OSCE TRAINING GUIDE FOR
CRIMINAL JUSTICE PRACTITIONERS

Ensuring Human Rights Compliance in Cybercrime Investigations

OSCE Organization for Security and Co-operation in Europe

Vienna, October 2023
© OSCE 2023

All rights reserved. The content of this publication may be freely used and copied for educational and other non-commercial purposes, provided that any such reproduction be accompanied by an acknowledgment of the OSCE as the source.

ISBN: 978-92-9271-245-7

Published by:
OSCE Secretariat
Transnational Threats Department
Strategic Police Matters Unit

Wallnerstrasse 6
1010 Vienna, Austria
Tel: +43-1 514 36 180
Fax: +43-1 514 36 105
email: info@osce.org | spmu@osce.org

www.osce.org

OSCE TRAINING GUIDE FOR
CRIMINAL JUSTICE PRACTITIONERS

Ensuring Human Rights Compliance in Cybercrime Investigations

Organization for Security and
Co-operation in Europe

ACKNOWLEDGEMENTS

This training guide was developed by the OSCE Secretariat's Transnational Threats Department/Strategic Police Matters Unit (TNTD/SPMU), with input from the OSCE Office for Democratic Institutions and Human Rights (ODIHR). TNTD/SPMU would like to thank Mr. Robert Golobinek and Mr. Hein Dries for their contributions to drafting this guide. The guide was developed under the OSCE extra-budgetary project "Capacity Building on Combating Cybercrime in Central Asia" funded by the United States of America, Germany and the Republic of Korea.

CONTENTS

ACRONYMS

CJEU	Court of Justice of the European Union
CoE	Council of Europe
CSCE	Conference for Security and Co-operation in Europe
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
FATF	Financial Action Task Force
GPS	Global Positioning System
ICCPR	International Covenant on Civil and Political Rights
IP address	Internet Protocol Address
ISP	Internet Service Provider
NGO	Non-Governmental Organization
ODIHR	Office for Democratic Institutions and Human Rights (of the OSCE)
OHCHR	Office of the United Nations High Commissioner for Human Rights
OSCE	Organization for Security and Co-operation in Europe
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
VPN	Virtual Private Network

INFO BOXES

1

Introduction

Our societies increasingly rely on digital technologies in all aspects of life, from business, science and education, to communication, travel, recreation and entertainment. Rapid evolution of these technologies in recent years has brought many opportunities, but also new security risks and challenges. One area that has been significantly affected by these developments is crime.

Digital technologies have transformed the criminal landscape. They have given rise to new forms of crime (e.g., cyber-dependent crime such as ransomware, phishing, cryptojacking) and altered the way existing forms of crime are committed (e.g., cyber-enabled crime such as online sexual exploitation or online trade in illicit goods and services). Many digital technologies have also become useful tools for traditional crimes in the physical world (e.g., burglary, theft and fraud). Furthermore, the widespread use of digital devices (personal computers, laptops, tablets, mobile phones, smartwatches, etc.) means that electronic evidence now plays an important role in almost all types of criminal investigation.

Cybercrime has some specific features that make investigations of cybercrimes different from investigations of other types of offences. In particular, a criminal does not need to be physically present at a crime scene or near a victim, and can be located in a foreign jurisdiction. In addition, the internet provides many opportunities for criminals to hide their identities behind nicknames and stolen credentials, and various encryption or anonymization tools can be used to conceal criminal activity. Cryptocurrencies allow users to make secure payments without a direct link to a real-world identity, making it easier to purchase illicit goods and services and launder the proceeds of crime.

Identifying, seizing and analysing electronic evidence of a cybercrime or other type of crime is also different in many respects from handling physical evidence. Relevant electronic evidence may not be stored on an individual device but on cloud servers controlled by private companies, which are often based abroad. Moreover, electronic data is volatile, and can be easily moved, altered or deleted.

Cybercrime[1] and electronic evidence thus pose significant challenges to criminal justice systems and the rule of law across the OSCE region. Investigating cybercrime and electronic evidence requires specific knowledge and skills, adequate technical means and legislative frameworks, as well as effective and efficient international co-operation with foreign criminal justice actors and private entities. States have been adapting to these developments by amending their laws, building their technical capacities and introducing new procedural investigative powers. All these measures and tools must be developed and deployed in line with States' responsibilities under international human rights law.

