

Van Hoboken, 'Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era Symposium: Who's Governing Privacy: Regulation and Protection in a Digital Era' (2013) 66 Maine Law Review 487; as well as Seda Gürses, Arun Kundnani and Joris Van Hoboken, 'Crypto and Empire: The Contradictions of Counter-Surveillance Advocacy' (2016) 38 Media, Culture & Society 576.

60 *Big Brother Watch v. the United Kingdom* (n 55), paras. 353–356.

61 See, inter alia: C-293/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (8 April 2014); C-362/14 *Maximilian Schrems v Data Protection Commissioner* (6 October 2015); 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 AB* (21 December 2016); and Opinion of the Court (Grand Chamber) 1/15 on PNR agreement with Canada (26 July 2017).

62 *Digital Rights Ireland Ltd.* (n 61).

63 *Tele2 Sverige*, (n 61), para. 77.

64 Opinion 1/15 on PNR agreement with Canada (n 61).

pointed out the need of data subjects – surveilled population – to have adequate control and access to court, and to have their data processed without the risk of unauthorised third party interference.[65]

3.2. SECURITY MEASURES AND STANDARDS IN DATA PROTECTION LAWS

Contrary to the human rights frameworks, data protection laws contain explicit provisions on security of (personal) data. This section will discuss the regional frameworks in Europe, Asia-Pacific and Western Africa, although it should be kept in mind that certain national legal systems, for example health data regulation in the United States under the Healthcare Insurance Portability and Accountability Act, also require the adoption of security measures.

3.2.1. European Union (EU)

The European Union is known for its strict data protection laws. Building upon the German, Swedish and French traditions of regulating data protection as early as the 1970's[66] the EU adopted the Data Protection Directive in 1995 (Directive 95/46/EC),[67] recently replaced by the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679).[68] Moreover, Member States are under a duty to protect data transmitted over public communication networks under the so-called ePrivacy Directive[69] (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

The Directive 95/46/EC was adopted in 1995. It applied to the processing of personal data wholly or partly by automatic means, and to the processing

65 *Maximilian Schrems* (n 61), paras. 86–87.

66 For a historical overview of data protection legislation in Europe, see Meg Leta Jones, 'The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 Social Studies of Science 216; or for a systemic comprehensive overview, see: Brendan Van Alsenoy, 'Regulating Data Protection : The Allocation of Responsibility and Risk among Actors Involved in Personal Data Processing' (Doctoral thesis, KU Leuven 2016) 163–206.

67 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L 281, 31–50.

68 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 (2016) OJ L 119, 1–88.

69 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002) OJ L201, 37–47.

otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. Recital 46 spelled out the need for security measures: when the protection of the rights and freedoms of data subjects required adoption of technical and organisational security measures, their adoption should be performed by taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected. Article 17 followed the recital, requiring controllers to adopt security measures having regard to the state of the art and the cost of their implementation. The level of security had to be appropriate to the risks represented by the processing and the nature of the data to be protected. However, encryption was not specifically mentioned in the text.

In 2018, the Directive was replaced by the GDPR, which entered into force on May 25 2018.

The GDPR similarly applies to processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system, according to its Article 2.

In the regime established in the GDPR, encryption plays a double role.

Firstly, according to Article 32 of the GDPR, encryption is a relevant measure in ensuring the security of personal data processing. The provision is risk-based, meaning that state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity to human rights must be taken into account when assessing the need for encryption or during its implementation. The risk assessment takes into account human rights – could the data processing lead to discrimination, or will there be government intervention. If so, the risks are considered to be significant (in the words of recital 75), and a higher level of security measures, including stronger encryption, is required.,[70] [71]

Secondly, encryption may contribute toward depersonalising personal data in the sense that it renders them unintelligible to third parties without the possession of the decryption key. There are, however, varying opinions on how anonymous encrypted data truly are. In its opinion on anonymisation techniques,[72] the Article 29 Working Party suggests that as long as the keys or the original,

---

70 Paul Voigt and Axel von dem Bussche, 'Organisational Requirements' in Paul Voigt and Axel von dem Bussche (eds), *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer International Publishing 2017).

71 In some instances, encryption can be used a data breach counter-measure. See, inter alia, Article 29 Working Party, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679 (Wp250rev.01)' (European Commission 2018) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052> accessed 28 June 2019; Ian Edwards, 'GDPR the Security Angle' (2018) 60 ITNOW 42.

72 Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (European Commission 2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> accessed 7 June 2019.

unencrypted data, are available, it is still possible to identify the data subject. On the other hand, in its Breyer[73] judgment, the CJEU has introduced the criterion "lawful means reasonably likely", when assessing the notion of identifiability of a data subject. Accordingly, some authors have suggested that encrypted data could be considered anonymous for actors, which do not possess the key and are reasonably unlikely to obtain it by lawful means. This also means that when assessing the anonymous nature of encrypted data, the strength of the encryption algorithm, the key length, and the key management system must be taken into account; and the decryption key(s) must be kept separate from the data.[74]

The rules on privacy in electronic communications in the EU have been harmonised through the ePrivacy Directive, which is scheduled to be replaced by a newer ePrivacy Regulation[75] (COM/2017/010).

Articles 4 and 5 of the ePrivacy Directive require that providers of public communications networks adopt security and confidentiality measures. While the Directive talks about such measures generally, the proposed Regulation, in its Recital 37, specifically recommends service providers, such as telecoms or internet service providers, to use encryption techniques as part of their products. Article 5 of the current ePrivacy Directive prohibits listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data. A similar provision is included in Article 5 of the proposed Regulation. However, both the Directive and the proposed Regulation explicitly exempt typical law enforcement actions out of their scope, such as prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This means that the security and confidentiality measures of the ePrivacy framework will not apply to the extent that law enforcement and security agencies are involved in wiretapping or otherwise interfering with electronic communications, as specified in Article 1(3) of the Directive.[76]

Nevertheless, this does not mean free rein for the agencies – as already mentioned above, data retention resulting from communications network monitoring for purposes of crime prevention has been subject to close scrutiny by the CJEU.,[77] [78]

---

73 The test of lawful means reasonably likely to be used was defined in the Patrick Breyer case of the European Court of Justice, and answers several questions posed in (n 70).

