HUMAN RIGHTS AND CYBERSECURITY

ROK DACAR
University of Maribor, Faculty of Law, Maribor, Slovenia
rok.dacar@um.si

Abstract The connection between virtual learning environments and human rights can be seen in two ways. On the one hand, non-binding documents set some rights to be implemented by states regarding the functioning of the worldwide web (and consequently also virtual learning environments). On the other hand, intrusions into virtual learning environments may cause violations of human rights, mainly the right to personal data security and the right to privacy and family life. From the vast jurisdiction of the European Union Court of Justice and the European Court of Human Rights, one can find out the pre-conditions for such a district intervention to represent violations of human rights. The aim of this article is to disseminate the relevant know-how to all interested parties, especially students, teachers and other practitioners.

Keywords:
right to privacy and family life, virtual learning environments, right to personal data security, European Court of Human Rights, European Union Court of Justice

University of Maribor Press

DOI https://doi.org/10.18690/um.1.2023.5
ISBN 978-961-286-693-8

1 Introduction

In the past decades, the Internet has grown from an effective work tool to a key component of our lives. Via the Internet, we purchase goods, watch TV programmes, meet partners, access cultural and educational content, and work. During the coronavirus pandemic, its importance grew additionally, as, for many of us, it became the only window to the world placed in isolation and lockdowns. Digital life became almost equal to actual physical life. It is, therefore, no surprise that the Internet can be an environment where serious violations of human rights can occur, while at the same time, the internet is essential for the enjoyment of several fundamental rights. The chapter clarifies some of the more current questions on the relationship between the Internet and human rights that are relevant to virtual learning environments. Firstly, the term cybersecurity and its meaning for society is briefly presented, followed by discussions about some rights connected to the use of the Internet established by the legally non-binding Convention on Human Rights and principles of the Internet. Furthermore, the chapter highlights potential violations of human rights connected to intrusions into virtual learning environments while concentrating on the right to privacy and family life and the right to personal data security, as determined by the Charter of Fundamental Rights of the European Union (henceforth: the Charter) and the European Human Rights Law. The chapter then presents the relevant case Law of the Court of Justice of the European Union (henceforth: CJEU) and the European Court of Human Rights (hereafter: ECHR). Finally, the chapter synthesises the most relevant points of the text.

2 Cybersecurity and Virtual Learning Environments

As the chapter is connected to the term cybersecurity, a short explanation of the subject is in order. There is no single definition of cybersecurity, but we can understand it as "security of systems, networks and programmes from computer attacks usually aiming at access, change or destruction of sensitive data, extorsion of money or interruption of usual commercial flows[1]". Thus, cybersecurity provides a safe virtual learning environment. Effective cybersecurity policies and measures are

[1] Cisco, What is Cybersecurity, accessible under: https://www.cisco. com/c/en/us/ products/ security/ what-is-cybersecurity.html (6.6.2021).

important due to the generally high importance of the digital space in contemporary society, notably for the protection of various social and socio-technical subsystems. In the case of an intrusion into a virtual learning environment, the functioning of an educational system might be endangered (at a time when a vast part of learning activities is done through the Internet, it is not hard to imagine the destructive effect of a cyberattack disabling virtual learning environments), and theft of data (names of participants, e-mail addresses, theft of records of internet camera recordings, theft of uploaded documents, etc.).

2 Online Human Rights

»The Internet has become much more than just a communication tool, as it intertwines with the real world in numerous fields[2]«, human rights and basic liberties being especially relevant for this chapter. Due to this, the *Charter of Human Rights and Principles for the Internet* based on the Declaration of principles at the *WSIS*[3] *(Word Summit of the Information Society)* and at the Tunis Agenda of the *WSIS*[4] were passed*«*. The Convention is not legally binding, and consequently, there are no obligations imposed on national states, the managers of websites, web browsers, etc. The adoption of the above-mentioned acts highlights the importance of the Internet. Also, it represents a domain of values helping us in the search for concrete legal solutions, where the rights mentioned have to be seen as orientations. Of course, in practice, these rights cannot always be guaranteed in all cases. The Convention lists ten basic rights and principles connected to using the Internet (online human rights) that may be transferred to virtual learning environments. They are[5]:

1. Universality and equality – equality and personal freedom of all have to be protected and met on the Internet *(all participants of the virtual learning environment have, e. g., an equal right to participate in debates, discussions, …)*

[2] Moise, ibidem, p. 161.
[3] Two-part world summit of the information society took place within the UNO in 2003 in Geneva and in 2005 in Tunis. At the summit in Tunis the Tunis Declaration proposed by the Internet Governance Forum was adopted and a special platform for the worldwide web, in which various stakeholders were involved, ~~was established~~.
[4] Moise, ibidem, p. 162.
[5] Taken from: Internet Governance Forum, The Charter of Human Rights and Principles for the Internet, accessible under:
https://www.ohchr.org/Documents /Issues/Opinion/ Communications/ Inter netPrinciplesAndRightsCoalition.pdf (6.6.2021).