As with any other criminal investigation, cybercrime investigations and the use of particular procedural powers affect the human rights and freedoms set out in international instruments at the global and regional levels. These include the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR).

While these rights and freedoms must be respected and protected in any criminal investigation, this need is perhaps even more pertinent in the context of cybercrime and electronic evidence. The data that digital devices and online services collect about their users is unprecedented in both

Note: All electronic resources were accessed on 1 June 2023.

1 In this text, "cybercrime" is used as an umbrella term that refers to both cyber-dependent and cyber-enabled crimes, unless specified otherwise.

scope and volume. This data can provide many personal details about people's lives, including their health, economic activity, private relations, and political preferences. When collecting electronic evidence during an investigation, criminal justice practitioners frequently find relevant evidence alongside large amounts of other, often personal, data. This type of investigation is thus potentially much more intrusive than traditional "offline" investigations which only collect physical evidence.

Awareness of the human rights implications of cybercrime investigations and other investigations involving electronic evidence is therefore important for police investigators, prosecutors and judges. The violation of human rights during criminal investigations and proceedings might lead to wrongful conviction, or to evidence being dismissed resulting in the acquittal of a perpetrator. Lack of respect for human rights also undermines trust at the national and international levels. It is an obstacle to international co-operation, both with law enforcement and other authorities in partner countries, as well as with private companies located abroad. Furthermore, respecting and protecting human rights in practice helps to strengthen trust between criminal justice authorities and wider society, and so encourages individuals to co-operate with – and provide important information to – cyber-crime investigators. Taking a human rights-based approach therefore increases the effectiveness of cybercrime investigations.

This Guide aims to raise awareness among criminal justice practitioners of the implications that the investigation of cybercrimes and other crimes involving electronic evidence can have for human rights, and to support them to uphold human rights in their daily investigative work. It does so by focusing on those human rights that are particularly affected by investigations of cybercrimes and other crimes involving electronic evidence, namely:

- The right to privacy;
- The right to a fair trial;
- The right to freedom of expression/speech;
- The right to the protection of property.

The Guide draws on the jurisprudence of the European Court of Human Rights (ECtHR) and, occasionally, the Court of Justice of the European Union (CJEU) to explain and illustrate how human rights apply in the context of cybercrime investigations and in the collection and use of electronic evidence.

8

2

Human rights legal framework applying to cybercrime investigations

2.1 WHAT ARE HUMAN RIGHTS?

Human rights are legal entitlements of individuals for the protection of their dignity and freedoms. They are inherent to all human beings, without distinction as to race, colour, gender, language, religion, political or other opinion, national or social origin, property, birth or any other status. All human rights, whether they are civil and political rights (such as the rights to life, equality before the law and freedom of expression); economic, social and cultural rights (such as the rights to work, social security and education); or collective rights (such as the rights to development and self-determination) are indivisible, interrelated and interdependent. The improvement of one right facilitates advancement of the others.

Universal human rights are expressed and guaranteed by law in the form of treaties, customary international law, general principles and other sources of international law. International human rights law imposes specific obligations on States, including parliaments, ministries, local authorities, law enforcement and criminal justice authorities, as the “duty bearers” responsible for respecting, protecting and fulfilling human rights. This includes both so-called “negative” obligations to refrain from certain acts (e.g., from unlawfully interfering in a person's private life), as well as the responsibility to take “positive” actions to protect a person's rights (e.g., by effectively investigating and prosecuting crimes) and promote human rights and fundamental freedoms (e.g., by providing public information and training for relevant state officials).

2.2 INTERNATIONAL HUMAN RIGHTS LEGAL INSTRUMENTS AND BODIES

States recognized the importance of the protection of human rights after World War II with the establishment of the United Nations (UN) and the Council of Europe (CoE) and the elaboration of international human rights instruments within the framework of these organizations. The European Union (EU) has also highlighted the importance of human rights by adopting a dedicated human rights charter. Box 1 presents the international human rights legal instruments particularly relevant in the context of cybercrime.

BOX 1 INTERNATIONAL HUMAN RIGHTS LEGAL INSTRUMENTS PARTICULARLY RELEVANT TO CYBERCRIME INVESTIGATIONS

- Universal Declaration of Human Rights of 1948[2] (UDHR) of the UN (in particular Articles 8–11, 12 and 19);
- International Covenant on Civil and Political Rights of 1966[3] (ICCPR) of the UN (in particular Articles 14, 17 and 19);
- European Convention on Human Rights of 1950[4] (ECHR) of the CoE (in particular Articles 6, 8 and 10);
- Charter of Fundamental Rights of the European Union[5] of 2000.