74 Gerald Spindler and Philipp Schmechel (n 4).

75 Commission, '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)' COM/2017/010 final – 2017/03 (COD).

76 See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2000] OJ L 201, Article 1(3).

77 See CJEU cases Digital Rights Ireland Ltd (C-293/12), Tele2 Sverige AB (C-203/15).

78 Frederik J Zuiderveen Borgesius and Wilfred Steenbruggen, 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust' (2019) 20 Theoretical Inquiries in Law.

3.2.2. Convention no. 108 of the Council of Europe

The Council of Europe is an international organisation of 47 member states spanning across the geographical Europe.[79] The legislative efforts of the Council and the case law of the European Court of Human Rights have resulted in important contributions to European data protection and privacy law.

In 1981, the Council of Europe adopted the first international binding treaty on data protection, the Convention no. 108. It applies to protection of personal data, which are defined in Article 2(a) as 'any information relating to an identified or identifiable individual'. Chapter II, which lays out the basic principles of the Convention, contains a provision on data security, which requires that appropriate security measures are taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination. According to the Explanatory report to the Convention 108, there should be specific security measures for every file, taking into account its degree of vulnerability, the need to restrict access to the information within the organisation, requirements concerning long-term storage, and so forth. The security measures must be appropriate, i.e. adapted to the specific function of the file and the risks involved. They should be based on the current state of the art of data security methods and techniques in the field of data processing.

The Convention has been amended twice and modernised in 2018; since the last update, it has been referred to as Convention 108+.[80] Unlike the original 1981 version, the modernised convention extends its scope to non-automated data processing.

The security rule contained in the Convention 108+ is slightly extended compared to its previous iteration. The first paragraph requires controllers and processors to put in place appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. The second paragraph obliges the controller to notify the supervisory authority if the security of personal data has been breached and the breach could impact the rights and fundamental freedoms of data subjects.

As with its previous version, an explanatory report is provided for Convention 108+ as well. The security provision is interpreted in paragraphs 62–66, which state that the implementation of technical and organisational security measures must take into account the nature of the personal data, the volume of personal data processed, the degree of vulnerability of the technical architecture used for the processing, the need to restrict access to the data.

79 'Council of Europe' <https://www.coe.int/en/web/portal/home> accessed 4 July 2019.

80 Full text of the original Convention, Additional Protocols and Convention 108+ available at: 'Convention 108 and Protocols' (n 42).

Moreover, they must be adopted according to the current state of the art, taking into account the implementation costs proportional to the potential risks.

3.2.3. Economic Community of West African States (ECOWAS)

The ECOWAS is an economic union of 15 states in the Western part of Africa with legislative powers; hence, the rules it adopts are binding for its member states.[81]

Its Model Data Protection Act,[82] adopted in 2010, obliges the member states to adopt their own data protection laws. The framework is similar to the pre-GDPR regime in the European Union regarding its basic definitions, principles and obligations; however, the enforcement mechanisms among different states lack coordination and harmonisation, nor does the act provide for judicial remedy nor civil liability.[83]

The Act specifically provides for security of personal data in two provisions. First, in Article 28, the principle of confidentiality and security requires the protection of personal data especially in transit – although whether that obliges data controllers to implement encryption at rest is debatable. Secondly, according to Article 43, data controllers must adopt measures to ensure that data are not deformed, damaged or accessible to unauthorised third parties.[84]

3.2.4. Asia-Pacific Economic Cooperation (APEC)

The APEC is an intergovernmental forum, set up by 21 states around the Pacific Rim in the 1980's with the aim of promoting free trade in the region.[85] Its Privacy Framework, first adopted in 2005[86] and renewed in 2015,[87] was adopted in order to promote electronic commerce in Asia and the Pacific, by inter alia facilitating trans-border flows of personal data. The Framework is based upon OECD's 2013 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data and is not binding for member states. It contains a preamble, scope

---

81 'Economic Community of West African States (ECOWAS)' <https://www.ecowas.int/> accessed 18 July 2019.

82 Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS (adopted at the 37th session of the Authority of ECOWAS Heads of State and Government on 12/02/2010, Abuja, Nigeria).

83 Uchenna Jerome Orji, 'Regionalizing Data Protection Law: A Discourse on the Status and Implementation of the ECOWAS Data Protection Act' (2017) 7 International Data Privacy Law 179.

84 Economic Community of West African States (ECOWAS) (n 81).

85 'Asia-Pacific Economic Cooperation' <https://www.apec.org/> accessed 4 July 2019.

86 Full text of the 2005 Privacy Framework is available at 'APEC Privacy Framework' (*Asia-Pacific Economic Cooperation*) <http://publications.apec.org/Publications/2005/12/APEC-Privacy-Framework> accessed 4 July 2019.

87 Privacy Framework (adopted in 2015 by Ministers of Member States of Asia-Pacific Economic Cooperation). Full text likewise available at ibid.

provisions, nine information privacy principles and provisions on domestic and international implementation.

Information Privacy Principle no. VII of the 2015 Privacy Framework[88] requires controllers of personal data to adopt appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Similarly to the GDPR, the security requirements are balanced against other criteria, such as sensitivity of the information and the context in which it is held, they must be proportionate to the likelihood and severity of the harm threatened, and periodically reviewed and reassessed.[89]

3.3. RECOMMENDATIONS OF EXPERT BODIES

This section will explore expert opinions on cryptography and encryption by international bodies and national expert agencies. While such opinions are non-binding (so-called soft law), they are nevertheless important as they can represent an important contribution to the scientific and practical state of the art in the field.

