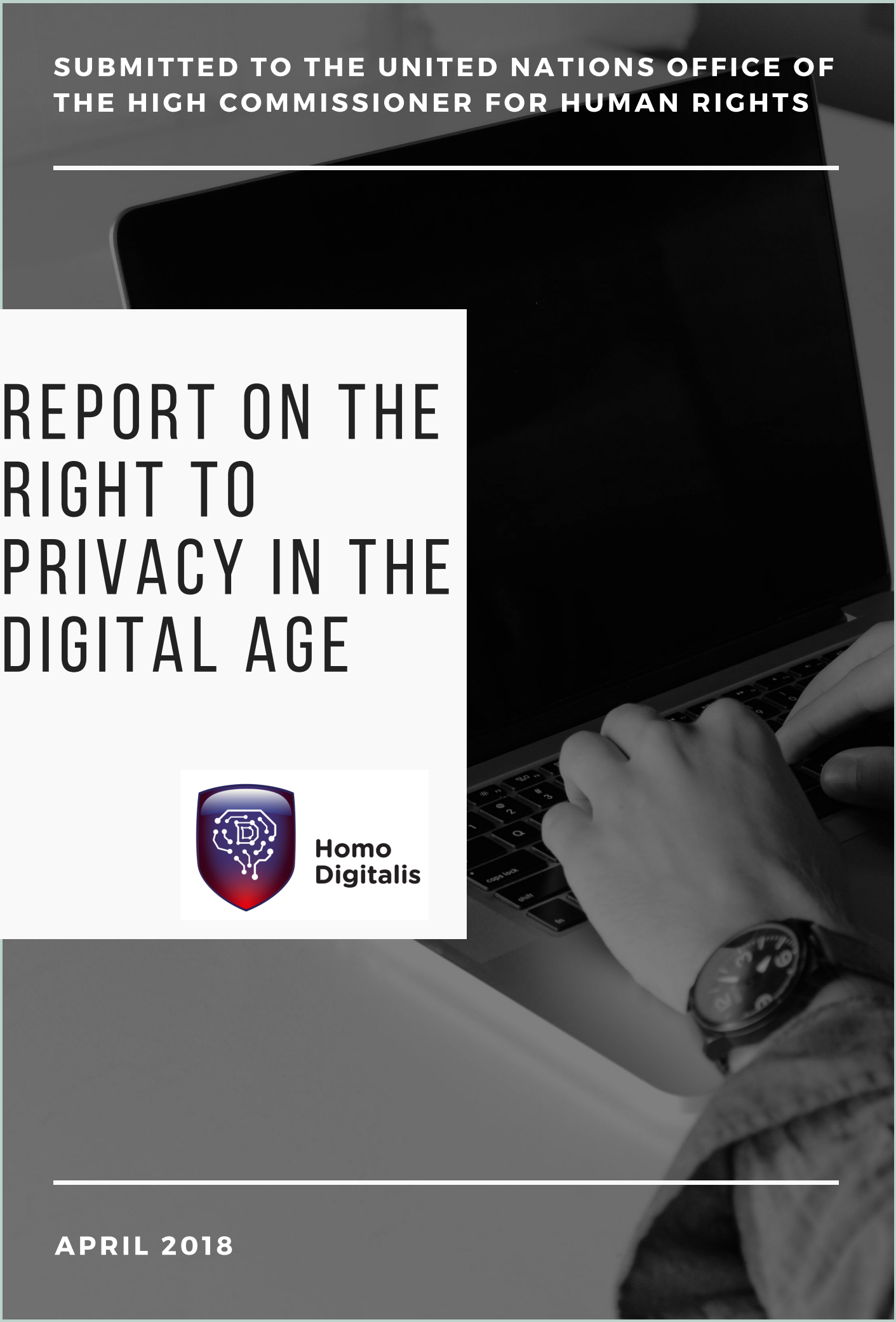
SUBMITTED TO THE UNITED NATIONS OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS

REPORT ON THE RIGHT TO PRIVACY IN THE DIGITAL AGE



Homo Digitalis

APRIL 2018

Homo Digitalis

Date: 04 April 2018

Report on the right to privacy in the digital age

Submitted to the United Nations Office of the High Commissioner for Human Rights

Table of Contents

Introduction

1. *Homo Digitalis* would like to thank the Office of the High Commissioner for Human Rights for the opportunity to provide its input as regards human rights challenges relating to the right to privacy in the digital age. *Homo Digitalis* is a civil society non-governmental organization located in Athens, Greece, dedicated to the protection of human rights and freedoms in the digital environment.