Annex 1 presents the full text of the ICCPR and ECHR articles mentioned above.

With the exception of the Holy See, all OSCE participating States have ratified the ICCPR and are therefore bound by its provisions. The majority of OSCE participating States are also members of the CoE and thus parties to the ECHR. Some OSCE participating States are also EU Member States and are therefore bound by the Charter of Fundamental Rights of the European Union when they are implementing EU law (Article 51, paragraph 1 of the Charter).

There are a number of human rights institutions mandated to interpret and promote the human rights enshrined in these legal texts. At the UN level, the Human Rights Committee is the treaty body of the ICCPR. It is composed of 18 independent experts who monitor the implementation of the ICCPR by its States Parties.[6] It reviews the implementation of the Covenant through periodic reports, and can examine individual complaints regarding alleged violations of the ICCPR by States that have acceded to the Optional Protocol to the Covenant.[7]

At the regional level, the European Court of Human Rights (ECtHR) adjudicates on applications lodged by individuals, groups of individuals, or one or more of the CoE member States, alleging violations of the rights set out in the ECHR. While the judgments of the ECtHR are legally binding on CoE member States concerned, its jurisprudence can also provide important guidance to other countries regarding the scope and application of civil and political rights. The Court of Justice of the European Union (CJEU) interprets EU law, including the Charter of Fundamental Rights of the European Union.[8] Its judgments are legally binding on EU member States.

Other bodies have an advisory mandate to strengthen the promotion and protection of human rights. At the international level, these include the UN Human Rights Council[9] and the various

2 *Universal Declaration of Human Rights*, 10 December 1948, UN General Assembly Res. 217 A (III).

3 *International Covenant on Civil and Political Rights*, 16 December 1966, UN General Assembly Res. 2200A (XXI), entered into force on 23 March 1976.

4 *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, CETS No. 5, entered into force on 3 September 1953.

5 *Charter of Fundamental Rights of the European Union*, 18 December 2000, OJEC 2012/C 326/02, entered into force on 1 December 2009.

6 OHCHR (no date), *Human Rights Committee*, available at https://www.ohchr.org/en/treaty-bodies/ccpr.

7 *Optional Protocol to the International Covenant on Civil and Political Rights*, 16 December 1966, UN General Assembly Res. 2200A (XXI), entered into force on 23 March 1976.

8 *Protocol 3 on the Statute of the Court of Justice of the European Union*, 16 December 2004, OJEU C 310/210.

9 *UN Human Rights Council*, 15 March 2006, UN General Assembly Res. 60/251, replacing the UN Commission on Human Rights on 16 June 2006.

special procedures established under it, including special rapporteurs, special representatives, independent experts and working groups.[10] In addition, the Office of the UN High Commissioner for Human Rights (OHCHR) promotes and protects all human rights through research, education, advocacy and assistance to governments.

Respect for human rights and fundamental freedoms are also key to the OSCE's comprehensive concept of security. Since the signing of the Helsinki Final Act in 1975, the Conference for Security and Co-operation in Europe (CSCE) and subsequently the OSCE have accumulated a substantial body of commitments in the fields of human rights, democracy, rule of law and national minorities adopted by various CSCE, and later OSCE, decision-making bodies.[11] Many of these commitments have relevance for the work of criminal justice institutions, including in the context of investigating and prosecuting cybercrimes and other crimes involving electronic evidence. Although the OSCE commitments do not have the character of legally binding treaties under international law, they represent important politically binding commitments, adopted by consensus by all participating States.

2.3 NATIONAL HUMAN RIGHTS LEGISLATION AND INSTITUTIONS

To be effective, international human rights standards need to be implemented and protected by national legislation, policy and practice. Ensuring that the national legislative framework reflects and incorporates international human rights standards is primarily a task for legislators. Typically, human rights protections are integrated in a country's constitution and other cross-cutting or sector-specific legislation. Procedural rights are generally incorporated into criminal procedure codes through various conditions and safeguards.

National human rights legislation is interpreted by national courts, including – where constitutional provisions are concerned – constitutional courts. The body of national case law provides important guidance on how domestic human rights legislation should be applied in practice.

National human rights bodies (such as national human rights institutions or ombudspersons) also have an important function in the protection of human rights at the national level by providing advice and acting on individual cases of violations. In addition, civil society, including non-governmental organizations (NGOs) and the media, play a crucial role in raising awareness of human rights, advocating for public interests and promoting public scrutiny of human rights compliance.