The OECD was set up in 1961 to promote international trade and progress. Today, it counts 36 member countries from mainly Western or Western-style economies, including the US, Canada, Japan and several EU member states.

In the 90's, during the first crypto war, talks resulted in the 1997 Recommendation concerning Guidelines for cryptography policy.[90] The Guidelines address policy-makers with the goal of decreasing obstacles in international trade and evolution of information and communication networks by reducing policy disparities. Encryption is linked to both privacy and data protection as well as security, similarly to the approach adopted by the European legislator. The Guidelines stipulate eight principles to be taken into account when designing cryptography policies at government level: (1) user trust into cryptography to facilitate electronic and online commerce, (2) user choice in using specific cryptographic techniques, (3) market-driven development rather than top-down requirements, (4) voluntary standardisation, (5) cryptography as a privacy and data protection preserving technique, (6) lawful access to

88 The provision in the 2015 Privacy Framework is identical to the 2005 one.

89 The APEC Framework has been criticised as unambitious and purposefully legislating lower standards than the European ones – see Graham Greenleaf, 'APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific' in Andrew T Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law* (Cambridge University Press 2006) <https://www.cambridge.org/core/product/identifier/CBO9780511494208A012/type/book_part> accessed 20 May 2019.

90 Stewart A Baker and Paul R Hurst, *The Limits of Trust : Cryptography, Governments, and Electronic Commerce* (Kluwer law international 1998).

encrypted communications, (7) the need for liability provisions, and (8) international cooperation to ensure compliant free flow of data across borders.[91]

While the Guidelines seem to promote strong encryption, the background of the talks must be taken into account. The impetus for discussion were cryptographic export controls in the US and its erstwhile administration's attempts to impose the use of specific cryptographic products, called the Clipper Chip, which enabled lawful access to communications by the FBI. This explains the notions of lawful access (Principle 6) and the use of cryptographic methods subject to applicable law (Principle 2).[92] In the end, the Clipper Chip initiative was dropped due to serious concerns following the outcry of civil rights advocates and the crypto community, while the principles remained in the text.[93]

United Nations adopted brief guidelines on computerised files in 1990. Principle no. 7 deals with security of files, requiring adoption of appropriate measures to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.[94] A follow-up report was discussed in 1999, though the series seem to have been discontinued.

ENISA is the EU agency responsible for network and systems security to the benefit of individuals, society and member states with the aim of facilitating smooth functioning of the EU single digital market. According to the upcoming Cybersecurity Act,[95] ENISA will play an important role in the upcoming certification scheme of cyber security products – however, cryptographic products are conspicuous by their absence from the Regulation. In fact, encryption is mentioned only once throughout the Act, in recital 40, which prompts ENISA to raise awareness about it as a counter-measure against cyber-attacks.

ENISA has tackled encryption in its non-binding recommendatory work, both from the perspective of privacy by design and the security/law enforcement access aspects.

---

91 Recommendation Concerning Guidelines for Cryptography Policy (adopted on 27/03/1997 by the Council of the Organisation for Economic Cooperation and Development on the proposal of the Committee for Information, Computer and Communications Policy) (the OECD Guidelines). See Organisation for Economic Cooperation and Development, 'OECD Guidelines for Cryptography Policy – OECD' (*OECD.org*) <https://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm> accessed 4 July 2019.

92 Baker and Hurst (n 90).

93 See Landau and Diffie (n 21).

94 Louis Joinet, 'Revised Version of the Guidelines for the Regulation of Computerized Personal Data Files' (*United Nations Commission on Human Rights,* 1990) <http://digitallibrary.un.org/record/43365> accessed 17 July 2019.

95 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151, 7.6.2019, p. 15–6.

The 2014 Report on Privacy by design[96] addresses policy-makers and engineers involved in different levels of privacy design processes. Encryption plays different roles; as a privacy-enhancing technique, privacy preserving technique, a tool to secure conversations, enable secure storage of data at rest, and as a computational tool. However, it does not address larger concerns about encryption, such as backdoors or access to plaintext.

ENISA's Opinion paper on encryption[97] focuses on cryptography as a confidentiality and authentication measure, both from design perspective, as well as in the context of lawful access for law enforcement and intelligence services context. Its position is strongly negative toward backdoors and key escrow due to their previous ineffectiveness, arguing that criminals will always find a way around the law, and that backdoors will decrease the level of cyber-security across the board, making criminals' work easier. More specifically, ENISA and Europol in their Joint Statement on Encryption[98] argue for 'encryption circumvention', echoing 'encryption workarounds' from Kerr and Schneier's work.[99]

On the other side of the Atlantic, the *National Institute of Standards (NIST)*, part of the US Department of Commerce has led many important initiatives in the field of cryptography, for example promoting the Data Encryption Standard from 1970 until its eventual obsolescence.[100] It published cryptography guidelines in 2016 and in 2019.

NIST's report on Cryptographic Standards and Guidelines Development Process[101] suggests to base crypto development processes on balance of interests of government, industry and academia. The standards developed must be strong and practical, and they must be capable of meeting the needs of (federal) government, as well as the user community in the broad sense. Standards adopted should be globally acceptable since encrypted products, developed in the US, are sold internationally. The document also stresses the need for consultation with government agencies, such as the National Security Agency

96 George Danezis, Josep Domingo-Ferrer and Marit Hansen, 'Privacy and Data Protection by Design – from Policy to Engineering' (ENISA 2014) <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> accessed 7 June 2019.

97 Ioanna Kampouraki, 'ENISA's Opinion Paper on Encryption' (2016) <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption> accessed 7 June 2019.

98 ENISA and Europol, 'ENISA- Europol Issue Joint Statement' (*ENISA*, 23 May 2016) <https://www.enisa.europa.eu/news/enisa-news/enisa-europol-issue-joint-statement> accessed 4 July 2019.