2. Availability/Accessibility – everybody has an equal right to access a safe and open internet *(all students have a right to access a virtual learning environment disregarding their personal background)*
3. Neutrality – everybody must have access to content on the Internet without prioritisation, discrimination, censuring, filtering and control of traffic *(e.g., certain topics of a virtual learning environment must not be prohibited from discussion)*
4. Respect of human rights – as the Internet is a space for fostering, protecting human rights, everybody must respect the human rights of everyone else in the use of the Internet *(users of a virtual learning environment, for example, are not allowed to humiliate their peers)*
5. Right of expression – everybody has a right to express opinions on the Internet and obtain and seek information without arbitrary interference and surveillance. Everybody has a right to anonymous communication on the Internet *(users of a virtual learning environment may freely express their views on a given topic)*
6. Life, freedom and security – on the Internet, the right to life, freedom and safety have to be respected; these rights may not be violated to interfere with the human rights of other people *(in virtual learning environments there must not be any incitement of dangerous activities)*
7. Privacy – everybody has a right to privacy in the use of the Internet. This includes the right to use the Internet without being subject to surveillance. The individual to whom the data refers must have control over the collecting, storing and use of his or her personal data *(activities in a virtual learning environment are not allowed to be controlled by a third party/organisation)*
8. Diversity – on the Internet, cultural and language diversity must be fostered, and technical innovations should facilitate this *(fostering these values in a virtual learning environment)*
9. Standards of good management – an architecture of the Internet shall be built on standards allowing the simplification and inter-operability of the working environment *(user of the virtual learning environment X can freely access the virtual learning environment Y and transfer its content)*
10. Good management – human rights and social justice shall be the core values on which the Internet functions.

3 Potential Violations of Human Rights Through Virtual Learning Environments

As all of us spend more and more time on the Internet (this almost radically increased during the pandemic of Covid-19 with virtual lectures, video meetings, home office, and such like), resulting in numerous possible violations of human rights by a state. These violations can be caused mainly by state surveillance of the use of the Internet, in our case of virtual learning environments. In connection to this, all of us remember the *Patriot Act*[6] in the USA, which widened the possibilities of surveillance of the cyberlives of citizens after September 11. However, one does not need to go over to the Atlantic Ocean to find an act widening limits of legal surveillance over the Internet, neither do we have to go far back in history, as we may look at France, where, following the terrorist attacks on the satiric revue *Charlie Hebdo* the *Loi relative au renseignement*[7] (an approximate translation might be the Law on Intelligence Activities) was adopted, allowing for a broad and non-discriminatory collection of metadata on the Internet based on searches by individual users, without providing sufficient judicial protection. The stated purpose of both laws is the defence of society from terrorism, that was a clear and present danger at the time of their adoption (i.e., providing for public safety) and not the seeking of non-democratic or autocratic goals. In connection with the two above Acts, questions on the respect of human rights and fundamental freedoms on the Internet (cyberspace) have been raised. Surveillance of user activities in virtual learning environments reaches into numerous human rights areas, like the right to privacy and family life and the right to personal data security are the most endangered rights[8].

[6] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, accessible: https://www. fincen.gov /resources /statutes-regulations/usa-patriot-act (6.6.2021)

[7] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement (1), accessible: https://www. legifrance.gouv.fr/loda/id/JORFTEXT000030931899/ (6.6.2021)

[8] Also interferences in the right to expression, gathering, interferences into various political rights are imaginable, etc.