10 UN Human Rights Council (no date), *Special Procedures of the Human Rights Council*, available at https://www.ohchr.org/EN/HRBodies/SP/Pages/Welcomepage.aspx.

11 For a comprehensive overview, see OSCE/ODIHR, *OSCE Human Dimension Commitments: Volume 1 - Thematic Compilation*, 4th edition (Warsaw, 2023); and OSCE/ODIHR, *OSCE Human Dimension Commitments: Volume 2 - Chronological Compilation*, 4th edition (Warsaw, 2023).

3

Human rights and cybercrime investigations

3.1 WHY ARE HUMAN RIGHTS IMPORTANT IN THE CONTEXT OF CYBERCRIME INVESTIGATIONS?

State actors, including ministries and criminal justice practitioners, have primary responsibility to respect, protect and fulfill human rights. This includes ensuring the implementation in practice of the human rights standards included in international conventions to which the State is a party. States' obligations apply to all aspects of the criminal justice response to cybercrime. They include ensuring that domestic legislation is human rights-compliant and contains the necessary procedural safeguards, making practitioners aware of their responsibility to uphold human rights, monitoring the implementation of human rights in practice, and providing individuals with avenues for recourse when their human rights have been violated.

In addition to being a responsibility under international law, upholding human rights has clear practical benefits for cybercrime investigations and the work of criminal justice authorities in general, as the following examples show.

Firstly, respect for human rights is important for securing necessary evidence from abroad and enabling international co-operation between criminal justice authorities and with private companies. Failure to abide by human rights standards can, for example, be a reason for refusing a mutual legal assistance request. For many States, a prerequisite for providing formal assistance is that the requesting State guarantees a fair trial and respects the human rights laid down in international and regional human rights instruments. Private companies, including major service providers such as Microsoft, Google or Meta, also consider a State's human rights record when deciding how to respond to a request to preserve or share data for use in a criminal investigation.[12]

Secondly, non-compliance with human rights and procedural safeguards when conducting an investigation can result in evidence being deemed inadmissible in court. This is particularly relevant in cybercrime investigations, which may involve intrusive investigative techniques and rely on volatile electronic evidence. Ensuring that human rights standards are applied throughout an investigation therefore increases the likelihood of a successful conviction of perpetrators.

Thirdly, criminal justice authorities that fail to conduct cybercrime investigations in line with human rights standards can be subject to complaints procedures or legal action. Individual police officers and managers, for example, could face administrative or criminal sanctions if they are involved in investigations that are found to have been conducted unlawfully. This can have a damaging effect on authorities' morale and reputation, as well as on the likelihood of securing the conviction of perpetrators of cybercrimes.

Finally, violations of human rights during cybercrime investigations can lead to a loss of public trust in criminal justice authorities, making it more difficult to achieve the co-operation necessary to effectively counter cybercrime. A lack of trust not only undermines actions to prevent cyber-crime but can also negatively impact the public's willingness to report such crimes or provide witness statements. Respecting and protecting human rights in the context of cybercrime investigations is therefore essential to ensure that efforts to combat cybercrime are sustainable, effective, and ultimately successful.

12 See e.g., UNODC, *Practical Guide for Requesting Electronic Evidence across Borders* (Vienna, 2021), p. 18, 37.

3.2 HUMAN RIGHTS PARTICULARLY AFFECTED BY CYBERCRIME INVESTIGATIONS

Cybercrime investigations may impact the enjoyment of numerous human rights. The following human rights are particularly relevant in the context of cybercrime investigations:

- The right to privacy;
- The right to a fair trial;
- The right to freedom of expression/speech;
- The right to the protection of property.

The full text of the ICCPR and ECHR articles setting out these rights can be found in Annex 1.

Other rights that may be directly or indirectly affected by cybercrime investigations include: non-discrimination, freedom of religion or belief, freedom of association, right to liberty, and the rights of the child.

