'Online Anonymity in the Modern Digital Age: Quest for a Legal Right'

Dr. Evgeni Moyakine[1]

1. Introduction

Currently, we live in an undeniably interconnected world characterised by heavy reliance on the Internet and related infrastructures that can be used and abused by not only individuals, but also governments, corporations, criminal and terrorist organisations and others. In such challenging climate, it is essential to be aware of the importance of freedom of opinion and expression and the fundamental rights to privacy and data protection. These human rights standards are necessary for the realisation of other human rights offering protection to European citizens and enable them to pursue a sufficiently high level of life when they enter the borderless realm of the World Wide Web. In this regard, in addition to encryption online anonymity is a core concept in protecting these and other fundamental rights that deserve a close scrutiny.

Anonymity stems from the Greek word 'anonymia' meaning 'without a name' or 'namelessness' and can be qualified as 'a condition of avoiding identification'[2]. Pseudonymity is 'a variety of anonymity' meaning the use of a false name as a substitute for the real name for hiding one's identity.[3] Anonymity as such enables individuals to carry out their activities in public places without being identified. In essence, anonymity online means that an individual acts or communicates on the Web and does not use his or her own name or identity, uses a substitute name making his or her own name unidentifiable or the real name or identity are protected and cannot be determined.[4] Without any doubt, anonymity of Internet users is of significance to any free and democratic society. After the events of 11 September 2001, one can perceive, however, much suspicion on the part of governments and efforts to not only increase security, but also to establish identity of individuals using the Internet.[5] In this regard, the use of a variety of identification technologies, such as voice and facial recognition relying on the use of biometric data, has become significantly widespread.[6] After the recent terrorist attacks in Paris and Brussels, there are more prominent signs of governments' intentions – such as those voiced in the United Kingdom and France – to introduce far-going surveillance mechanisms on the Internet, significantly restrict anonymity of online users and limit their right to privacy.[7] In the society where information about individuals can be collected, stored and

---

[1] Postdoctoral Researcher, STeP ('Security, Technology and e-Privacy' Research Group), the University of Groningen.

[2] UN Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, p. 4, par. 9.

[3] Lilian Edwards and Geraint Howells, 'Anonymity, Consumers and the Internet: Where Everyone Knows You're a Dog' in Chris Nicoll, Corien Prins and Miriam van Dellen (eds), *Digital Anonymity and the Law: Tensions and Dimensions* (TMC Asser Press 2003), p. 213.

[4] Electronic Frontier Foundation, 'Anonymity and Encryption: Comments Submitted to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (10 February 2015) <http://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf> accessed 7 January 2016.

[5] Craig R. Scott, 'Benefits and Drawbacks of Anonymous Online Communication: Legal Challenges and Communicative Recommendations' (2004) 41(1) Free Speech Yearbook, p. 127.

[6] Gary T. Marx, 'Identity and Anonymity: Some Conceptual Distinctions and Issues for Research' in Jane Caplan and John Torpey (eds), *Documenting Individual Identity: The Development of State Practices in the Modern World* (Princeton University Press 2001) (available at <http://web.mit.edu/gtmarx/www/identity.html>), pp. 311-327.

[7] Alex Hern, 'How Has David Cameron Caused a Storm over Encryption?' (*The Guardian*, 15 January 2015) <http://www.theguardian.com/technology/2015/jan/15/david-cameron-encryption-anti-terror-laws> accessed 8 June 2016; Amnesty International, 'France: New Surveillance Law a Major Blow to Human Rights' (24 July 2015) <https://www.amnesty.org/en/latest/news/2015/07/france-new-surveillance-law-a-major-blow-to-human-rights/> accessed 7 January 2016; Arik Hesseldahl, 'France Has a Powerful and Controversial New Surveillance Law'

processed with ease, this practice certainly constitutes a matter of major concern. Therefore, a pertinent question arises as to whether there is indeed a legal right to online anonymity that can offer a reasonably high degree of protection to Internet users and guarantee their security. By exploring whether a right or an emerging right to anonymity online can be identified as a fundamental right under international law, the current contribution draws attention to the fact that some traces of this right can be identified in international law, establishes its acceptance level and elaborates on its interplay with freedom of expression and the rights to privacy and data protection. It is done by adopting literature review as the main legal research method that is potentially capable of unravelling the truth regarding the right of online users to be and remain anonymous on the Internet.

2. Online anonymity

It is not an overstatement to say that the Internet has been incorporated in practically every aspect of our life, has drastically changed the way in which individuals interact and communicate with each other and has developed into a crucial tool for not only accessing information but also making it available to others: what is certain, is that there is no turning back to this development. This extremely advanced 'network of networks' is comprised of a variety of interconnected networks consisting of uncountable computers.[8] As noted by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue 'the Internet is one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies'.[9]

Anonymity as a concept is essential to the realisation of human rights and fundamental freedoms: in particular, it plays an important role for the protection of the freedom of expression and the rights to privacy and data protection. Traditionally, privacy and data protection rights are considered to be at the core of the protection of anonymity on the Internet.[10] Willing to safeguard privacy interests and seeking to protect personal data, individuals engaging in online interactions need to remain unidentified and to have their personal information hidden from others. Anonymity can also be seen as a specific characteristic of online communications and a crucial element of freedom of expression that facilitates a free and undisturbed flow of personal and other data of Internet users.[11] By being anonymous online, individuals can voice their opinions even on ideas that are unpopular, express themselves in a variety of ways and engage in different types of interactions on the World Wide Web without having to fear that their privacy and data protection rights would be violated. Using Internet services nowadays is, however, by no means a completely anonymous activity.[12]

(*Recode.net*, 14 November 2015) <http://recode.net/2015/11/14/france-has-a-powerful-and-controversial-new-surveillance-law/> accessed 7 January 2016.

[8] Janice C. Dowd, 'Preface' in Janice C. Dowd (ed), *Internet Issues and Trends: Selected Analyses* (Nova Science Publishers 2014), p. vii.

[9] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue' (16 May 2011) UN Doc. A/HRC/17/27, p. 4.

[10] ARTICLE 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity Online' (February 2015) available at <http://www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 7 January 2016, p. 7.

[11] Lisa Collingwood, 'Privacy, Anonymity and Liability: Will Anonymous Communications Have the Last Laugh?' (2012) 28 Computer Law & Security Review, pp. 328-329.

[12] Rolf H. Weber and Ulrike I. Heinrich, *Anonymization* (SpringerBriefs in Cybersecurity, Springer 2012), p. 11.

Online anonymity is endangered by a variety of measures that are taken by public and private actors. First of all, Internet users can be identified by their IP addresses.[13] Additionally, anonymity of online users is threatened by data retention practices that often lead to storage of personal data, which allows identification of individuals.[14] Also, low levels of information security and lack of or insufficient security measures ensuring protection of data lead to the decrease in online anonymity.[15] Therefore, in order to protect anonymity those who use Internet services should be aware of data protection pitfalls and take all necessary steps in order to improve online security.