99 Kerr and Schneier (n 24).

100 Later on, DES turned out to be relatively easy to crack, and was replaced by the AES – advanced encryption standard.

101 Computer Security Division, Information Technology Laboratory, 'Crypto Standards Development Process | CSRC' (*CSRC | NIST*, 24 May 2016) <https://csrc.nist.gov/Projects/Crypto-Standards-Development-Process> accessed 16 July 2019.

(NSA) and the Department of Homeland Security. Cooperation with NSA is especially advised due to its high level of expertise.

The 2019 Guidelines for Using Cryptographic Standards in the Federal Government[102] exhort the government to use cryptography in order to protect important data it stores as part of its daily business. While the report does not address backdoors or access to plaintext, it does provide for key storage principles under section 5.4.3. Some keys might have to be stored for longer periods of time should there be a legal order to decrypt text. However, the report also addresses an older standard which would have enabled key escrow if it had been implemented. The use of such a standard as part of an algorithm, called Skipjack, is disallowed, according to section 3.2.1.4.[103]

3.4. OTHER UPCOMING INITIATIVES BY REGIONAL ORGANISATIONS

In the wake of the digital economy, several other regional international organisations are adopting, or considering adopting, relevant legislation on encryption, either in a data protection context or as part of cybersecurity measures.

MERCOSUR, i.e. the Common Southern Market, is a trading bloc in Latin America, established in 1991. Its member states include Argentina, Brazil, Paraguay and Uruguay, with associated countries such as Chile and Peru, thus unifying a major part of South American economies.[104] While MERCOSUR's focus areas are agriculture, social development and human rights, it has recently tackled development and cooperation in the digital economy. It has been noted[105] that MERCOSUR countries are interested in laying down rules on data protection, but a GDPR-type of legislation is considered to be too inflexible. Under current Argentinian leadership, expert groups are consulting on future direction of the organisation's digital agenda,[106] though no legislation

---

102 The Guidelines are not final – a draft version is available for public perusal, and the final version should be available in September 2019. Thelma A Allen, 'Guideline for Using Cryptographic Standards in the Federal Government – Cryptographic Mechanisms: NIST Releases Draft NIST SP 800–175B Rev. 1' (*NIST*, 3 July 2019) <https://www.nist.gov/news-events/news/2019/07/guideline-using-cryptographic-standards-federal-government-cryptographic> accessed 16 July 2019.

103 There have been some allegations that NIST endorses standards, which include a secret backdoor for NSA's exclusive use. Thomas C Hales, 'The NSA Back Door to NIST' (2014) 61 Notices of the American Mathematical Society.

104 'MERCOSUR Official Website' (*MERCOSUR*) <https://www.mercosur.int/en/> accessed 15 July 2019.

105 Kati Suominen, 'Fueling Digital Trade in Mercosur: A Regulatory Roadmap' (*Inter-American Development Bank* 2018) <https://publications.iadb.org/handle/11319/9339> accessed 15 July 2019.

106 'Avanza la agenda digital en el Mercosur' (*MERCOSUR*, 27 June 2019) <https://www.mercosur.int/avanza-la-agenda-digital-en-el-mercosur/> accessed 15 July 2019.

has been proposed yet. Moreover, MERCOSUR is collaborating with the Pacific Alliance, a trading bloc in the same area, on topics such as digital trade and cybersecurity.[107]

ASEAN, Association of Southeast Asian Nations, is an intergovernmental organisation which was set up in 1967.[108] Its 2016–2020 ICT Masterplan, adopted in 2015,[109] lists development of regional data protection principles, as part of establishing information security in the regional framework.[110] However, as per the Masterplan's Annex A, only sharing best practices is currently planned. The adoption of cyber-norms foreseen in the Masterplan would be a major step forward, though its effective use is in doubt due to costly barriers to market entry and lack of user trust into using digital services.[111]

To conclude, while privacy and data protection are strongly recognised human rights at international level, very few legal instruments specifically provide for encryption. Since the 80's, when computers became more ubiquitous, regional instruments on data protection have emerged, such as the APEC Privacy Framework, the Convention 108, and the European Union data protection legislation; however, none of these apply globally. In the next section, three potential pathways to ensure global encryption obligations will be explored.

4. ENABLING GLOBAL ENCRYPTION OBLIGATIONS IN THE ABSENCE OF SPECIFIC TREATY PROVISIONS

4.1. OPTION 1 – A GLOBAL TREATY WITH ENCRYPTION REQUIREMENTS

The first scenario is to have a relevant international organisation (United Nations, International Telecommunications Union) adopt treaty on encryption, which would be open to accession for all states. A provision mandating encryption could also be part of a broader treaty, e.g. on data protection, confidentiality of communications, or a more general instrument on law of ICT or cybersecurity should the UN decide to adopt a treaty on those matters. However, the UN is

107 Mikio Kuwayama, 'Pacific Alliance: A Latin American Version of "Open Regionalism" in Practice' [2019] IDEAS Working Paper Series from RePEc <http://search.proquest.com/docview/2188997245/> accessed 18 July 2019.

108 'ASEAN | One Vision One Identity One Community' (*ASEAN.org*) <https://asean.org/> accessed 16 July 2019.

109 Association of Southeast Asian Nations, 'ASEAN ICT Masterplan 2020 (AIM 2020) – ASEAN THAILAND 2019' (2015) <https://www.asean2019.go.th/en/infographic/asean-ict-masterplan-2020-aim-2020/> accessed 16 July 2019.