RIGHT TO PRIVACY

The right to privacy is set out in ICCPR Article 17 and ECHR Article 8, where it is referred to as the right to respect for private and family life. In addition to their obligations under these instruments, the OSCE participating States have committed themselves in the 1991 Moscow Document to the right to the protection of private and family life, domicile, correspondence and electronic communications, as well as to the prevention of arbitrary intrusion in the realm of the individual.[13]

The right to privacy is instrumental in a democratic society. It includes the protection of the privacy of messages, phone calls and emails, as well as protection against unlawful and unnecessary state surveillance. To fulfil the right to privacy, States have both a positive obligation (to protect the right) and a negative obligation (to refrain from interference in the right). The right to privacy also enables individuals to take steps to protect their private life, for example by making use of privacy-enhancing technologies such as encryption and virtual private networks (VPNs).

The importance of the right to privacy means that it has been described as a "gateway right." Without privacy, the full enjoyment of a broad range of other rights is compromised, for example, to express one's opinions, to associate with others or to participate freely in public and political life.[14]

Data protection is an important part of the right to privacy, as recognized by the UN Human Rights Committee[15] and the ECtHR.[16] A number of international and regional instruments contain

13 OSCE/CSCE, *1991 Moscow Document*, 3 October 1991, CSCE/CHDM.49/Rev.1, para 24; OSCE/CSCE, *1990 Copenhagen Document*, 27 June 1990, CSCE/CHDC.43, para 26, note 16.

14 OHCHR (2018), *Universal Declaration of Human Rights at 70: 30 Articles on 30 Articles, Article 12*, available at: https://www.ohchr.org/en/press-releases/2018/11/universal-declaration-human-rights-70-30-articles-30-articles-article-12.

15 See UN Human Rights Committee, *General Comment No. 16 on Article 17, Right to privacy*, 8 April 1988, U.N. Doc. HRI/GEN/1/Rev.1, p. 21–23, para 10.

16 ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Strasbourg, 2022); see also ECtHR (2023), *Factsheet on Personal Data Protection*, available at https://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

specific data protection principles that need to be respected to ensure full compliance with the right to privacy.[17] These include, for example, the principles that personal data undergoing automatic processing shall be:

- Obtained and processed fairly and lawfully;
- Stored for specified and legitimate purposes (purpose limitation);
- Adequate, relevant and not excessive (data minimization);
- Preserved for no longer than is required (limited data retention);
- Protected against unauthorized access.

As with many rights, the right to privacy is not absolute and can be limited in certain circumstances. Any interference with the exercise of this right must be **based in law**, **necessary** in a democratic society, such as to protect national security or public safety or for the prevention of disorder or crime, and **proportionate** (see also section 3.3). For example, the police may be permitted by a competent judicial authority to intercept an individual's communications if they have reasonable grounds to believe that the individual is about to commit a serious crime.

RIGHT TO A FAIR TRIAL

The right to a fair trial is a key element of human rights protection and serves as a procedural means to safeguard the rule of law.[18] Both ICCPR Article 14 and ECHR Article 6 set out a number of distinct requirements that together make up the right to a fair trial, including that everyone charged with a criminal offence:[19]

- Is entitled to a fair and public hearing by an independent and impartial tribunal;
- Should be presumed innocent until proved guilty according to law;
- Should have adequate time and facilities to prepare their defence;
- Should be able to defend themselves in person or through legal assistance of their own choosing;
- Should be tried within a reasonable time without undue delay.

Certain elements of the right to a fair trial can be limited under certain conditions. Others – such as the presumption of innocence, the entitlement to a hearing by a competent, independent and impartial tribunal, as well as the requirement for the trial as whole to be fair – are considered absolute and cannot be limited under any circumstances.[20]

17 See, e.g., *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, CETS No.108; EU Charter of Fundamental Rights, Article 8 in combination with EU General Data Protection Regulation, 27 April 2016, Reg. (EU) 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and the Free Movement of such Data.

18 See UN Human Rights Committee, *General Comment No. 32 on Article 14: Right to equality before courts and tribunals and to a fair trial*, 23 August 2007, UN Doc. CCPR/C/GC/32, para 2.

19 ECtHR, *Guide on Article 6 of the European Convention on Human Rights: Right to a fair trial (criminal limb)* (Strasbourg, 2022).

20 See UN Human Rights Committee, *General Comment No. 32 on Article 14: Right to equality before courts and tribunals and to a fair trial*, 23 August 2007, UN Doc. CCPR/C/GC/32, para 6, 19.