It stands to reason that it is possible to achieve online anonymity by different means. One of the most efficient and effective ways is the process of implementing encryption constituting a powerful technical instrument capable of ensuring freedom of expression and privacy and data protection rights online by protecting confidentiality of data or Internet communications. It can be defined as 'the process of encoding or "scrambling" the contents of any data or voice communication with an algorithm (a mathematical formula) and a randomly selected variable associated with the algorithm, known as a "key".[16] The main purpose of this encoding process is to make data readable by only intended recipients and not by those who do not have access permission.[17] Logically, recipients are capable of reading this information only after having decrypted it. Regarding the role played by both anonymity and encryption in the modern society, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, was quite clear:

> Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression.[18]

As stressed by Professor Joseph Cannataci, the first and only UN Special Rapporteur on the Right to Privacy in the Digital Age, encryption is an essential tool in the struggle of protecting the right to privacy and the year 2014 can truly be referred to as the year of encryption.[19] The same idea is applicable to the year 2015 and even more so to the year 2016 bringing new challenges to the protection and respect of the right to privacy. Notably, Apple as a representative of the industry is perfectly aware of this fact: its CEO Tim Cook has recently indicated strong commitment of the tech giant towards implementing encryption on its devices and providing encryption for its services in order to ensure that privacy of Apple's clients is respected.[20] Subsequently, Apple put its money where its mouth is and took a firm position with regard to the requests from the FBI by refusing to unlock the iPhone 5C used by the San

---

[13] Rolf H. Weber and Ulrike I. Heinrich, *Anonymization* (SpringerBriefs in Cybersecurity, Springer 2012), pp. 11-12.
[14] Ibid, p. 13.
[15] Ibid, pp. 13-15.
[16] David Banisar, 'Stopping Science: The Case of Cryptography' (1999) 9 Health Matrix, p. 253.
[17] SANS Institute, 'History of Encryption' (2001) available at <https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730> accessed 2 July 2016.
[18] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, p. 3.
[19] As emphasised by Professor Joseph Cannataci at the annual congress of PI.lab 'Privacy as Opportunity' held in Utrecht, the Netherlands, on 11 December 2015.
[20] Trevor Timm, 'Apple's Tim Cook Defends Encryption. When Will Other Tech CEOs Do So?' (*The Guardian*, 23 December 2015) <http://www.theguardian.com/commentisfree/2015/dec/23/apple-tim-cook-defends-encryption-when-will-other-tech-ceos-do-so> accessed 24 December 2015.

Bernardino shooter, to grant access to his personal data and to introduce a backdoor into Apple's systems for surveillance of data of Apple's clients. While this situation led to a legal dispute between Apple and the FBI, the latter dropped its case against the Cupertino company given that it was granted access to the suspect's phone with help of a third party.[21] Being aware of importance of encryption techniques to the use of modern technology, WhatsApp has adopted a policy of end-to-end encryption not only in relation to messages sent between its users, but also files including photographs and video.[22] While major companies seem to understand the importance of encryption and online anonymity, the Internet Right Charter of the Association for Progressive Communications (hereinafter: APC) also refers to the right to use encryption and provides that individuals engaging in online communications are entitled to the right to make use of encryption tools ensuring 'secure, private and anonymous communication'.[23]

Other means to achieve anonymity online could include the use of virtual private network connections, proxy servers, Tor, https:// protocols and other possible technical solutions that are aimed at making Internet users anonymous and thus hiding their identity from others. These tools are currently used with mixed results. While the Internet is characterised by its relative anonymity,[24] it is certain that no technical instrument is capable of guaranteeing 100% anonymity of online users and it is a matter of time, invested effort and other allocated resources, such as finances, to reveal a person's identity.

3. Two sides of one coin

On the one hand, anonymity is essentially a useful means for individuals to exercise their civil and political rights when they need to remain unidentified, such as in cases of protecting privacy or even fighting against dictatorships and tyranny and preventing retaliation or persecution. Anonymity and pseudonymity have been and still are of crucial importance to many people around the world. In 1787, Alexander Hamilton, James Madison and John Jay used a pseudonym 'Publius' to write and publish the *Federalist Papers* that significantly contributed to American political thought and to the adoption of the US Constitution.

Different ways in which anonymity can be used for the purposes of exercising freedom of expression are especially evident in the current society where the use of the Internet and digital communications stimulates people to express their opinions and share thoughts online or hurt feelings of others and spread hate and violence. It is obvious that when anonymity of communications online or offline is ensured, individuals can exercise their freedom of expression and express opinions and ideas without any fear for being censored.[25] Additionally and importantly, individuals might desire to remain anonymous in order to protect their privacy and anonymisation is necessary to protect personal data when it is handled by data controllers and processors. Gary Marx provides a summary of reasons why anonymity and thus also online

[21] Trevor Timm, 'The FBI May Have Dropped One Case Against Apple, but the Battle is Far from Over' (*The Guardian*, 29 March 2016) <http://www.theguardian.com/commentisfree/2016/mar/29/fbi-apple-case-dropped-san-bernardino-iphone-far-from-over> accessed 7 April 2016.

[22] Russell Brandom, 'WhatsApp is Now Entirely End-to-end Encrypted' (*The Verge*, 5 April 2016) <http://www.theverge.com/2016/4/5/11370106/whatsapp-messenger-end-to-end-encryption-open-whisper> accessed 7 April 2016.

[23] APC, *Internet Rights Charter* (November 2006) available at <https://www.apc.org/node/5677> accessed 3 January 2016, Section 5.3.

[24] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue' (16 May 2011) UN Doc. A/HRC/17/27, p. 7.

[25] Adam D. Moore, *Privacy Rights: Moral and Legal Foundations* (The Pennsylvania State University Press 2010), p. 134; UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, pp. 5-6.

anonymity deserve attention in our society and need to be realised and protected.[26] According to him, full or partial anonymity is necessary in order to, *i.a.*, 1) facilitate the free flow of information and communication on public matters; 2) obtain personal information for research purposes when the identity of individuals must be hidden; 3) focus attention on the content of a message and behaviour in question rather than the source and its characteristics; 4) stimulate collection and sharing of information, communication, reporting regarding sensitive and personal matters; 5) protect individuals who take certain actions, such as donors, from subsequent obligations and other forms of contact; 6) protect strategic economic interests as a buyer or as a seller; 7) protect individuals from unwanted intrusions in their private sphere; 7) protect reputation and assets; 8) avoid persecution; 9) protect personhood and autonomy of a person by respecting that person's dignity and guaranteeing protection of his or her personal information.

On the other hand, there are also individuals or groups who engage in unlawful activities and wish to remain hidden from the authorities and the public eye. Anonymity enjoyed by individuals online is 'a great tool for evading detection of many varieties of illegal and immoral activity'.[27] Terrorists, criminals and others use anonymity in order to stay below the radar of governments that are unable to detect and prevent crimes of these individuals and protect human rights of their citizens.[28] In Australia, for example, anonymity of Internet users facilitates the sale of drugs and makes it possible to use them without being criminally prosecuted.[29] The situation in other countries is often also quite complicated when individuals are involved in the commission of similar or other crimes and manage to escape any responsibility.

4. Legal right

In the first instance, before investigating the acceptance of the right to online anonymity at the international level it needs to be determined what the notion of 'a legal right' adopted in the current research actually entails. Legal rights are essentially entitlements to something and imply the availability of enforceable obligations created by law and imposed on others who have to act in a certain way toward the owners of those rights.[30] In contrast to a legal right, a natural or moral right means a moral duty of others in relation to the owner of this right and not a duty recognised by law. Therefore, in order to maintain appropriate focus on the essence of the right to online anonymity and not to engage in a lengthy philosophical discussion on the nature of moral rights, the concept of a legal right will be used throughout this contribution.

Under international law, including global and regional human rights treaties and European Union law, the rights to privacy and data protection and freedom of expression have been recognised to a certain extent and are protected by various legal instruments that will be addressed below. In many domestic jurisdictions, one can also find legal rules and principles relating to these rights. A brief examination of the current state of affairs reveals that the right to online anonymity does not constitute a codified legal right, which can be found in an international treaty. There can be, however, legal acts and policies at the domestic level of States

[26] Gary T. Marx, 'Identity and Anonymity: Some Conceptual Distinctions and Issues for Research' in Jane Caplan and John Torpey (eds), *Documenting Individual Identity: The Development of State Practices in the Modern World* (Princeton University Press 2001) (available at <http://web.mit.edu/gtmarx/www/identity.html>), pp. 316-318.
[27] A. Michael Froomkin, 'Anonymity in the Balance' in Chris Nicoll, Corien Prins and Miriam van Dellen (eds), *Digital Anonymity and the Law: Tensions and Dimensions* (TMC Asser Press 2003), p. 7.
[28] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, p. 6.
[29] Amy Phelps and Allan Watt, 'I Shop Online – Recreationally! Internet Anonymity and Silk Road Enabling Drug Use in Australia' (2014) 11 *Digital Investigation.*
[30] Samuel Dorner, 'What is a Right?', (1996) 30 The Journal of Value Inquiry, p. 428.

covering this right or evidence of the emerging right of online anonymity found in customary international law. The aim is to identify this right in its current form or to predict whether and in which form it will emerge in the future.