3.1 Right to Privacy and Family Life and the Right to Protection of Personal Data

The right to privacy and family life is provided by article 8 of the European Convention on Human Rights (henceforth: EHRC) and article 7 of the European Charter on Human Rights (hereafter: the Charter). Article 8 of the EHRC and article 7 of the Charter have the same text, with only the word »correspondence« used by EHRC being replaced by »communication« in the Charter. The reason for the change of words is probably the technological progress within the five decades that passed, from the writing of the text of the ECHR to the adoption of the Charter. In the Charter, the text of article 7 is »Everyone has the right of respect for his or her private and family life, home and communications.«, and in the EHRC », Everyone has the right of respect for his personal and family life, his home and his correspondence.«, whilst article 8 EHRC contains an additional second section determining that »there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others«. The word »correspondence« is interpreted widely by the ECHR. Among others, it entails e-mails[9], the use of the Internet[10], data stored on computer servers[11], etc. The text of the article refers to four values: privacy, family life, inviolability of housing and inviolability of communications or correspondence, respectively. In connection to the security of virtual learning environments, the most relevant of them is the right to inviolability of communications, despite the possibility that an intrusion might also violate another value among the four previously cited. Despite the right to the protection of personal data not being directly mentioned in the ECHR, the ECHR has been guaranteeing it through article 7. In the Charter, the right to protection of personal data is guaranteed by article 8, which states that everyone has the right to the protection of personal data concerning him or her (section 1), that data must be processed fairly for specified purposes, and on the basis of the consent of the person concerned or some other legitimate basis laid

[9] ECHR, Copland vs. UK (62617/00) from 3.7.2007, para. 41 in ECHR, Barbulescu vs. Romania (61496/08) from 5.9.2017, para. 72.
[10] ECHR, Copland vs. ZK (62617/00) from 3.7.2007, para. 41-42.
[11] ECHR, Wieser and Bicos Beteiligungen GmbH vs. Austria (74336/01) from 16.10.2007, para. 45.

down by law and everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified (section 2). Finally, compliance with these rules shall be subject to control by an independent authority (section 3). On the EU level, the right to personal data protection is operationalised mainly through the provisions of the GDRP *(General Data Protection Regulation)* that operationalises various aspects of personal processing data and is presented in more detail in another chapter of this manual.[12]

3.2 Jurisdiction of the ECHR and EUCJ

Since December 2009, when the Charter gained binding value, the CJEU has been competent to decide on violations of human rights guaranteed by the Charter and committed by institutions and bodies of the EU and member states when applying EU law[13]. Where the Charter contains rights that are analogue to the rights from the EHRC, their contents and range are the same as the one determined by the EHRC, and a higher level of security can be assured[14]. If a member of the Council of Europe violates the right to privacy and family life of a citizen, this individual can file a complaint to the ECHR after seizing national courts of justice. The same violation can also be addressed by the CJEU, but only if the violation was committed by an EU member state (all EU member states are also members of the European Council) in the execution of European law. If a violation is committed by a body or institution of the EU, the individual could only seize the CJEU, as the ECHR is not competent for conflicts against European institutions and bodies. As stated, the ECHR is dealing with violations of the right to protection of personal data based on article 8 of the ECHR. The ECHR always interpreted the right to privacy and family life very widely. Thus, in the case of *López Ostra vs. Spain,*[15] it was decided that the right to privacy and family life of the plaintiff was violated by the setting up of a cleaning facility just a short distance from her house, which decreased the quality of her residence and consequently her life.

[12] See Aljoša Polajžar, Personal Data Security (Directives of Education Institutions and Students).
[13] Article 51 section 1 Charter.
[14] Article 52 section 3 Charter.
[15] ECHR, López Ostra vs. Spain (16789/90) from 9.12.1994.

Regarding the Internet, the ECHR found that, due to its general availability and the capability to store a vast amount of information, it plays an important role in enabling the public to obtain information and news of a public character[16], but at the same time poses a danger for human rights (mainly for the right to privacy and family life) that is higher than the one from traditional media[17]. In connection to cybersecurity, the case of *Breyer vs. Germany*[18] must be mentioned, where ECHR recognised that in the context of the fight against organised crime and terrorism and in light of contemporary telecommunication methods and the changes in the communication behaviour of individuals, investigative methods should also be changed. In the case of *Szabó and Vissy vs. Hungary*[19] the ECHR similarly found that regarding the forms of modern terrorism, it is totally understandable that states use the most advanced technologies of mass surveillance of communication with the aim of preventing terrorist attacks. Still, the legal regulation of such measures must contain safeguards against discrimination, and unlimited surveillance must not take place. This was once again stressed by the ECHR in the case of *Zaharov vs. Russia*[20]. In connection to the protection of family life and privacy, the case of *Rotaru vs. Romania*[21] is also important. The ECHR found that the lack of clarity of legal regulation regarding terms of storage and use of data about the privacy of citizens by public authorities represents a violation of the rights guaranteed by the Convention. In the case of *S. and Marper vs. the United Kingdom*[22] the ECHR stressed that modern scientific methods for crime prevention must not be used at any price, and careful balancing of the positive effects of their use and the consequences to the right to privacy is needed. Every state has a leading role in developing such technologies and has a special responsibility to ensure an appropriate balance between the general need of society for crime prevention and the rights of individuals. The term »modern scientific technologies« must be interpreted as including technologies that have the potential to violate the right to family life and privacy and to the protection of personal data, by intrusions in virtual learning environments. In the case of *Gaughran vs. the United Kingdom,* the ECHR stressed that national courts, when deciding on the necessity of a measure violating the right to