110 Ibid pt. 8.1.1.

111 Candice Tran Dai and Miguel Alberto Gomez, 'Challenges and Opportunities for Cyber Norms in ASEAN' (2018) 3 Journal of Cyber Policy 217.

unlikely to adopt a non-binding resolution on end-to-end encryption,[112] let alone adopt a comprehensive treaty (geo- and cyber-political interests would not allow for one).[113]

A potential forum for discussion could be the UNCTAD,[114] the UN Conference on Trade and Development, since its ICT policy work includes data protection, e-commerce and development of the digital economy.[115] Another possible forum is the UNCITRAL, the UN Commission on International Trade Law. The UNCITRAL has adopted the Model Law on Electronic Signatures,[116] which inter alia lays down the rules on signature authenticity, including certificates. It does not, however, contain specific rules on cryptographic techniques or protocols, which are left to national legislation.[117]

However, in order for the UN to adopt a treaty, there must be enough consensus in the General Assembly to pass the vote. Could countries, which use the international forums as a battleground for asserting geopolitical and geostrategic interests, ever agree on issues such as backdoors, access to plaintext, key disclosure and key strength? In the words of Greenleaf – "the likelihood of a new UN treaty being developed from scratch are miniscule"[118]; or, according to Bygrave, there is "realistically, scant chance".[119]

The World Trade Organisation is another potential candidate to adopt a treaty including encryption requirements. One if its policy areas is e-commerce in the context of trade development[120]; however, its progress in legislating has been slow since the 1998 adoption of its ecommerce work programme. Moreover, as Bygrave has noted, any WTO legislation would have a commercial bias,[121] and thus regulate protection of personal data from a trade/competition point of view rather than a human rights one.

---

112 Grant Hodgson, 'Breaking Encryption and Gathering Data: International Law Applications' (2015) 20 Journal of Technology Law & Policy 39.

113 'Data Privacy Law: An International Perspective by Lee Andrew Bygrave' (2014) 25 King's Law Journal 497.

114 'UNCTAD | Home' <https://unctad.org/en/Pages/Home.aspx> accessed 4 July 2019.

115 For example, the UNCTAD has addressed authentication measures, security measures and encryption in Chapter One of its report on e-commerce development: United Nations Conference on Trade and Development, 'Building Confidence – Electronic Commerce and Development' (*UNCTAD*) <https://unctad.org/en/pages/PublicationArchive.aspx?publicationid=1532> accessed 4 July 2019.

116 'UNCITRAL Model Law on Electronic Signatures (2001)' (*United Nations Commission on International Trade Law*) <www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html> accessed 4 July 2019.

117 Apollònia Martínez-Nadal and Josep Lluís Ferrer-Gomila, 'Comments to the UNCITRAL Model Law on Electronic Signatures' in Agnes Hui Chan and Virgil Gligor (eds), *Information Security* (Springer Berlin Heidelberg 2002); United Nations (ed), *UNCITRAL Model Law on Electronic Signatures: With Guide to Enactment 2001* (United Nations 2002).

118 Greenleaf, 'A World Data Privacy Treaty?' (n 5).

119 Lee Andrew Bygrave, 'Data Privacy Law: An International Perspective' (2014) 25 King's Law Journal 497.

120 'WTO | Electronic Commerce Gateway' (*World Trade Organization*) <https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm> accessed 4 July 2019.

121 Bygrave (n 119).

4.2. OPTION 2A – GLOBALISATION BY MEANS OF ACCESSION

As explored above, several regional data protection instruments provide for security requirements, which may specifically include encryption. To globalise an existing treaty or framework, non-regional actors would accede to the treaty according to its rules, thus extend its scope onto a larger scene. According to the Vienna Convention on the law of Treaties,[122] accession is only possible if the treaty implicitly or explicitly provides for it, or if the states signatories agree on it.[123]

The ECOWAS Act does not provide for non-member accession, nor does the APEC Privacy Framework. Unlike them, Convention 108+ allows non-member accession in its Article 27(1), which states that the Committee of Minister of the Council of Europe may invite any non-member state or an international organisation to accede to the Convention. Member states must agree to this accession. So far, only Uruguay has acceded to the treaty, whereas nine non-member states acceded to the 1981 Convention.[124] As already discussed above, the treaty does not explicitly provide for encryption, but it is recommended that data controllers adopt it. Therefore, globalisation of the Convention 108+ could be a viable option to ensure global encryption requirements, although it goes without saying that the economic powers of acceding non-members should be taken into account as well when assessing the Convention's globalisation success.

4.3. OPTION 2B – GLOBALISATION BY GDPR'S 'ADEQUATE PROTECTION' STANDARD

Under Chapter V of the GDPR, there are special rules for transferring personal data outside the EU.[125] There are three possible legal grounds to justify cross-border transfer:

1. transfer based on an adequacy decision,
2. transfer based on appropriate safeguards and
3. transfer based on exemptions for specific situations.

An adequacy decision is a decision by the European Commission that a non-EU country guarantees an adequate level of protection of personal data according to

---

122 Vienna Convention on the Law of Treaties (adopted on 23/5/1969, entered into force on 27/1/1980), UNTS 1155 (Vienna Convention).

123 SeeArticle 15 of the Vienna Convention.

124 'Chart of Signatures and Ratifications of Treaty 223' (*Council of Europe*) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223> accessed 4 July 2019.

125 The GDPR applies also in Norway, Iceland and Liechtenstein, therefore personal data can be transferred to those countries without reference to Chapter V.

the criteria set down in Article 45 of the GDPR, such as the rule of law, respect for human rights and fundamental freedoms, legislation dealing with security, law enforcement access to data, personal data regulation etc., as well as their enforcement in practice, and possible international contractual obligations with regards to personal data protection. One of the criteria is also meeting the requirement of security and confidentiality measures.

As long as these criteria are met, then the personal data flow freely between the EU and the state whose level of protection has been deemed adequate. Currently, these are Andorra, Argentina, Canada (applies only to Canadian commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America.,[126] [127]

Unlike the GDPR, the current proposal for the ePrivacy Regulation, which covers other data involved in a communication context that are not personal data, does not include a similar clause, thus restricting its scope to EU proper instead of globalising its standards.