5. Online anonymity and international law

In the process of identifying the right to online anonymity in the body of contemporary international law, one needs to devote significant attention to the sources of international law that might contain this right or indicate its development and possible future recognition. There are four sources of international law that are taken into account by the International Court of Justice in The Hague deciding disputes in cases brought before it.[31] These sources are international treaties of general or specific character, customary international law, the general principles of law that are recognised by civilised nations and finally judicial decisions and the teachings of the most qualified publicists used as subsidiary means to determine rules and principles of international law. In the current contribution, judicial decisions of international and national judicial bodies and publications of various authors are used to trace the right to online anonymity while the main focus is put on international conventions, customary international law and the general principles of law.

5.1. International legal instruments and the right to online anonymity

Although the right to online anonymity has not explicitly been codified at the international level[32], an attempt can be made to deduce it from international and regional human rights instruments that concern freedom of opinion and expression and the rights to privacy and data protection.[33] The discussion will be focussed on legal documents at different levels: the United Nations, the Organisation for Economic Co-operation and Development (hereinafter: OECD), the Council of Europe (hereinafter: CoE), the European Union, the Organization of American States, the African Union and the Association of the Southeast Asian Nations (hereinafter: ASEAN).

Investigation into the roots of the right of online anonymity should commence at the level of the United Nations where legal instruments exist protecting these interrelated rights that often have to be balanced against each other. Internationally, the right to privacy is in the first instance protected by Article 12 of the Universal Declaration of Human Rights (hereinafter: UDHR)[34] providing that no one may be subjected to arbitrary interference with his or her privacy, family, home or correspondence, nor to attacks in relation to his honour and reputation. Importantly, this provision states that every individual has the right to protection by law against these types of interference or attack. Article 17 of the International Covenant on Civil and Political Rights (hereinafter: ICCPR)[35] basically reflects Article 12 UDHR and adds that interferences and attacks can be not only arbitrary but also unlawful.

Other UN human rights treaties build upon Article 12 UDHR and Article 17 ICCPR. Article 16 of the Convention on the Rights of the Child (hereinafter: CRC)[36] concerns the right of children

[31] See Article 38 Paragraph 1of the Statute of the International Court of Justice.
[32] Rolf H. Weber and Ulrike I. Heinrich, *Anonymization* (SpringerBriefs in Cybersecurity, Springer 2012), p. 23.
[33] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, p. 6.
[34] Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III).
[35] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.
[36] Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3.

not to be subjected to arbitrary or unlawful interference with their privacy, family or correspondence and to unlawful attacks on their honour and reputation. Article 22 of the Convention on the Rights of Persons with Disabilities (hereinafter: CRPD)[37] also ensures respect of the right to privacy for persons with disabilities. Importantly, while the First Paragraph of this Article essentially mirrors Paragraphs 1 and 2 of Article 17 ICCPR specifying that it involves interference with not only privacy, family, home or correspondence but also other types of communication. In addition, the Second Paragraph of Article 22 CRPD requires States to protect the privacy of personal, health and rehabilitation information of disabled persons on an equal basis with others. Finally, Article 14 of the Convention on the Protection of the Rights of all Migrant Workers and Members of Their Families (hereinafter: Migrant Workers Convention)[38] also builds upon Article 17 ICCPR and similarly to the CRPD adds that arbitrary and unlawful interference can be with other communications in addition to privacy, family and correspondence of individuals.

The freedom of opinion and expression is incorporated in Article 19 UDHR and Article 19 ICCPR. Article 19 UDHR specifically declares that this provision includes the right to seek, receive and impart information and ideas through any media. Other human rights treaties also contain similar references. Article 19 ICCPR maintains that the right to freedom of expression includes freedom to seek, receive and impart information and ideas of all possible kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. Article 13 CRC, Article 21 CRPD and Article 13 of the Migrant Workers Convention also focus on the freedom of expression and opinion and access to information and include all possible forms of communication that can be used to exercise this particular freedom.

At the level of the United Nations, there are the Guidelines for the Regulation of the Computerized Personal Data Files adopted by the UN General Assembly in 1990. They contain principles regarding minimum guarantees that should be provided by States at the domestic level, but do not establish binding State obligations. Importantly, this document makes a reference to the principle of security requiring authorities to adopt appropriate measures aimed at protecting computerised personal data files against natural dangers, including accidental loss or destruction, and human dangers, such as unauthorised access and fraudulent misuse of data.[39] Also, the principle of transborder data flows implies that information can be circulated freely between two or more States as this circulation takes place inside a territory of one of these States when the legislation of these countries offers comparable standards of privacy protection.[40] The Guidelines specify the scope of their application by stressing that these two and other principles need to be made applicable to all public and private computerised files. States do have an option to extend the reach of these principles to manual files and make them applicable to files on legal persons containing personal information. Finally, the Guidelines also apply to personal data files kept by governmental international organisations.

OECD

Within the framework of the OECD, there is a set of non-binding Guidelines on the Protection of Privacy and Transborder Flows of Personal Data that were adopted in 1980 and revised in

[37] Convention on the Rights of Persons with Disabilities (adopted 13 December 2006) UN Doc. A/RES/61/106.
[38] International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families (adopted 18 December 1990) UN Doc. A/RES/45/158.
[39] UN General Assembly, 'Guidelines for the Regulation of Computerized Personal Data Files', adopted by UN General Assembly Resolution 45/95 (14 December 1990) (available at <http://www.refworld.org/pdfid/3ddcafaac.pdf>), Principle 7: Principle of Security.
[40] Ibid, Principle 9: Transborder Data Flows.

2013.[41] This document provides several principles with respect to the protection of privacy and data protection. While this is clearly a non-binding legal tool, OECD Member States are expected to observe these guidelines and implement them at the national level and many legislators have been inspired by them.

Council of Europe

The CoE comprises 47 European States and is an international organisation with significant influence. Under its auspices, the main European human rights treaty and other conventions focusing on the protection of personal data and other matters were adopted. Article 8 of the European Convention on Human Rights (hereinafter: ECHR)[42] specifically concerns the right of individuals to respect for their private and family life, home and correspondence. The notion of private life is fairly broad and cannot be exhaustively defined.[43] It includes the privacy of communications, covering security and privacy of email, telephone, mail and other communication means and information derived from monitoring and examining Internet usage.[44] Importantly, Article 8 ECHR protects the right to personal development and the right to establish and develop relationships with other people and the outside world.[45] In addition, Article 8 ECHR has been interpreted by the European Court of Human Rights (hereinafter: ECtHR) as to also include the right to data protection that is crucial to a person's enjoyment of the right to private and family life.[46] The right to freedom of expression has been laid down in Article 10 ECHR. This provision contains a reference to the freedom to receive and impart information and ideas, similar to the UDHR and ICCPR. In its case-law, the ECtHR has stressed that the Internet is nowadays one of the most important means of exercising the right to freedom of expression and information.[47] Sometimes, the right to privacy and freedom of expression need to be balanced, especially when the privacy rights and the right of the public to be informed are at stake.[48]

In addition, the Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data[49] adopted under the auspices of the CoE seeks to ensure respect for fundamental rights and freedoms, in particular the right to privacy, with respect to automatic processing of personal data to every individual residing in the territory of States Parties.[50] Automatic processing means, among other things, storage, retrieval and dissemination of data

---

[41] OECD, 'The OECD Privacy Framework' (2013) (available at <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>).

[42] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols nos 11 and 14 (4 November 1950) ETS 5 (Council of Europe, ECHR) (available at <http://www.echr.coe.int/Documents/Convention_ENG.pdf>).