[16] ECHR, Times Newspapers Ltd vs. United Kingdom from 10.6.2009, para. 27.
[17] ECHR, M.L. and W.W. vs. Germany (60798/10 and 65599/10) from 28.9.2018, para. 91.
[18] ECHR, Breyer vs. Germany (50001/12) from 30.1.2020, para 88.
[19] ECHR, Szabó and Vissy vs. Hungary (37138/14) from 12.1.2016, para. 68, 73-75.
[20] ECHR, Zaharov vs. Russia (47143/06) from 4.12.2015, para 302-305.
[21] ECHR, Rotaru vs. Romania (28341/95) from 4.5.2000, para. 50.
[22] ECHR, S. and Marper vs. United Kingdom (30562/04 and 30566/04) from 4.12.2008, para. 112.

privacy and family life and the right to personal data protection of an individual, must consider the complexity of the newest technological achievements and their influence[23]. Furthermore, in the case of *Klass vs. Germany* the ECHR decided that data collection on citizens by the government limited to judicial controls (e.g., under-cover investigation approved by the decision of an investigating judge) does not represent a violation of the rights guaranteed by the Convention. The case *Digital Rights Ireland Ltd. vs. Minister of Communications*[24] must also be mentioned, where the CJEU established that the metadata collection on individuals violated their right to the protection of personal data, as it was possible to obtain personal data from metadata. In the case of *Schrems 2*[25], the CJEU examined the forwarding of personal data from an EU member state to the USA and decided that the Decision on the Personal Shield was illegal, as it had doubts that the level of personal data protection in the USA was comparable with the one guaranteed in the EU. In addition, the case of *Tele2/Watson*[26] must be mentioned, where the CJEU decided that »national legislation introducing storage of all traffic and localisation data of all registers of electronic communication users for the purpose of fighting crime generally and non-discriminatory, violates the right to privacy and the right to the protection of personal data. Access to such data has to be limited only to cases of fighting against severe crime. Still, even in that case, an *ex ante* supervision by an independent judicial or administrative institution has to be provided for[27]«.

3.3 What Intervention is Allowed?[28]

Violations of fundamental rights via the intrusion into virtual learning environments are extremely rare. Despite this, based on the above-mentioned case Law, one may conclude what conditions such an intervention must meet to be allowed. In order not to represent a violation of a fundamental right, such an intervention must be, be (i) non-arbitrary, (ii) transparent and (iii) must contain sufficient safeguards.

[23] ECHR, Gaughram vs. United Kingdom (45245/15) from 13.6.2020, para. 96-98.
[24] EUCJ, Compiled matters C-293/12 and C-594/12.
[25] EUCJ, C-311/18.
[26] EUCJ, C-698/15
[27] Privacy International, Tele2/Watson, accessible: https://privacyinternational.org /taxonomy/ term /410 (6.6.2021).
[28] Pre-conditions partially taken from: Cross, ibidem, p. 629-633.

(i) The fundamental rights of individuals could be violated via an intrusion into a virtual learning environment only where some justifiable reason would exist (e.g., a potential terrorist activity, a decision by an investigating judge, and likewise). However, a general gathering of personal data of all users of the virtual learning environment can never be allowed. For example, the intrusion into a virtual learning environment could be justified if its users were potentially preparing terrorist activities (e.g., surveillance concerning jihadist websites via an Internet browser or those who seek computer codes connected to terrorism).

(ii) There must be at least some degree of transparency in the execution of measures with the aim of preventing violations. This can be reached by surveillance of the way of carrying out-measures from an independent institution (e.g., a parliamentary committee). This mainly means that information on the execution of the measures, and technical processes and likewise would not be known only to a narrow circle of people, but also to some external supervisory body.

(iii) This pre-condition, to a certain degree, is connected to the condition of transparency, despite its broader range. While transparency only means that some institution supervises the legality of the measure *ex-post*., the presence of legal safeguards could be satisfied, for e.g., by including the judicial branch in the execution or control of the measures. In connection to this, the French case Loi *relative au renseignement* is to be mentioned as lacking measures on sufficient supervision, as in France, the prime minister directly decides on the more invasive measures and the independent authority (where legal jurisdiction is poorly represented) merely gives advice to him.