Nevertheless, there are some possible drawbacks to globalising European standards (Europeanising?) through the Convention 108+ and the GDPR. As Greenleaf points out, there is a pro-European bias in the current enforcement system of the Convention 108+. There is no adjudication forum for non-European countries who accede to the treaty: while European countries, members of the Council of Europe, can be directly challenged in the European Court of Human Rights, the Court's jurisdiction does not extend to non-members regardless of their accession to the Convention 108+, therefore depriving local data subjects of effective remedies against violations of the Convention.[128] Another drawback are data localisation rules, such as data export restrictions in the GDPR's Chapter V. Such rules can bring high costs to outside actors seeking to enter the system and who are not yet compliant with it and may bring welfare losses to national economies.[129]

Moreover, what if a new (cryptographic or other) technology were to emerge; one that is better at promoting human rights than the current encryption requirements imposed by European instruments? Of course, if the security provisions are interpreted broadly enough, then the rules should be flexible

---

126 European Commission, 'Adequacy Decisions' (*European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 4 July 2019.

127 After the invalidation of the Safe Harbour agreement, the US negotiated the Privacy Shield framework, in which participating companies are certified to comply with the criteria laid down by the Federal Trade Commission.

128 Greenleaf, 'A World Data Privacy Treaty?' (n 5).

129 Data localization rules have recently been implemented by inter alia EU, Brazil, China and India. See: Matthias Bauer and others, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (2014) European Centre for International Political Economy <http://hdl.handle.net/10419/174726> accessed 19 July 2019.

enough to accommodate such new technologies; nevertheless, this is a question that can be better answered in the future by case law (especially decisions by the CJEU), further expert work and industry effort.

4.4. OPTION 3 – MAINTAIN THE STATUS QUO

Last but not the least, it may be business as usual for the foreseeable future. In this scenario, the legal frameworks will apply regionally or nationally as currently provided with or without reference to encryption. However, when governments change policies – especially when the government's geo-political weight is significant – the ripple effects emanating from their actions could be sizeable. For example, requiring a foreign company to disclose decryption keys to the law enforcement could lead to loss of consumer trust in confidential communication, and potentially to competitive advantages for domestic companies. Such ripple effects could be mitigated by informal talks and coordination between governments, or by assessing policy impact ahead of its adoption.[130]

5. CONCLUSION

This paper explored instruments, applicable to encryption in an international human rights legal framework, and given the absence of an international encryption treaty, discussed a potential imposition of a binding legal obligation on states to mandate the use of encryption.

First, the connection between encryption, privacy/data protection and human rights was explained. Encryption functions as a measure to prevent unauthorised parties from seeing the data in their plaintext form. It enables safe communications and data transactions. It holds a very important role in a global economy, where data are transferred between different countries with different levels of data protection. Moreover, thanks to these functions, encryption facilitates the exercise of human rights, such as freedom of expression and the right to privacy.

Then, applicable legal instruments were analysed. The elementary texts of human rights law, such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the EU Charter of Fundamental Rights all provide for the right to privacy, including privacy of communications, with the EU Charter also explicitly providing for the right to personal data protection. None of those,

130 Ryan Budish, Herbert Burkert and Urs Gasser, 'Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects' Stanford University 28.

however, mentions explicitly the need for security – let alone encryption – measures.

More detailed rules on data protection were found in regional instruments. This chapter examined the EU framework (GDPR, ePrivacy Directive and the proposed Regulation), Convention 108 of the Council of Europe, the ECOWAS's Model Data Protection Act and the APEC Privacy Framework, as well as some upcoming legislative initiatives by other regional organisations. The EU legal framework specifically refers to encryption as a security or data masking measure, whereas the other instruments require data security measures in general.

Recommendations on encryption by the expert bodies argue for use of encryption in order to facilitate online commerce and data security. The OECD 1997 guidelines provide, however, for potential backdoors or plaintext access by law enforcement, which puts the strength of encryption in jeopardy.

Lastly, a global encryption obligation is discussed – a global treaty, possibly under the United Nations or World Trade Organisation, is unlikely. As an alternative, globalisation of the GDPR or of the Convention 108+ is proposed, although such globalisation does not come without drawbacks, such as bias. Should the states decide to maintain the status quo, further ripple effects of national encryption policies are to be expected.

ACKNOWLEDGEMENT

The research for this paper was carried out as part of a Horizon 2020 research and innovation programme funded by the European Commission under grant agreement No 780108 (FENTEC – Functional ENcryption TEChnologies).

BIBLIOGRAPHY

–, 'APEC Privacy Framework' (*Asia-Pacific Economic Cooperation*) <http://publications.apec.org/Publications/2005/12/APEC-Privacy-Framework> accessed 4 July 2019

–, 'ASEAN | ONE VISION ONE IDENTITY ONE COMMUNITY' (*ASEAN.org*) <https://asean.org/> accessed 16 July 2019

–, 'Asia-Pacific Economic Cooperation' <https://www.apec.org/> accessed 4 July 2019

–, 'Chart of Signatures and Ratifications of Treaty 223' (*Council of Europe*) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223> accessed 4 July 2019

–, 'Crypto Law Survey – Page 2' <www.cryptolaw.org/cls2.htm> accessed 4 March 2019

–, 'Economic Community of West African States (ECOWAS)' <https://www.ecowas.int/> accessed 4 July 2019

–, 'The Encryption Tightrope: Balancing Americans' Security and Privacy | Committee Repository | U.S. House of Representatives' (*U.S. House of Representatives*, 1 March 2016) <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=104573> accessed 4 July 2019

–, 'World Map of Encryption Laws and Policies | Global Partners Digital' <https://www.gp-digital.org/world-map-of-encryption/> accessed 2 July 2019

–, 'UNCTAD | Home' <https://unctad.org/en/Pages/Home.aspx> accessed 4 July 2019

–, 'UNCITRAL Model Law on Electronic Signatures (2001)' (*United Nations Commission on International Trade Law*) <www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html> accessed 4 July 2019

Abelson H and others, 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' (1997) 2 World Wide Web J. 241