[43] *S. and Marper v. the United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008), par. 66.

[44] *Halford v. the United Kingdom* App no 20605/92 (ECtHR, 25 June 1997), par. 44; *Copland v. the United Kingdom* App no 62617/00 (ECtHR, 3 April 2007), par. 41.

[45] *S. and Marper v. the United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008), par. 66.

[46] *Klass v. Germany* App no 5029/71 (ECtHR, 6 September 1978); *Malone v. the United Kingdom* App no 8691/79 (ECtHR, 2 August 1984); *Leander v. Sweden* App no 9248/81 (ECtHR, 26 March 1987). See also *Z. v. Finland* App no 22009/93 (ECtHR, 25 February 1997) where the ECtHR used the notion of personal data protection for the first time.

[47] *Times Newspapers Ltd. v. the United Kingdom* App nos 3002/03 and 23676/03 (ECtHR, 10 March 2009), par. 27; *Ahmet Yildirim v. Turkey* App no 3111/10 (ECtHR, 18 December 2012), para. 48-49.

[48] See, for instance, *Von Hannover v. Germany* App nos 59320/00 and 30566/04 (ECtHR, 24 June 2004) para. 59-60.

[49] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (28 January 1981) CETS No. 108 (Council of Europe, Convention No. 108) (available at <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>).

[50] Article 1 Convention No. 108.

carried out in whole or in part by automated means.[51] According to Article 3 Paragraph 1, States are required to comply with their obligations under the Convention with regard to automated personal data files and automatic processing of personal data in both public and private sectors. As part of their duties, they must take appropriate security measures for protecting personal data stored in automated data files against accidental and unauthorised destruction; accidental loss; unauthorised access, alteration or dissemination.[52]

The Convention on Cybercrime is another international convention adopted within the framework of the CoE.[53] Its scope of application is limited to crimes committed via the Internet and other computer networks and it is acknowledged that there is a need to find a proper balance between the interests of law enforcement and the respect for fundamental rights, including the right to privacy and the right to freedom of expression.[54] While the Convention emphasises that powers and procedures provided for the purpose of criminal investigations or proceedings must be respectful of human rights standards and offer an adequate level of protection[55], it provides that States shall adopt legislative and other measures necessary for real-time collection of traffic data[56] and interception of content data[57].

Supporting the idea of avoiding identification by online users, in 2003, the Committee of Minsters of the Council of Europe (hereinafter: CoE) addressed the principle of anonymity in its declaration on freedom of communication on the Internet. The declaration provides that 'in order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity'.[58] While the will of Internet users to remain anonymous and not to reveal their identity is to be respected by the CoE Member States, these States are not prevented from taking measures and cooperating with each other in order to find and bring to justice individuals involved in criminal activities when it is done in accordance with their national laws, the ECHR and other international agreements.

European Union

In the EU, Article 7 of the Charter of Fundamental Rights of the European Union (hereinafter: EU Charter)[59] addresses the right to privacy. The right to data protection as a separate right has been laid down in Article 8 of the EU Charter and Article 16 Paragraph 1 of the Treaty on the Functioning of the European Union[60]. Article 11 of the EU Charter concerns the right to freedom of expression and it is recognised that freedom of expression is a universal right equally applicable to all individuals.[61] It must be protected and respected everywhere – offline and online – and in relation to everyone.

---

[51] Article 2 (c) Convention No. 108.
[52] Article 7 Convention No. 108.
[53] Convention on Cybercrime (23 November 2001) CETS No. 185 (Council of Europe, Convention on Cybercrime) (available at <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>).
[54] Preamble of the Convention on Cybercrime.
[55] Article 15 Paragraph 1 Convention on Cybercrime.
[56] Article 20 Convention on Cybercrime.
[57] Article 21 Convention on Cybercrime.
[58] Declaration on Freedom of Communication on the Internet, adopted by the Committee of Ministers on 28 May 2003 (Council of Europe) (available at <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805dfbd5>), Principle 7: Anonymity.
[59] Charter of Fundamental Rights of the European Union [2012] OJ C326/391.
[60] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47.
[61] EU Human Rights Guidelines on Freedom of Expression Online and Offline (12 May 2014) (Council of the European Union, Foreign Affairs Council Meeting) (available at

Furthermore, secondary EU legislation specifically deals with privacy and data protection issues of personal data processing and online communications. This legal framework has significantly been changed after years of being reviewed. In 2012, the European Commission introduced a data protection reform package including a proposal for the new regulation and directive.[62] The new General Data Protection Regulation is essentially replacing the Directive 95/46/EC and has entered into force on 24 May 2016.[63] It will be directly applicable and legally binding in its entirety in all EU countries two years after entering into force or on 25 May 2018. The Police and Criminal Justice Data Protection Directive is repealing the Council Framework Decision 2008/977/JHA and entered into force on 5 May 2016.[64] The Directive requires implementation by EU Member States and needs to be transposed into their national legislation, regulations and administrative practices within two years after entering into force or before 6 May 2018.

Both the Regulation and the Directive encourage the use of pseudonymisation and encryption. Pseudonymisation contributes to the reduction of risks to data subjects and help data controllers and data processors to meet their obligations.[65] In this regard, controllers are natural or legal persons, competent authorities or other bodies that determine the purposes and means of the processing of personal data.[66] Processors are natural or legal persons, competent authorities or other bodies that process personal data on behalf of controllers.[67] Both legislative acts underline the importance of data protection by design and by default and oblige data controllers to implement all appropriate technical and organisational measures, such as pseudonymisation, in order to comply with data protection principles in an effective manner and to introduce necessary safeguards into the processing of personal data.[68] Moreover, the Regulation specifically mentions pseudonymisation and encryption as instruments to be implemented by controllers and processors in the processing of personal information. Additionally, it contains the right to erasure making it possible for a data subject to obtain the erasure of his or her

<http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf>), par. 23.

[62] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' (25 January 2012) COM(2012) 11 final (available at <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>); European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data' (25 January 2012) COM(2012) 10 final (available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=EN>).

[63] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[64] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Police and Criminal Justice Data Protection Directive) [2016] OJ L119/89.

[65] Recital 28 General Data Protection Regulation.

[66] Article 4 (7) General Data Protection Regulation; Article 3 (8) Police and Criminal Justice Data Protection Directive.

[67] Article 4 (8) General Data Protection Regulation; Article 3 (9) Police and Criminal Justice Data Protection Directive.

[68] Article 5 Paragraph 1 General Data Protection Regulation; Article 20 Paragraph 1 Police and Criminal Justice Data Protection Directive.

personal data from the controllers or the controllers might be obliged to do so under certain circumstances.[69]

Also, there is another directive – the Directive 2002/58/EC – focusing on the processing of personal data and the protection of privacy in the sector of electronic communications. It does not contain the right to online anonymity, but indirectly protects it.[70] It stresses that EU Member States, providers, users and EU bodies must cooperate in order to develop and introduce technologies to apply the guarantees laid down in the Directive and to take into account the objectives of minimising the processing of personal data and using anonymous and pseudonymous data where it is possible.[71] Providers of electronic communications services must adopt appropriate technical and organisation measures to ensure security of these services[72]; traffic data processed and stored by the providers must be erased or made anonymous when it is no longer needed[73]; and location data other than traffic data of users and subscribers can only be processed when it is made anonymous or when the consent of users or subscribers is provided[74].

In the EU, Directive 2006/24/EC[75] adopted in 2006 sought to harmonise Member States' national laws regarding the retention of certain data by providing that Internet Service Providers (hereinafter: ISPs) were required to retain traffic and location data and other related information generated or processed by them. This requirement was necessary to ensure that this data is available for detection, investigation and prosecution of serious crimes. In April 2014, the CJEU declared the Directive to be invalid.[76] According to the Court, this data can be analysed in order to distil clear information about private lives of individuals and therefore the Directive seriously interferes with the fundamental rights to respect for private life and to data protection laid down in Articles 7 and 8 of the EU Charter. This interference could, however, not be justified given that the Directive did not meet the requirement of proportionality.