2. In Chapter One of the present report, *Homo Digitalis* is focusing on encryption and anonymity as enablers for the enjoyment of human rights, including the right to freedom of expression and of opinion. In Chapter Two, *Homo Digitalis* examines the regulatory framework in Greece that provides for the retention of electronic communications' metadata. Finally, in the last chapter of this report, *Homo Digitalis* offers its recommendations with regard to the promotion and protection of the human rights discussed in the two main chapters.

Chapter One: Encryption and anonymity as enablers for the enjoyment of human rights, including the right to freedom of expression and of opinion; challenges raised by encryption and anonymity and ways to address these challenges.

3. Anonymity constitutes an indispensable part of liberal societies. Anonymous speech in the form of proclamations, brochures, posters, books and now through the Internet is an important element of the right to political participation.

4. The protection of freedom of expression and of opinion entails anonymous speech. *Homo Digitalis* underlines the importance of such a protection under the rule of law and considers it imperative. Anonymity safeguards the speaker from potential reactions of the majority. Therefore, it enhances freedom of expression, particularly heretical expression. It enhances the freedom of opinion of the minorities and the ones who contest the authorities. The latter is a fundamental aspect of democracy.

5. By having the right to anonymous expression, every person is able to express his opinions, regardless of their bravery, skills in public speaking or the popularity of his views. Anonymity provides for the necessary ground for every opinion to be heard.

6. Internet constitutes the biggest innovation in human history regarding the freedom of expression and of opinion. Its universality and the fact that it is available to every person with a mobile phone or a phone line, as well as the outstanding velocity in which an opinion can reach every other person, is unprecedented.

7. As of 31 December 2016, Internet users worldwide were estimated at 45.91% of the global population.[1] This number has definitely increased by April 2018 when this report is being written. Thus, Internet constitutes the most massive means for expression. It provides for a step for expression for every person with a global audience. This fact is in favour of dialogue and democracy, it enhances civil commitment and participation.

8. Anonymity is fully guaranteed only through encryption in the digital era. Notably, encryption acts as a means of protection for personal data and e-communications.[2] Therefore, anonymity and encryption in the Internet are crucial for the full enjoyment of the right to freedom of expression and of opinion. The Special Rapporteur on Free Expression of the Inter-American Commission on Human Rights (IACHR) made clear that "in all cases, users have the right to remain anonymous and any dispute on this point needs to be resolved exclusively in court."[3]

9. However, under the salutary safeguards of anonymity, it is possible that, speech of bad quality is also protected. Enormous amounts of useless, false, even pestilential, illegal and unethical information are produced daily. Anonymity and encryption may intentionally or unintentionally reinforce the production of this information. This constitutes the gravest challenge of the Internet and anonymity, on which its function is based.

10. *Homo Digitalis* submits that the challenges created by anonymity and encryption can fortunately be addressed. Anonymity and encryption do not guarantee asylum for illegal acts. The Internet user who proceeds to violations of the law can be traced and brought before justice. Anonymity is not absolute and has to yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.[4]

11. The most significant concern regarding anonymity and encryption is that it reinforces the production of false or offensive speech. However, two fundamental characteristics of the Internet decrease the impact of malicious speech. First, the promptness and the interactivity of the Internet ensure that the person insulted has immediate access to the content published against him/her and the right to respond. It is very important that this procedure is free of charge. The person insulted can address the same audience who viewed the spiteful publication, or even a larger one, and convince them for the falseness of the commentary against him/her. Third persons who are interested in unveiling the truth may also act in the same way.

12. Second, the credibility of the Internet dictates that if anonymous expression is to overcome the prejudice of unreliability, it has to be serious in its content. Competition for credibility is perhaps the biggest race in the contemporary digital era for all stakeholders. Credibility, in its turn, emits false or offensive forms of expression.

13. The credibility and interactivity of the Internet are based on the factor 'Internet user'. Therefore, *Homo Digitalis* considers that raising public awareness regarding these issues and measures taken towards this direction are of the utmost importance. The architecture of the Internet was based on anonymity and subsequently encryption. Without these two elements, the Internet cannot fulfil its objective. Anonymity and encryption are also vital for the promotion and protection of the right to freedom of expression and opinion. Only through proper and constant education and training towards the right use of the Internet may the challenges described above be alleviated.