Abelson H and others, 'Keys Under Doormats' (2015) 58 Commun. ACM 24

Aljifri H and Sánchez Navarro D, 'International Legal Aspects of Cryptography: Understanding Cryptography' (2003) 22 Computers & Security 196

Allen TA, 'Guideline for Using Cryptographic Standards in the Federal Government – Cryptographic Mechanisms: NIST Releases Draft NIST SP 800–175B Rev. 1' (*NIST*, 3 July 2019) <https://www.nist.gov/news-events/news/2019/07/guideline-using-cryptographic-standards-federal-government-cryptographic> accessed 16 July 2019

Amnesty International, 'Encryption: A Matter of Human Rights' (2016) <https://www.amnesty.nl/content/uploads/2016/03/160322_encryption_-_a_matter_of_human_rights_-_def.pdf?x68337> accessed 16 July 2019

Association of Southeast Asian Nations, 'ASEAN ICT Masterplan 2020 (AIM 2020) – ASEAN THAILAND 2019' (2015) <https://www.asean2019.go.th/en/infographic/asean-ict-masterplan-2020-aim-2020/> accessed 16 July 2019

Baker SA and Hurst PR, *The Limits of Trust : Cryptography, Governments, and Electronic Commerce* (Kluwer law international 1998)

Bauer M and others, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (European Centre for International Political Economy 2014) <http://hdl.handle.net/10419/174726> accessed 19 July 2019

Blind K, 'The Impact of Standardization and Standards on Innovation' (Manchester Institute of Innovation Research 2013) 13/15 <www.innovation-policy.org.uk/compendium/section/Default.aspx?topicid=30> accessed 18 July 2019

Brown (ed.) G, *The Universal Declaration of Human Rights in the 21st Century* (Open Book Publishers 2016)

Budish R, Burkert H and Gasser U, 'Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects' Stanford University 28

Bygrave LA, 'Data Privacy Law: An International Perspective' (2014) 25 King's Law Journal 497

Computer Security Division, Information Technology Laboratory, 'Crypto Standards Development Process | CSRC' (*CSRC | NIST*, 24 May 2016) <https://csrc.nist.gov/Projects/Crypto-Standards-Development-Process> accessed 16 July 2019

Danezis G, Domingo-Ferrer J and Hansen M, 'Privacy and Data Protection by Design – from Policy to Engineering' (ENISA 2014) <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> accessed 7 June 2019

Deeks A, 'The International Legal Dynamics of Encryption' Stanford University 28

Drezner DW, 'Globalization, Harmonization, and Competition: The Different Pathways to Policy Convergence' (2005) 12 Journal of European Public Policy 841

Edwards I, 'GDPR the Security Angle' (2018) 60 ITNOW 42

ENISA and Europol, 'ENISA – Europol Issue Joint Statement' (*ENISA*, 23 May 2016) <https://www.enisa.europa.eu/news/enisa-news/enisa-europol-issue-joint-statement> accessed 4 July 2019

European Commission, 'Adequacy Decisions' (*European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 4 July 2019

G7, 'Outcome Document. Combatting the use of the internet for terrorist and violent extremist content.' (*elysee.fr*) <https://www.elysee.fr/admin/upload/default/0001/04/287b5bb9a30155452ff7762a9131301284ff6417.pdf> accessed 4 July 2019

Gebauer M, 'Unification and Harmonization of Laws', *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2009) <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1123> accessed 4 June 2019

Google, 'Requests for User Information – Google Transparency Report' (*Google*) <https://transparencyreport.google.com/user-data/overview> accessed 4 July 2019

Greenleaf G, 'APEC's Privacy Framework Sets a New Low Standard for the Asia-Pacific' in Andrew T Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law* (Cambridge University Press 2006) <https://www.cambridge.org/core/product/identifier/CBO9780511494208A012/type/book_part> accessed 20 May 2019

Greenleaf G, 'A World Data Privacy Treaty? "Globalisation" and "Modernisation" of Council of Europe Convention 108', Emerging Challenges in Privacy Law: Comparative Perspectives (Cambridge University Press 2014)

Greenleaf G, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' (2012) 2 International Data Privacy Law 68

Gürses S, Kundnani A and Van Hoboken J, 'Crypto and Empire: The Contradictions of Counter-Surveillance Advocacy' (2016) 38 Media, Culture & Society 576

Hales TC, 'The NSA Back Door to NIST' (2014) 61 Notices of the American Mathematical Society

Harding L, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (Vintage Books 2014)

Hodgson G, 'Breaking Encryption and Gathering Data: International Law Applications' (2015) 20 Journal of Technology Law & Policy 39

Hurwitz JG, 'Encryption.Congress Mod (Apple + CALEA).(Communications Assistance for Law Enforcement Act of 1994)' (2017) 30 Harvard Journal of Law & Technology

Joinet L, 'Revised Version of the Guidelines for the Regulation of Computerized Personal Data Files' (United Nations Commission on Human Rights 1990) <http://digitallibrary.un.org/record/43365> accessed 17 July 2019

Jones ML, 'The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 Social Studies of Science 216

Kampouraki I, 'ENISA's Opinion Paper on Encryption' (2016) <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption> accessed June 7 2019

Kaye D, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (United Nations Human Rights Council 2015) A/HRC/29/32 <www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc> accessed 28 June 2019

Kerr OS and Schneier B, 'Encryption Workarounds' (2018) 106 Georgetown Law Journal

Kuwayama M, 'Pacific Alliance: A Latin American Version of"Open Regionalism"in Practice' [2019] IDEAS Working Paper Series from RePEc <http://search.proquest.com/docview/2188997245/> accessed 18 July 2019

Landau S, *Listening in: Cybersecurity in an Insecure Age* (Yale University press 2017)

Landau S and Diffie W, *Privacy on the Line* <https://mitpress.mit.edu/books/privacy-line> accessed March 5 2019