Organization of American States

Articles 11 and 13 of the American Convention on Human Rights (hereinafter: ACHR)[77] protect the rights to privacy and to freedom of expression respectively. Article 13 ACHR contains almost the same notion of freedom to seek, receive and impart information as laid down in the ICCPR. Furthermore, Article IV of the American Declaration of the Rights and Duties of Man[78] states that individuals have the right to freedom of investigation, opinion and expression and

[69] Article 13 General Data Protection Regulation.
[70] Directive (EU) 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) [2002] OJ L201.
[71] Recital 9 Directive 2002/58/EC.
[72] Article 4 Paragraph 1 Directive 2002/58/EC.
[73] Article 6 Paragraph 1 Directive 2002/58/EC.
[74] Article 9 Paragraph 1 Directive 2002/58/EC.
[75] Directive (EU) 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC [2006] OJ L105/54 (available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>).
[76] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238.
[77] American Convention on Human Rights (entered into force 18 July 1978) OAS Treaty Series No 36, 1144 UNTS 123.
[78] American Declaration of the Rights and Duties of Man, OAS Res XXX adopted by the Ninth International Conference of American States (1948) reprinted in Basic Documents Pertaining to Human Rights in the Inter-American System OEA/Ser L V/II.82 Doc 6 Rev 1 at 17 (1992).

dissemination of ideas by all possible means. Article V stresses that every person has the right to the protection of the law against abusive attacks upon his honour, reputation and private and family life. Article X provides that every person has the right to the inviolability and transmission of his correspondence.

The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (hereinafter: IACHR) emphasised that 'both the right to freedom of thought and expression and the right to private life protect anonymous speech from government restrictions'[79]. Furthermore, the Special Rapporteur observed that 'in all cases, users have the right to remain anonymous and any dispute on this point need to be resolved exclusively in court'.[80]

African Union

The African Charter on Human and Peoples' Rights (hereinafter: ACHPR)[81] does not contain specific provisions on the right to privacy, but there is Article 9 on the freedom of expression with the first Paragraph proclaiming the right of every individual to receive information. There is also the African Union Convention on Cyber Security and Personal Data Protection.[82] It obliges States to establish a legal framework for strengthening fundamental rights and freedoms, especially the protection of physical data, and to punish any violations of privacy.[83] Interestingly, the Convention contains a provision stating that the interconnection of personal files helps to comply with legal and statutory objectives of data controllers, but needs to be achieved by adopting necessary security measures and without limiting data subjects' rights and freedoms.[84]

Association of Southeast Asian Nations

The Human Rights Declaration of the ASEAN[85] lists in Paragraph 21 the right of every person to be free from arbitrary interference with his or her privacy, family, home or correspondence, which includes personal data, or attacks upon his or her honour and reputation. In this regard, individuals must be protected by the law against such interferences or attacks. In addition, Paragraph 23 provides for the right to freedom of opinion and expression including the freedom to hold opinions without interference and to seek, receive and impart information in various forms and by various means.

5.2. Customary international law and the right to online anonymity

Customary international law or simply 'international custom, as evidence of a general practice accepted as law' is another source of international law[86] where the right to online anonymity

---

[79] IACHR, 'Annual Report of the Office of the Special Rapporteur for Freedom of Expression' (31 December 2013) OEA/Ser.L/V/II.149 <http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20_FINALweb.pdf> accessed 15 July 2016, p. 516, par. 134.

[80] Ibid, p. 510, par. 109.

[81] African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) (1982) 21 ILM 58.

[82] African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014) EX.CL/846(XXV) (available at <http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf>).

[83] Article 8 Paragraph 1 African Union Convention on Cyber Security and Personal Data Protection.

[84] Article 15 African Union Convention on Cyber Security and Personal Data Protection.

[85] ASEAN Human Rights Declaration (adopted 18 November 2012).

[86] See Article 38 Paragraph 1 under b of the Statute of the International Court of Justice.

could be traced. International custom requires State practice and *opinio juris* in order to contain legal rules binding upon States.[87] In this respect, State practice entails the actual practice and behaviour of States that find expression in the acts of State organs, legislation, case-law etc. and must be extensive and virtually uniform.[88] *Opinio juris* is a psychological factor meaning the belief of States that they are legally obliged to act in a certain way. Therefore, domestic approaches towards the right to online anonymity need to be examined in order to distil possible foundations of this right in both State practice and *opinio juris*.

At the national level, standards on online anonymity are still being developed.[89] On the one hand, there are States seeking to promote anonymity of Internet users. In the United States, the First Amendment protects the right of an individual to express himself or herself. The US Supreme Court indicated that anonymity serves as 'a shield from the tyranny of the majority'.[90] One of the US district courts observed that people are allowed to interact with each other while remaining anonymous or using pseudonyms if they do not violate law.[91] This possibility of communicating anonymously and pseudonymously leads to 'open communication and robust debate' and enables individuals to get access to information regarding some sensitive and intimate issues without any fear of embarrassment.[92] Other US courts upheld the right of individuals to read anonymously online and prohibited disclosure of their personal data by the publishers.[93]

In Canada, the Supreme Court addressed in 2014 protection of online anonymity of Internet users and linked it to the notion of privacy.[94] The Supreme Court stressed:

> In this case, the primary concern is with informational privacy. Informational privacy is often equated with secrecy or confidentiality, and also includes the related but wider notion of control over, access to and use of information. However, particularly important in the context of Internet usage is the understanding of privacy as anonymity…

It further observed that 'some degree of anonymity is a feature of much Internet activity and depending on the totality of the circumstances, anonymity may be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure'.

In Brazil, the Marco Civil da Internet Law from 2014 aims at ensuring the inviolability and secrecy of online communications and permits exception only by a court order.[95] In South Korea, the Constitutional Court declared in 2012 the policy on using real names on the Internet

---

[87] *Case Concerning the Continental Shelf (Libyan Arab Jamahiriya/Malta)* (Merits) [1985] ICJ Rep 3, p. 29, par. 27; *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, p. 253, par. 64.

[88] *North Sea Continental Shelf Case (Federal Republic of Germany v. Netherlands)* [1969] ICJ Rep 3, p. 43, par. 74.

[89] ARTICLE 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity Online' (February 2015) available at <http://www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 7 January 2016, p. 8.

[90] *McIntyre v. Ohio Election Comm'n* [1995] 514 U.S. 334 (US Supreme Court) (available at <http://caselaw.findlaw.com/us-supreme-court/514/334.html>), Section VI.

[91] *Columbia Insurance Company v. Seescandy.com* [1999] 185 F.R.D. 573 (US District Court for the Northern District of California).

[92] Ibid.

[93] See, for instance, *Melanie Senter LUBIN, Securities Commissioner for the State of Maryland v. AGORA, INC* [2005] 882 A.2d 833 (US Court of Appeals of Maryland) (available at <http://caselaw.findlaw.com/md-court-of-appeals/1237646.html>).

[94] *R. v. Spencer* [2014] 2 S.C.R. 212 (Supreme Court of Canada) (available at <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do>).