Chapter Two: Electronic communications and metadata retention: Are we living in an age, when the right to privacy is sacrificed on the altar of security?

14. According to Eurostat, almost eight out of ten (79 %) of the people in EU use the Internet regularly at home, at work or elsewhere, while specifically in Greece, more than the half of its population (57%) use the Internet every day or almost every day. [5] Mobile phones or smartphones are the most used devices by internet surfers in EU Member states (over three-quarters, 79%), and the same goes for Greece (66%).[6]

15. These numbers showcase that information and communication technologies (ICTs) constitute an important part of people's daily life. No matter what is the channel that individuals use for their e-communications (such as traditional telecommunications service providers or "Over The Top- OTT-" providers), it is an indisputable fact that, the metadata of their e-communications can reveal personal and highly sensitive information about them. In general, EU citizens appear to be particularly concerned about who can access the data of their e-communications. More precisely, 72% of them consider as very important that the confidentiality of their communications, such as instant messaging, is guaranteed.[7] However, in half of the Member States, only less than a third of their citizens know that instant messaging and online voice conversations can be accessed without their permission. Apropos of Greece, the numbers are even worst, since the percentage is only 6%.[8]

16. With the present report, *Homo Digitalis* warns that the lack of common safeguards across the European Union as regards the retention and access to metadata of e-communications poses a significant risk to the fundamental rights of the people of the EU.

17. In addition, *Homo Digitalis* underlines the fact that Greece, ignores the requirements set out in the case law of the Court of Justice of the European Union (CJEU) and has shown over the last years no progress in adopting new legislation on data retention. Instead, Greek Law 3917/2011 transposing the annulled[9] Directive 2006/24/EC[10], still remains in force, thus allowing for a disproportionate interference with the right to privacy of e-communication services users in Greece. *Homo Digitalis* reminds that the latter Directive was annulled because its provisions applied to all means of electronic communications and to all users, without providing for any differentiation, limitation or exception (such as professional secrecy). Specifically, the Directive 2006/24/EC did not require any relationship between the metadata retained and a particular time period, or a particular geographical zone, or a circle of particular persons that are involved in serious crime.[11]

18. Reflecting on CJEU's judgments national legislation allowing the general and indiscriminate retention of all metadata of subscribers and users relating to all means of electronic communication is incompatible with EU law.[12] Metadata of electronic communications reveal information, such as the source of a communication and its destination, the date, time, duration, or type of a communication, and the users' communication equipment or location. Moreover, the name and the address of the user, the telephone number of the caller and the number called can be revealed as well. Thus, metadata allow for very precise conclusions to be drawn concerning the private lives of the individuals involved, such as their habits, the places of their residence or visit, and their social circle.[13] Therefore, the retention of these metadata constitutes a serious interference with the right to respect for private and family life. Moreover, as ruled by the CJEU, apart from the retention itself, the access to the retained metadata by the national law enforcement authorities constitutes a "further interference" with this right.[14]

19. However, the retention of e-communications metadata additionally interferes with other human rights, such as the right to the protection of personal data, the right to freedom of expression, and the right to an effective remedy.

20. More precisely, the retention of metadata constitutes a processing of personal data and, therefore, necessarily has to satisfy the requirements of EU data protection law.[15] Thus, national legislation must describe in a clear manner under which circumstances – subject to the principle of proportionality and only when it is necessary - metadata retention can be adopted as a preventive measure for the fight against serious crime.[16]

21. In addition, as the CJEU has ruled that, metadata does not constitute e-communications content, and thus, its retention does not interfere with the essence of the right to freedom of expression. However, such a retention could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression. Same goes for corresponding rights and freedoms, such as the freedom of thought, conscience and religion.[17]

22. Furthermore, the CJEU has stressed that the national law enforcement authorities to whom access to the retained metadata has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy.[18]

Recommendations

23. *Homo Digitalis* suggests that anonymity and encryption are fundamental characteristics of the World Wide Web, without which, the latter would be transformed into a null void. Anonymity and encryption enhance freedom of expression and shall be protected, rather than combated. In order to meet the challenges raised by anonymity and encryption in the digital era, ***Homo Digitalis*** **recommends** that:

    - campaigns are funded and organized in order to raise public awareness on the importance of anonymity and its correct use in the digital era,
    - special courses are taught in schools of all levels of education regarding the proper use of the internet,
    - state authorities are urged to fight cybercrime and illegal acts, concealed under the veil of anonymity and encryption
    - legislative and judicial action is taken in order to ensure that the protection of freedom of expression entails the protection of anonymous speech

24. Furthermore, *Homo Digitalis* suggests standards that national legislation should have in place to comply with the requirements set by the CJEU's rulings on metadata retention.