RIGHT TO FREEDOM OF EXPRESSION

Freedom of expression, as set out in ICCPR Article 19 and ECHR Article 10, is one of the essential foundations of a democratic society. It includes the right to seek, receive and share information and ideas through any media, regardless of frontiers, and without interference by public authority. Importantly, freedom of expression applies not only to information and ideas that are favourably received, but also to those that may offend or disturb.[21] OSCE participating States reaffirmed that "everyone will have the right to freedom of expression including the right to communication," and "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."[22]

Freedom of expression may be subject to exceptions in limited circumstances, for example to protect national security or public order, or to prevent disorder or crime. Case law emphasizes that these exceptions must be interpreted narrowly. This helps to avoid excessive interference and a so-called "chilling effect," where individuals self-censor for fear of being subjected to criminal proceedings (see box 4).

The internet has created new opportunities for individuals to exercise their right to freedom of expression by sharing information very widely and at an unprecedented speed. Because of its accessibility and its ability to store and transmit vast amounts of information, the internet plays an important role in improving public access to news and facilitating the dissemination of information.[23] These benefits are, however, accompanied by a number of dangers, in particular that unlawful speech, including hate speech and speech inciting discrimination, hostility or violence, can spread globally in a matter of seconds and often remains permanently available online.[24]

As in the offline world, States have a duty to ensure that any limitations to online expression are are **prescribed by law**, **necessary** and **proportionate**.[25]

RIGHT TO THE PROTECTION OF PROPERTY

The ECHR establishes that people – and companies – have the right to possess property that is lawfully theirs. This includes the physical objects one owns, financial resources such as bank deposits and shares, as well as intellectual property.[26] Property also encompasses virtual assets such as cryptocurrencies.

States cannot deprive individuals or companies of their property unless it is in the public interest and subject to conditions set out in law.

---

21 CoE Department for the Execution of Judgments of the European Court of Human Rights, *Thematic factsheet: Freedom of expression*, April 2021, available at https://rm.coe.int/thematic-factsheet-freedom-expression-eng/1680a235d0.

22 CSCE/OSCE, *1990 Copenhagen Document*, 27 June 1990, CSCE/CHDC.43, para 9.1.

23 See, e.g., ECtHR, *Delfi AS v. Estonia* [GC], 10 October 2013, No. 64569/09, § 133; ECtHR, *Times Newspapers Ltd (No. 1 and 2) v. the United Kingdom*, 10 March 2009, No. 3002/03 and 23676/03, § 27.

24 See, e.g., ECtHR, *Delfi AS v. Estonia* [GC], 10 October 2013, No. 64569/09, § 110; ECtHR, *Annen v. Germany*, 20 September 2018, No. 3682/10, § 67.

25 OHCHR (no date), *Factsheet on Freedom of Opinion and Expression*, available at https://www.ohchr.org/sites/default/files/Documents/Issues/Expression/Factsheet_1.pdf.

26 CoE Department for the Execution of Judgments of the European Court of Human Rights, *Thematic factsheet on protection of property*, June 2022, available at https://rm.coe.int/thematic-factsheet-protection-of-property-eng/1680a6f07f.

3.3 THE PRINCIPLES OF LEGALITY, NECESSITY AND PROPORTIONALITY

Most human rights, including the right to privacy and freedom of expression, are not absolute and can be limited in specific circumstances. It is a well-established principle of international human rights law that any such restrictions on a right must be prescribed by law, necessary and proportionate.

The principle of **legality** requires that any measure restricting a right must have a basis in national legislation. This legal basis must be accessible to those liable to be affected and sufficiently clear to inform individuals adequately about the circumstances and conditions under which public authorities are entitled to resort to measures affecting their rights. The legislation must contain adequate safeguards against arbitrary application and must not confer excessive discretion on the officials entrusted with its application.

The principle of **necessity** comprises two elements. Firstly, any limitation of a right must **pursue a legitimate aim**. Some rights specify these legitimate aims. For example, the ECHR allows the right to respect for private and family life and the right to freedom of expression to be limited in the interests of national security, public safety or for the prevention of disorder or crime, among other aims. Secondly, the limitation must be restricted to what is **necessary to achieve this aim**. In other words, the limitation must not be overly broad or last longer than is necessary to achieve the aim, i.e., it must be narrowly defined and of limited duration.

The **proportionality** principle means that any measure that interferes with a right must be proportionate to the legitimate aim being pursued. This requires demonstrating that no less restrictive measures are available, that the essence of the right is preserved and that the limitation on the right is not discriminatory. The existence and effective application of procedural safeguards is a key aspect of determining whether the limitation of a right is proportionate.