[95] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, p. 13.

unconstitutional.[96] In Austria, the use of encryption tools is not restricted and the authorities actively engage in educating citizens on the matters of digital security.[97] In Sweden and Slovakia, laws also do not prohibit or restrict encryption by Internet users and Germany, Norway and Ireland actively promote it and are against any restrictions on encryption protocols.[98] In Greece, there are legislative acts and policies promoting the use of anonymity instruments and encryption.[99] Also, other governments, such as those of the Netherlands, Sweden and Canada, fund initiatives promoting the use of encryption and other anonymity instruments and educate citizens on the ways to enhance their online security.[100] In the beginning of 2016, the Dutch government formally acknowledged that it is against the use of legal measures prohibiting or restricting the use and development of encryption instruments and introduction of backdoors in them.[101]

On the other hand, there are efforts undertaken by some governments to restrict online anonymity in order to pursue such interests as prevention of crimes and terrorism and achieve other goals. These restrictions and prohibitions constitute interferences with the right to freedom of expression[102] and can be seen as interfering with the rights to privacy and data protection. The recent most striking example of governmental efforts to disregard individuals' rights to privacy and data protection and make it impossible to communicate anonymously online can be found in the practice of mass surveillance and interception of communication the US secret agencies as revealed by Edward Snowden. The US Supreme Court has rightly observed that 'the right to remain anonymous may be abused when it shields fraudulent conduct'[103], but the limitations of this right in the US are often extensive and disregard the most basic human rights standards and guarantees. Recently, in the US a proposal of the Compliance with Court Orders Act of 2016 or the Encryption Bill was put forward. This Bill requires all entities, including device and software manufacturers, to comply with US court orders in order to protect Americans from criminals and terrorists and to provide the authorities with information or data for investigation or prosecution of serious crimes and to provide any technical assistance for obtaining them. In essence, it introduces decryption requirements giving the government access to personal data of individuals and can be said to disregard digital security considerations. In April 2016, a draft of this legislative act was released by two senators[104] but currently it does not have much support in the US.

In the United Kingdom, the Investigatory Powers Bill was introduced in November 2015 and its latest version was published on 1 March 2016.[105] The Bill sparkled much debate over its

[96] Decision 2010 Hun-Ma 47, 252 (consolidated) announced on 28 August 2012 (South Korean Supreme Court).
[97] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, pp. 13-14.
[98] Ibid, p. 14.
[99] Ibid.
[100] Ibid.
[101] Human Rights Council, 'Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci' (8 March 2016) UN Doc. A/HRC/31/64, pp. 11-12.
[102] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, p. 18.
[103] *McIntyre v. Ohio Election Comm'n* [1995] 514 U.S. 334 (US Supreme Court) (available at <http://caselaw.findlaw.com/us-supreme-court/514/334.html>), Section VI.
[104] 'Intelligence Committee Leaders Release Discussion Draft of Encryption Bill' (*www.feinstein.senate.gov*, 13 April 2016) <http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649> accessed 2 July 2016; Mark Hosenball and Dustin Volz, 'Senate Panel Releases Draft of Controversial Encryption Bill' (*Reuters*, 13 April 2016) <http://www.reuters.com/article/us-apple-encryption-legislation-idUSKCN0XA2B4> accessed 2 July 2016.
[105] Investigatory Powers Bill (available at <http://www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/16143.pdf>).

effect on the rights to privacy and data protection and was criticised by the UN Special Rapporteur on the Right to Privacy, Joseph Cannataci, in his report from 8 March 2016.[106] It provides a new legal framework for the use and oversight of investigatory powers by law enforcement and security and intelligence agencies. This Bill leads to significant privacy and data protection concerns by introducing privacy-intrusive measures, such as bulk surveillance and bulk hacking. For instance, it makes it possible for the Secretary of State to give any telecommunications operator in the UK a national security notice or a technical capability notice that require that operator to take certain steps as deemed necessary by the Secretary of State or impose obligations and require a person to take all steps in order to comply with these duties.[107] A person to whom a notice is given must comply with it[108] and obligations relating to a technical capability notice, for instance, may include the removal of electronic protection of communications or data[109]. The Bill successfully went through the House of Commons, came through two readings in the House of Lords and awaits the committee stage.

Constitutions of some States specifically prohibit anonymous speech and anonymity: this is the case in Brazil and the Bolivian Republic of Venezuela.[110] Vietnam has prohibited the use of pseudonyms online in 2013; Iran introduced in 2012 a registration requirement for all national IP addresses and made it compulsory for Internet café users to register their real names; and in Ecuador it is required for mobile phone owners and those who want to comment on websites to use real names for registration purposes.[111] In Russia, online anonymity is also threatened given that cybercafé users must provide their identification in order to make use of public wireless Internet connectivity and bloggers with 3.000 or more readers have to register with the media regulator.[112] Similarly, China requires registration with actual names for accessing certain websites and South Africa has regulations of real name registration for online and mobile phone users.[113]

The assessment of regulations and policies of some States reveals that approaches towards online anonymity and anonymity tools, such as encryption, around the globe are rather diverse and range from recognition of importance of these instruments and encouragement of their use to prohibitions and restrictions. It is to be observed that these are mostly governments of Western European (or EU Member States) and North American countries that are largely supportive of ensuring online anonymity, while other States, including Russia, Iran and China, remain reluctant to guarantee the rights to freedom of expression and privacy by allowing online users to anonymously make use of Internet services. While some traces of customary international law can be perceived in the practice of EU countries having much influence given their technological advancement and the role of forerunners as democratic States complying with and promoting human rights standards, they do not constitute real evidence of an emerging rule of customary international law recognising the right to online anonymity.

[106] Human Rights Council, 'Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci' (8 March 2016) UN Doc. A/HRC/31/64, pp. 14-15.
[107] Section 216 Investigatory Powers Bill.
[108] Section 218 (9) Investigatory Powers Bill.
[109] Section 217 (4) (c) Investigatory Powers Bill.
[110] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, p. 18.
[111] Ibid.
[112] Ibid.
[113] Ibid, pp. 18-19.

5.3. General principles of law and the right to online anonymity

As such, general principles of law recognised by civilised nations constitute a source of international law with a rather limited scope.[114] These principles include such concepts as the idea that every violation of an engagement leads to an obligation to make reparation, the notion of *res judicata*, the principle of estoppel, respect for acquired rights, good faith, the concept of full compensation of prejudice through awarding to an injured party the *damnum emergens* and *lucrum cessans* and possibly other principles.[115] By examining these general principles, a conclusion can be drawn that the right to online anonymity or online anonymity do not belong to this specific source of international law but should be found somewhere else.

6. The right to online anonymity

The analysis of human rights instruments and other legal documents is useful in identifying the right to anonymity online. First of all, provisions on the rights to privacy and freedom of opinion and expression of the UN human rights treaties reflect customary international law norms, especially the ICCPR, and are binding upon all States.[116] They have not originally been designed to deal with the Internet infrastructures, but nevertheless, can be interpreted in such a manner as to include the right to online anonymity. Furthermore, the Guidelines for the Regulation of the Computerized Personal Data Files do not directly address the issue of anonymity online, but provide that information must be able to freely flow between States and that security measures, including encryption, need to be adopted in order to protect data files. This might be an indication of the fact that ensuring anonymity of Internet users and their personal data is one of State responsibilities in regulating computerised personal data files. The Guidelines, however, deal with the collection and processing of personal information and compilation of personal data files, which can be considered as contrary to the idea of online users being anonymous.

Secondly, it might appear obvious that the OECD Guidelines in their current form – similar to the UN regime – do not directly address the right to online anonymity; their principles, however, do improve many aspects of privacy protection and thus can lead to more anonymity of online users.

Thirdly, the ECHR's Articles 8 and 10 can be said to encompass the right of individuals to remain anonymous while accessing Internet services. They address the rights to privacy, data protection and freedom of expression and anonymity forms an important requirement that needs to be fulfilled in order for Internet users to fully enjoy these rights and freedoms. Under the Convention No. 108, States have an obligation to take necessary security measures for protecting personal data, such as encryption, and thus must protect anonymity of individuals. However, the fact that the treaty concerns, among other things, the storage and collection of personal data does not ensure or strengthen the right to online anonymity. Also, the Convention on Cybercrime of 2001 underlines the importance of sufficiently protecting human rights and fundamental freedoms in combating cybercrime, but does introduce State duties to collect and intercept traffic data and content data, which are as such against the purpose of a general right to online anonymity and constitute restrictions of this right.