25. As regards the retention of metadata itself, CJEU does not prevent a Member State from adopting, as a preventive measure, legislation permitting the targeted data retention for the purpose of fighting serious crime if the retention of data is limited to what is strictly necessary, with respect "*to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted".*[19] ***Homo Digitalis*** **recommends** that in order to comply with such a requirement national legislation should:

    - provide for the protection of professional secrecy,
    - request evidence capable of suggesting that a user's conduct might have a link - even an indirect or remote one - with serious criminal offences,
    - provide for different metadata retention periods depending on the usefulness of the metadata for the purpose of fighting serious crime.

26. Moreover, the CJEU has ruled that access to the retained metadata by national law enforcement authorities would be allowed when it is solely restricted to the purpose of fighting serious crime, it is subject to prior review by a court or an independent administrative authority, and the metadata it concerns are retained within the European Union.[20] ***Homo Digitalis*** **recommends** that in order to comply with such requirements national legislation should:

    - determine that e-communication service providers should grant access to the retained metadata to the law enforcement authorities solely for the purpose of fighting serious crime.
    - request a prior review by a court or an independent administrative authority (except in cases of validly established urgency),
    - request metadata to be retained inside the EU.

27. Finally, *Homo Digitalis* stresses that national legislation should provide for individuals, affected by metadata retention measures, to be able to exercise their right to legal remedies. In addition, national supervisory authorities must be able to review the metadata retention

practices and control compliance with the EU data protection law. ***Homo Digitalis*** **recommends** that in order to put in place such safeguards, national legislation should:

- request law enforcement authorities to notify the individuals affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the ongoing investigations,
- ensure that national supervisory authorities have adequate human and financial resources and are independent in order to carry out their supervisory and enforcement tasks.

28. The above recommendations of *Homo Digitalis* are in line with the Council of Europe law, and specifically with the principles and the safeguards set out by the Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data[21], and the criteria provided for by the Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector.[22]

[1] The World Bank, Open Data, Individuals using the Internet (% of population), International Telecommunication Union, World Telecommunication/ICT Development Report and database, 2017
[2] 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) recitals 20, 83; **General Data Protection Regulation** (GDPR) (EU) 2016/679, article 6, para. 4e
[3] IACHR (2013). Annual Report of the Office of the Special Rapporteur for Freedom of Expression. Chapter IV (Freedom of Expression and the Internet). OEA /Serv.L/V/II.149, 31 December 2013, para. 109
[4] European Court of Human Rights, K.U. v. Finland. Application no. 2872/02, 2 December 2008, para. 49.
[5] Eurostat, Internet use and frequency of use (% of individuals), 2016.
[6] Eurostat, Internet use by individuals: Different patterns across Member States in managing personal information, 2016.
[7] European 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), 2017.
[8] European Commission, Flash Eurobarometer 443 Report: ePrivacy, p.27, 2016.
[9] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014.
[10] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13.4.2006, p. 54–63.
[11] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014, paras. 56-59.
[12] CJEU, 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, 21 December 2016.
[13] CJEU, 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, 21 December 2016, para. 98.
[14] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014, para. 35. Please, see as regards Article 8 of the ECHR, Eur. Court H.R., Leander v. Sweden, 26 March 1987, para. 48, Rotaru v. Romania [GC], no. 28341/95, para. 46, and Weber and Saravia v. Germany (dec.), no. 54934/00, para 79.
[15] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014, para. 29. Please, see also Joint Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert, para. 47.
[16] CJEU, 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, 21 December 2016, para. 109 and 123.
[17] CJEU, 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, 21 December 2016, para. 92 and 100. Please see, by analogy, CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014, para. 25, 37, and 70.
[18] CJEU, 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, 21 December 2016, para. 212. Please see, by analogy, judgments of 7 May 2009, Rijkeboer, C-553/07, para. 52, and of 6 October 2015, Schrems, C-362/14, para. 95
[19] 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, 21 December 2016, para 108.
[20] 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, 21 December 2016, para 114 and 125.
[21] Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, 28 January 1981, ETS 108.
[22] Council of Europe, Recommendation No. R (87) 15, 198.