If some measure and the execution of it satisfies the previously mentioned pre-conditions, it means that it probably does not violate the right to privacy and family life, but it does not yet mean that it does not violate the right to personal data protection. For a measure not to violate the right to the protection of personal data further conditions have to be met, namely the measure must (iv) be determined specifically enough ahead, and (v)surveillance of its execution by an independent institution must also be present.

(iv) An exact determination of data to be collected is necessary to stop possible violations that might occur if all sorts of data could be obtained. A violation might happen, if, for example, the data on the content of the communication between a lawyer and a client, a reporter and his or her confidential source, etc. would be collected. As such communication (in principle) is not done within virtual learning environments, this condition is of limited relevance to this article.

(v) Article 8 section 3 of the Charter explicitly requires that the respect of the right to the protection of personal data is supervised by an independent authority. Demand for supervision by an independent authority is mainly contained in the pre-conditions under (ii) and (iii), already mentioned above.

These conditions are not permanently set in stone, and in line with the margin of appreciation doctrine, a certain freedom in the carrying out of the measures is granted to the member state of the Council of Europe, whilst the states must achieve »a fair relation between protection of the general public interest and respect of human rights, where the latter has to be subject to special attention[29]«.

4 Conclusion

This article explained that the development of the Internet has a potential influence on fundamental rights. On the one hand, programme documents emerge determining (online human) rights to guarantee undisturbed, equal, fair, etc. access to the Internet and consequently also to virtual learning environments. On the other hand, the Internet offers yet unseen possibilities for the violations of human rights. The contribution mainly dealt with the right to privacy and family life and the right to the protection of personal data. Still, one could also imagine intrusions into virtual learning environments violating other human rights, e.g., the freedom of association and the freedom of expression. In the past decade, the CJEU and the ECHR developed a vast body of case Law. Based on it we can conclude under which conditions intrusions into virtual learning environments would be allowed and even more importantly, what conditions must be met by an intervention, so it does not

[29] ECHR, subject »Relating to certain aspects of the Laws on the use of languages in education in Belgium« vs. Belgium (474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64), from 23.7.1968, chapter B, para. 5.

represent a violation of human rights. It must be stressed again that intrusions into the cybersecurity of virtual learning environments are extremely rare.

References

»Relating to certain aspects of the Laws on the use of languages in education in Belgium« vs. Belgium (474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64) from 23.7.1968.

Adrian Cristian Moise: Cybersecurity and Human Rights, v: Revista Universul Juridic 2016, no. Supplement (2016).

Cisco, What is Cybersecurity, accessible under: https:// www.cisco.com /c/en/us /products /security/what-is-cybersecurity.html (6.6.2021).

ECHR, Barbulescu vs. Romania (61496/08) from 5.9.2017.

ECHR, Breyer vs. Germany (50001/12) from 30.1.2020, para 88.

ECHR, Copland vs. UK (62617/00) from 3.7.2007.

ECHR, Gaughram vs. United Kingdom (45245/15) from 13.6. 2020, para. 96-98.

ECHR, López Ostra vs. Spain (16789/90) from 9.12.1994.

ECHR, M.L. and W.W. vs. Germany (60798/10 and 65599/10) from 28.9.2018, para. 91.

ECHR, Rotaru vs. Romania (28341/95) from 4.5.2000, para. 50.

ECHR, S. and Marper vs. United Kingdom (30562/04 and 30566/04) from 4.12.2008, para. 112.

ECHR, Szabó and Vissy vs. Hungary (37138/14) from 12.1.2016, para. 68, 73-75.

ECHR, Times Newspapers Ltd vs.United Kingdom from 10.6.2009, para. 27.

ECHR, Wieser and Bicos Beteiligungen GmbH vs. Austria (74336/01) from 16.10.2007.

ECHR, Zaharov vs. Russia (47143/06) from 4.12.2015, para 302-305.

Internet Governance Forum, The Charter of Human Rights and Principles for the Internet, accessible under: https://www.ohchr.org/Documents /Issues/Opinion/ Communications/ Internet Principles And Rights Coalition.pdf (6.6.2021).

Jennifer Cross: Cybersecurity and the Rights of the Internet User in France, v: Georgia Journal of International and Comparative Law, let. 45, no. 3 (2017).

Loi n° 2015-912 du 24 juillet 2015 relative au renseignement (1), accessible: https: //www.legifrance.gouv.fr/lo da/id/JORFTEXT000030931899/.

Privacy International, Tele2/Watson, accessible: https://privacy inte rnati o nal.org/taxonomy/term/410 (6.6.2021).

EUCJ, C-311/18.

EUCJ, C-698/15

EUCJ, Compiled matters C-293/12 and C-594/12.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, accessible: https://www.fincen.gov/resources/statutes-regulations/ usa-patriot-act.