Lin HS, 'Cryptography and Public Policy' (1998) 25 Journal of Government Information 135

Lloyd S and Adams C, 'Key Management' in Henk CA van Tilborg and Sushil Jajodia (eds), *Encyclopedia of Cryptography and Security* (Springer US 2011) <https://doi.org/10.1007/978–1–4419–5906–5_85> accessed 6 June 2019

Martínez-Nadal A and Ferrer-Gomila JL, 'Comments to the UNCITRAL Model Law on Electronic Signatures' in Agnes Hui Chan and Virgil Gligor (eds), *Information Security* (Springer Berlin Heidelberg 2002)

Mason S, 'Digital Signatures', *Electronic Signatures in Law* (School of Advanced Study, University of London 2016)

Mercosur, 'Avanza la agenda digital en el Mercosur' (*MERCOSUR*, 27 June 2019) <https://www.mercosur.int/avanza-la-agenda-digital-en-el-mercosur/> accessed 15 July 2019

Mercosur, 'MERCOSUR Official Website' (*MERCOSUR*) <https://www.mercosur.int/en/> accessed 15 July 2019

Moody G, 'Nobody Saw This Coming: Now China Too Wants Company Encryption Keys And Backdoors In Hardware And Software' (*Techdirt.*, 29 January 2015) <https://www.techdirt.com/articles/20150129/06262129848/nobody-saw-this-coming-now-china-too-wants-company-encryption-keys-backdoors-hardware-software.shtml> accessed 4 July 2019

Olsen M, Schneier B and Zittrain J, 'Don't Panic: Making Progress on the "Going Dark" Debate' (The Berkman Centre for Internet & Society 2016)

Organisation for Economic Cooperation and Development, 'OECD Guidelines for Cryptography Policy – OECD' (*OECD.org*) <https://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm> accessed 4 July 2019

Orji UJ, 'Regionalizing Data Protection Law: A Discourse on the Status and Implementation of the ECOWAS Data Protection Act' (2017) 7 International Data Privacy Law 179

Rotenberg M, Schwartz PM and Solove DJ, *Information Privacy Law* (2nd ed., Aspen 2006)

Schneier B, 'Essays: Why We Encrypt' (*Schneier on Security*, June 2015) <https://www.schneier.com/essays/archives/2015/06/why_we_encrypt.html> accessed 17 July 2019

Schneier B, 'The Importance of Strong Encryption to Security' (*Schneier on Security*) <https://www.schneier.com/blog/archives/2016/02/the_importance_.html> accessed 27 March 2019

Schneier B, Seidel K and Vijayakumar S, 'A Worldwide Survey of Encryption Products' (Social Science Research Network 2016) SSRN Scholarly Paper <https://papers.ssrn.com/abstract=2731160> accessed 18 July 2019

Scholl M and others, 'An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule' (National institute of standards and technology 2008) <https://csrc.nist.gov/publications/detail/sp/800–66/rev-1/final> accessed 19 July 2019

Software Freedom Law Center India, 'FAQ: Legal Position of Encryption in India' (*SFLC.in*) <https://sflc.in/faq-legal-position-encryption-india> accessed 4 July 2019

Spindler G and Schmechel P, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 Journal of Intellectual Property, Information Technology and Electronic Commerce Law [i]

Suominen K, 'Fueling Digital Trade in Mercosur: A Regulatory Roadmap' (Inter-American Development Bank 2018) <https://publications.iadb.org/handle/11319/9339> accessed 15 July 2019

Swire P and Ahmad K, 'Encryption and Globalization' (2011) 23 Columbia Science and Technology Law Review

Tran Dai C and Gomez MA, 'Challenges and Opportunities for Cyber Norms in ASEAN' (2018) 3 Journal of Cyber Policy 217

United Nations (ed), *UNCITRAL Model Law on Electronic Signatures: With Guide to Enactment 2001* (United Nations 2002)

United Nations Conference on Trade and Development, 'Building Confidence – Electronic Commerce and Development' (*UNCTAD, 2000*) <https://unctad.org/en/pages/PublicationArchive.aspx?publicationid=1532> accessed 4 July 2019

Van Alsenoy B, 'Regulating Data Protection : The Allocation of Responsibility and Risk among Actors Involved in Personal Data Processing' (Doctoral thesis, KU Leuven 2016)

Van Hoboken J and Schulz W, 'Human Rights and Encryption – UNESCO Digital Library' (2016) <https://unesdoc.unesco.org/ark:/48223/pf0000246527> accessed 31 January 2019.

Van Hoboken JVJ, 'Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era Symposium: Who's Governing Privacy: Regulation and Protection in a Digital Era' (2013) 66 Maine Law Review 487

Voigt P and von dem Bussche A, 'Organisational Requirements' in Paul Voigt and Axel von dem Bussche (eds), *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer International Publishing 2017) <https://doi.org/10.1007/978–3–319–57959–7_3> accessed 16 May 2019

Williams LC, 'Edward Snowden Says Encryption Is The Only Way To Counter Mass Surveillance' (*ThinkProgress*, 10 March 2014) <https://thinkprogress.org/edward-

snowden-says-encryption-is-the-only-way-to-counter-mass-surveillance-ee450433dca8/> accessed 4 July 2019

Wong JI, 'Here's How Often Apple, Google, and Others Handed over Data When the US Government Asked for It' (*Quartz*, 19 February 2016) <https://qz.com/620423/heres-how-often-apple-google-and-others-handed-over-data-when-the-us-government-asked-for-it/> accessed 4 July 2019

WTO, 'WTO | Electronic Commerce Gateway' (*World Trade Organization*) <https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm> accessed 4 July 2019

Zotos K and Litke A, 'Cryptography and Encryption' [2005] arXiv <http://arxiv.org/abs/math/0510057> accessed 4 March 2019

Zuiderveen Borgesius F J and Steenbruggen W, 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust' (2019) 20 Theoretical Inquiries in Law 291.