Fourthly, it is apparent that the EU is taking a forerunner's role with regard to the protection of human rights in the digital era. Its extensive legislation on the rights to privacy, personal data

[114] Malcolm N. Shaw, *International Law* (Sixth Edition, Cambridge University Press 2008), p. 99.
[115] Ibid, pp. 100-105.
[116] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, pp. 6-7.

protection and freedom of expression and recent case-law of the CJEU, including *Digital Rights Ireland and Seitlinger and Others*, *Google Spain*[117] and *Maximillian Schrems*[118] judgments are an indication of this position and show that within the EU the right to online anonymity can be in its emergence phase.

Fifthly, legal instruments adopted within the framework of the Organization of American States provide some clarity regarding the protection of privacy and freedom of expression and can be regarded as indirectly supporting the idea of the right to online anonymity of individuals.

Finally, human rights mechanisms available in the African Union and the ASEAN reflect similar guarantees adopted at the global level, but cannot be said to specifically address the right to online anonymity.

The Internet Rights & Principles Dynamic Coalition (hereinafter: IRPC), a network of individuals and organisations based at the UN Internet Governance Forum, firmly believes that there is a right to online anonymity. Its document entitled '10 Internet Rights and Principles' provides that everyone has a right to privacy online, which includes not only freedom from surveillance and the right to use encryption, but also the right to online anonymity.[119] ARTICLE 19, which is an international human rights organisation promoting freedom of expression and information around the world, clearly refers to the right to anonymity that is included in the right to freedom of expression, consists of the right to anonymous speech, the right to read anonymously and the right to browse anonymously online and requires strong protection.[120] The Association for Progressive Communication, a global network of civil society organisations, made a submission to the UN Special Rapporteur on the Rights to Freedom of Peaceful Assembly and Association and recommended the Special Rapporteur and other relevant UN bodies to discuss the need for a right to online anonymity with regard to the rights to freedom of peaceful assembly and association.[121]

Given that individuals not always express themselves on the Internet, but also seek and receive information and engage in other activities that do not require the exercise of the right to freedom of expression, the right to online anonymity cannot be limited only to the freedom of opinion and expression and its aim should be to protect individuals' online privacy. Anonymity and encryption play an important role in securing two interlinked rights to privacy and freedom of expression.[122] The right to anonymity online is inherent to these two fundamental rights that form its sources and has an important function to perform in today's world. It is apparent that online anonymity cannot effectively be realised without the use of privacy enhancing

[117] Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317.
[118] Case C-362/14 *Maximillian Schrems* [2015] ECLI:EU:C:2015:650.
[119] IRPC, '10 Internet Rights and Principles' (IRPC Campaign) <http://internetrightsandprinciples.org/site/campaign/> accessed 20 July 2016.
[120] ARTICLE 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity Online' (February 2015) available at <http://www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 7 January 2016, p. 24.
[121] Association for Progressive Communication, 'The Rights to Freedom of Peaceful Assembly and Association on the Internet: Submission to the United Nations Special Rapporteur on the Rights to Freedom of Peaceful Assembly and Association by Association for Progressive Communication (APC)' (2012) <https://www.apc.org/es/system/files/APC_Submission_FoA_Online.pdf> accessed 3 July 2016, par. 37.
[122] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue' (17 April 2013) UN Doc. A/HRC/23/40, p. 20.

technologies (hereinafter: PET), such as encryption tools, Tor and https:// protocols[123] shielding users' identity from the eyes of the public.

Anonymity is an instrument that, on the one hand, can be used by individuals in order to hide their identity on the Internet from others for the purposes of protecting their privacy and enjoying the freedom of expression. It might even be the only tool that regular online users have against tracking and profiling.[124] On the other hand, it is also a tool in the arsenal of data controllers and data processors for complying with their data protection obligations. From the examination of international conventions and other documents and case-law of regional judicial bodies, it follows that some traces of the right to online anonymity or guarantees associated with it can be found in these sources and this emerging right can be seen as a constitutive element of the rights to privacy and freedom of expression. This also becomes evident when one analyses State practice and *opinio juris* of EU Member States and the position of the EU itself.

7. Restrictions on online anonymity

Certainly, a possible right to online anonymity cannot be unlimited and absolute. Its protection should always be considered in relation to the accountability of individuals that might abuse it.[125] The interests of persons enjoying the right to anonymity on the Internet need to be balanced against the interest of the society to be protected against harmful activities resulting from the exercise of this right by others. It is necessary to understand that anonymity online should not facilitate criminal acts and other related activities by significantly limiting the scope of accountability of individuals in question.

International and regional human rights treaties, judicial bodies and institutions acknowledge the fact that the right to freedom of expression, similarly to the rights to privacy and data protection, can be limited only by law for the purposes of pursuing certain interests in specific circumstances. The ECtHR, for instance, has acknowledged that anonymity is crucial for ensuring freedom of expression but can be restricted when legitimate objectives justify such restrictions.[126] These limitations commonly introduced at the national level in form of legislative acts must serve such interests as national security and public order and be not only necessary in a democratic society, but also proportionate. The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights made clear the following:

> [T]he anonymity of the sender would in no way protect those who disseminate child pornography, engage in pro-war propaganda or the advocacy of hatred that constitutes the incitement of violence, or the direct and public incitement of genocide. This kind of speech is not protected by the American Convention, and anonymity cannot protect its issuers from the legal consequences established – in accordance with international human rights law – in each domestic legal system with respect to each one of those cases. The same thing would occur if the exercise of the right to freedom of thought and expression were subject to the subsequent imposition of liability of the kind authorized by the American Convention. In all of those cases, judicial authorities would be authorized to take

[123] A. Michael Froomkin, 'Anonymity in the Balance' in Chris Nicoll, Corien Prins and Miriam van Dellen (eds), *Digital Anonymity and the Law: Tensions and Dimensions* (TMC Asser Press 2003), p. 31.
[124] Ibid, p. 45.
[125] Indira Carr, 'Anonymity, the Internet and Criminal Law Issues' in Chris Nicoll, Corien Prins and Miriam van Dellen (eds), *Digital Anonymity and the Law: Tensions and Dimensions* (TMC Asser Press 2003), p. 195.
[126] UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, p. 17; UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye' (22 May 2015) UN Doc. A/HRC/29/32, p. 7.

> reasonable measures to determine the identity of the sender engaged in prohibited acts, in order to take proportionate action in response, as provided by law.[127]

A number of factors are at stake in the balancing exercise made by States with regard to the interests of individuals to remain anonymous and interests pursued by the authorities.[128] The first factor to consider is how users avoid identification online: it can be done by using anonymity or pseudonymity. Secondly, the level of information security of online activity providing a variable degree of traceability is of importance. Thirdly, the substance and circumstances of online activity form another criterion. It stands to reason that States tend to be more likely to interfere with the right to online anonymity when individuals are identified without major difficulties, when the level of information security is fairly low and when online activity in question concerns criminal acts.

If State authorities decide to restrict the right to online anonymity, there must be legislative acts providing for this limitation. These laws are required to be clear, precise, transparent and public and avoid giving States unlimited discretion in restrictions.[129] It is also required to introduce strong and coherent procedural and judicial safeguards to realise that.[130] One the most significant requirements in this regard should be the availability of a court order or another form of judicial supervision to reveal one's identity and to lift his or her online anonymity given that judicial institutions are the most suitable actors for striking a fair balance between different interests and weighting different human rights at stake in a given case. Additionally, limitations of online anonymity are only possible when they serve legitimate interests of protection of rights and freedoms of others, national security, public order, public health or morals.[131] Furthermore, any restriction must be necessary in a democratic society and go beyond the only reason of it being useful or desirable.[132] This process of limiting the right to online anonymity needs to be subjected to the scrutiny of an independent and impartial judicial authority.[133] Finally, these restricting measures are required to meet the requirement of proportionality and must form the least intrusive measures among others that can be used to achieve the same result.[134]

8. Conclusion

Online anonymity has not only positive and valuable but also negative and harmful consequences. Until now, the right to online anonymity has merely enjoyed limited recognition under international law and cannot be concluded to constitute a legal right universally