4

Cybercrime-specific procedural powers and human rights safeguards

4.1 SPECIFICITIES OF CYBERCRIME INVESTIGATIONS

Investigating and successfully prosecuting cybercrimes and other crimes involving electronic evidence poses specific challenges to criminal justice practitioners. Firstly, as physical presence or proximity to a victim is not required to commit cybercrimes, perpetrators can be in a different national jurisdiction to their victims. Indeed, there may be multiple perpetrators, each located in a separate jurisdiction.

Secondly, criminals are increasingly hiding their identities by using services such as Tor or Virtual Private Networks (VPNs), which enable them to use internet resources with relative anonymity. They also use various encryption tools to secure their data and communication, and to conceal their criminal activities. Mobile network operators use technologies such as Network Address Translation, which make it difficult to identify internet users by their Internet Protocol (IP) addresses. All of this makes the attribution of criminal acts in cyberspace increasingly challenging.

In addition, most evidence of cybercrimes – and indeed crucial evidence of many offline crimes – is in the form of digital data, which is inherently volatile and can be easily moved, altered or deleted. Furthermore, data is often stored in the "cloud" on servers that may be located in one or more foreign jurisdictions. A variety of private service providers can have access to, or control over, the digital traces and electronic evidence related to the crime being investigated.

This means that investigating cybercrimes often requires intensive international co-operation – with both criminal justice actors from other countries and private entities such as multinational service providers. Certain types of cybercrime, for example ransomware or business email compromise, also require a combination of financial and digital investigations.

4.2 PROCEDURAL AND INTERNATIONAL CO-OPERATION POWERS IN RELATION TO CYBERCRIME

The specificities related to the investigation of cybercrimes or other crimes involving electronic evidence prompt a number of questions such as:

- Who is/was using a specific IP address (static or dynamic) at a given time?
- Who is/was using a specific email address or nickname in a blog or social network?
- What are the conditions for retaining traffic data, including dynamic IP addresses, by service providers and under what conditions may criminal justice actors obtain such data?
- How to obtain data about a user account and/or content data from a multinational service provider based abroad?
- How to access, seize and investigate the content of electronic communication (e.g., email or messaging applications) or the data from various electronic devices, including those that are encrypted?

- How to monitor (online) encrypted communication?
- How to detect and trace online wealth, electronic money transfers and cryptocurrency transactions?
- How to seize cryptocurrencies or other virtual assets?

While the investigation of cybercrime follows the same procedural rules as any other criminal investigation, as defined in relevant national legislation, getting answers to these questions may in addition require investigators to have access to particular procedural powers.

The 2001 CoE Convention on Cybercrime, also known as the Budapest Convention, is the first international treaty on crimes committed via the internet and other computer networks.[27] It is open to ratification/accession by States that are not CoE members, and has been ratified by a large number of States across different regions, including a majority of the OSCE participating States. The Convention provides for specific powers relevant to the collection and use of electronic evidence, as well as to international co-operation in the context of cybercrime investigations. These powers apply both to cyber-dependent and cyber-enabled crimes, and to any other crime involving electronic evidence.

The Convention requires States Parties to integrate into their domestic legislation a number of investigative powers for the purpose of criminal investigations or proceedings. These are:

- Expedited preservation of stored computer data (Article 16);
- Expedited preservation and partial disclosure of traffic data (Article 17);
- Production order (Article 18);
- Search and seizure of stored computer data (Article 19);
- Real-time collection of traffic data (Article 20);
- Interception of content data (Article 21).

The Convention also contains provisions that form the basis for international co-operation in combating cybercrime. These include:

- Spontaneous information (Article 26);
- Expedited preservation of stored computer data (Article 29);
- Expedited disclosure of preserved traffic data (Article 30);
- Mutual assistance regarding accessing of stored computer data (Article 31);
- Mutual assistance in the real-time collection of traffic data (Article 33);
- Mutual assistance regarding the interception of content data (Article 34).

In addition, the Second Additional Protocol to the Budapest Convention was opened for signature by Parties to the main Convention in May 2022. It introduces new procedures for enhancing direct co-operation with providers and entities in other contracting Parties, and for streamlining

27 *Convention on Cybercrime*, 23 November 2001, CETS No. 185, entered into force on 1 July 2004.

international co-operation between authorities for the disclosure of stored computer data, including with respect to emergency mutual assistance.[28]

These powers provide criminal justice practitioners with important tools to successfully detect, investigate and prosecute criminal offences committed against or using computers. However, their application may interfere with human rights and fundamental freedoms. Investigators making use of these powers have a responsibility to ensure that any limitations to human rights are based in law, necessary and proportionate.