[127] IACHR, 'Annual Report of the Office of the Special Rapporteur for Freedom of Expression' (31 December 2013) OEA/Ser.L/V/II.149 <http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20_FINALweb.pdf> accessed 15 July 2016, pp. 516-517, par. 135.
[128] A. Michael Froomkin, 'Anonymity in the Balance' in Chris Nicoll, Corien Prins and Miriam van Dellen (eds), *Digital Anonymity and the Law: Tensions and Dimensions* (TMC Asser Press 2003), pp. 8-9.
[129] UN Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, 22 May 2015, UN Doc. A/HRC/29/32, pp. 11-12, par. 32.
[130] ARTICLE 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity Online' (February 2015) <http://www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 7 January 2016, p. 24.
[131] UN Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, 22 May 2015, UN Doc. A/HRC/29/32, p. 12, par. 33.
[132] Ibid, par. 34.
[133] Ibid.
[134] Ibid, par. 35.

recognised around the globe by States.[135] This contribution has argued that some traces of the emerging right to online anonymity flowing from the right to privacy, the associated with it right to data protection and the right to freedom of opinion and expression are observed in international law. When governments and private actors do not allow individuals to engage in anonymous communications online by monitoring their activities and gathering information, they essentially violate the rights to privacy and data protection.[136] In turn, these violations lead to the decreased confidence of people in Internet services and undermine their security online, which negatively affects the free circulation of ideas and information on the Internet and thus violates the freedom of expression. The right to online anonymity can be said to be an important constitutive element of this right to freedom of expression and the right to respect for private life. States cannot simply disregard their international legal obligations and breach these rights and freedoms. When users communicate online, they are entitled to the right to private correspondence, including different forms of communication, and it is an extensive State duty to take all necessary measures in order to ensure that emails and other messages sent by individuals reach their respective recipients without being inspected or interfered with by State organs or private actors.[137] The right to online anonymity can enhance the protection of these and other human rights, such as the right to freedom of peaceful assembly and association.

Similarly to the rights to privacy and freedom of expression, the right to anonymity online cannot be absolute. Responsibility comes with true and undisguised identity and in certain circumstances interferences with this right must be possible, such as for the prevention of crime or protection of rights of others. States must understand that they are not allowed to interfere with the online users' right to online anonymity without complying with international human rights duties. There must be guarantees in place for ensuring that human rights and fundamental freedoms are protected and respected and that those who abuse their right of being anonymous are deprived of this right in exceptional circumstances. If limitations are to be imposed, they must meet the recognised set of requirements adopted and recognised by various human rights instruments: these limitations must be imposed in accordance with the law, serve specific interests in a democratic society and be necessary and proportionate. Thus, State authorities may only in an exceptional situation take a decision to act in violation of the right to privacy when they are empowered to do so by law and have usually received an authorisation from the judiciary to do so in order to protect certain legitimate interests.[138] The same reasoning applies to the interference with the freedom of opinion and expression. In both types of limitation, such interference must be not only necessary, but also proportionate. What is also necessary, is the adoption of effective data protection laws providing clear rules on who is allowed to have access to personal data of individuals, for what purposes this data can be used, how it can be stored and for how long.[139] Even the highly criticised draft of the US Encryption Bill requires a court order to be issued with regard to entities before they are considered obliged to release individuals' information and data. This legal guarantee is potentially a useful measure to prevent possible abuse of power by State authorities in a democratic society. The oversight exercised by judges in such a manner is necessary to ensure that anonymity enjoyed by online users would not allow them to engage in illegal activities and perform other harmful acts.

---

[135] ARTICLE 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity Online' (February 2015) <http://www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 7 January 2016, p. 7.

[136] UN General Assembly, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue,* 16 May 2011, UN Doc. A/HRC/17/27, p. 15.

[137] Ibid, p. 16.

[138] Ibid.

[139] Ibid, p. 15.

The emerging right to online anonymity serves as a facilitator of safe and anonymous communications and allows individuals to use online services without revealing their actual identity and avoid intrusion into their private and family life. If we deny the existence of the right to online anonymity or abolish anonymity online as such, the Internet will never be free and open as it was conceived many decades ago. Given the rapid development of the Internet, this right is a crucial topic for discussion in the context of law and policy and eventually needs to be protected and respected by States. An important State duty in this regard is to educate online users on the issue of anonymity and different ways to achieve it.[140] It is to be observed that in the current technological climate with large data sets originating from Big Data, it becomes easier to identify individuals and deanonymise them by linking different data sets to each other.[141] Given that the level of legal protection of online anonymity is fairly low, online users turn to technical tools and solutions,[142] but it is impossible for them to remain completely anonymous by only resorting to these instruments. Additionally and importantly, online anonymity of Internet users requires protection from not only State actors, but must also be respected by private actors who can significantly affect the enjoyment of the fundamental rights to freedom of expression, privacy and data protection. What is needed, is a high level of legal protection and enforcement on the part of governments. The European Parliament made the following recommendation to the Council concerning the process of strengthening security and fundamental freedoms on the Internet:

> … 'digital identity' is increasingly becoming an integral part of our 'self' and in this respect deserves to be protected adequately and effectively from intrusions by both private and public actors – thus, the particular set of data that is organically linked to the 'digital identity' of an individual should be defined and protected, and all its elements should be considered inalienable personal, non-economic and non-tradable rights; take due account of the importance of anonymity, pseudonymity and control of information flows for privacy and the fact that users should be provided with, and educated about, the means to protect it efficiently, for instance through various available Privacy-Enhancing Technologies.[143]

The right to online anonymity can be constructed as an important element of both the right to privacy, including the right to data protection, and the right to freedom of expression. Given the nature of the Internet as an open and free information platform, efforts should be devoted to establishing a clear international standard for the protection of the right to anonymity online that is based on a coherent understanding of this concept. It can be done by introducing or modifying national laws protecting online anonymity, signing and ratifying international conventions or interpreting and amending existing international and regional human rights instruments. As observed by the UN Special Rapporteur on the Right to Privacy:

> For the passage of time and the impact of technology, taken together with the different rate of economic development and technology deployment in different geographical locations means that legal principles established fifty years ago (ICCPR) or even thirty-five years ago (e.g. the European

---

[140] Craig R. Scott, 'Benefits and Drawbacks of Anonymous Online Communication: Legal Challenges and Communicative Recommendations' (2004) 41(1) *Free Speech Yearbook*, pp. 138-139.

[141] European Digital Rights (EDRi), 'An Introduction to Data Protection' (2013) 6 The EDRi Papers, <https://edri.org/files/paper06_datap.pdf> accessed 18 July 2016, p. 7.

[142] ARTICLE 19, 'Response to UN Special Rapporteur's Call for Comments on Encryption and Anonymity Online' (February 2015) available at <http://www.ohchr.org/Documents/Issues/Opinion/Communications/Article19.pdf> accessed 7 January 2016, p. 11.

[143] European Parliament, 'Recommendation of 26 March 2009 to the Council on Strengthening Security and Fundamental Freedoms on the Internet' (2008/2160(INI)) (available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2009-0194+0+DOC+PDF+V0//EN>).

> Convention on Data Protection) let alone seventy years ago (UDHR) may need to be re-visited, further developed and possibly supplemented and complemented to make them more relevant and useful to the realities of 2016.[144]

In this regard, there is a significant role to be played by the EU and CoE Member States and institutions. Similar to the ECtHR establishing the idea of the right to data protection being part of the right to respect for private life laid down in Article 8 ECHR, this and other judicial bodies and institutions can expand the scope of the right to privacy and freedom of expression to accommodate this essential right as well. Its application to the current digital world is simply a necessity for ensuring respect and protection of these fundamental rights and freedoms by protecting the identity of individuals. While it is not a panacea against all risks that emanate from different actors present on the World Wide Web, it certainly will contribute to the realisation of the most crucial human rights standards that cannot be disregarded nowadays.

[144] Human Rights Council, 'Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci' (8 March 2016) UN Doc. A/HRC/31/64, p. 9.