4.3 CYBERCRIME-SPECIFIC HUMAN RIGHTS SAFEGUARDS

While the provisions of international and regional human rights standards apply to all criminal investigations, the CoE Convention on Cybercrime seeks to apply them specifically to investigations of cybercrimes and other crimes involving electronic evidence. Article 15 of the Convention requires each Party to establish in its domestic law certain conditions and safeguards to be applied when making use of the Convention's procedural powers (see box 2).

Article 15 does not specify these safeguards in detail, but instead refers to States' obligations under the ECHR and the ICCPR as the source of the safeguards. This ensures the provision accounts for the significant differences that exist in different legal traditions concerning the way safeguards are implemented.

BOX 2 CYBERCRIME CONVENTION ARTICLE 15 – CONDITIONS AND SAFEGUARDS

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to **conditions and safeguards** provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall **incorporate the principle of proportionality**.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, **include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.**
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section **upon the rights, responsibilities and legitimate interests of third parties.**

28 *Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence*, 17 November 2021, CETS No. 224.

Article 15 highlights the following conditions and safeguards:

- The principle of proportionality;
- The availability of judicial or other independent supervision;
- The need to specify clear grounds justifying an application;
- The limitation of the scope and the duration of the power or procedure – as appropriate in view of the power and the case at hand;
- The need to consider the impact of the power upon the rights, responsibilities and legitimate interest of third parties.

In practical terms, this means that officers investigating alleged cybercrimes must be aware of the impact that their actions have on the rights set out in international human rights treaties.

The principle of proportionality entails balancing different and competing investigative measures in relation to a specific cybercrime investigation. It means that interferences with human rights must be minimized and that investigators must use the least intrusive means for achieving their aim.

Such a balance is only possible if different – less and more intrusive – options exist in national legislation. For example, there are two possible methods to gain access to data stored by a service provider. One is to use a preservation and production order; the other is to use search and seizure to obtain the data. Generally, the preservation and production order mechanism is less intrusive than search and seizure, which requires access to a larger data set and is usually conducted on site. Investigators must clearly justify why they are using a more intrusive investigative method when less intrusive methods are available.

In any case, investigators must provide sufficient grounds for a court or an independent body to be able to authorize the use of intrusive investigative measures. Judicial or other independent authorities should grant permission for the use of such powers after a thorough assessment on a case-by-case basis. Depending on the severity of the criminal offence, specific conditions may be required under national legislation. Criminal justice practitioners must also ensure that intrusive investigative powers are not used for longer than is strictly necessary for the effective investigation of the case.

In addition, the Second Additional Protocol to the Budapest Convention[29] contains a detailed Article 14 on the protection of personal data. This provision applies to the new procedural powers provided by the Second Additional Protocol, and sets out obligations on Parties to ensure that important aspects of the rights to privacy and data protection – such as purpose and use, data quality and integrity, sensitive data, data retention, automated decision-making, data security and onward sharing of data – are upheld in the use of these powers.

29 Ibid.

5

Applying human rights safeguards in cybercrime investigations

This chapter explores the elements that criminal justice practitioners should consider to ensure that human rights are protected during cybercrime investigations. It draws extensively on the guidance provided by the jurisprudence of the ECtHR and the CJEU. This guidance is relevant also for States that are not members of the CoE or the EU, as it provides concrete examples of how respect for human rights can be ensured in cybercrime investigations. Several particularly important ECtHR judgments are presented in more detail in Annex 2.

5.1 RIGHT TO PRIVACY

The investigation of cybercrimes and other crimes involving electronic evidence may interfere with the right to privacy when they:

- Make use of personal data;
- Involve the retention and processing of subscriber, traffic or content data;
- Interfere with the privacy of communications, for example when intercepting messages or traffic data;
- Involve secret surveillance, such as undercover operations to catch criminals on online (dark web) marketplaces.

There is an extensive body of case law from both the ECtHR and the CJEU regarding the implementation of the right to privacy.

SCOPE AND APPLICATION OF THE RIGHT TO PRIVACY IN CYBERCRIME INVESTIGATIONS

The jurisprudence of the ECtHR provides detailed guidance on the scope and application of the right to privacy in the context of cybercrime investigations. In its case law, the Court has defined the scope of the right to private and family life broadly, so that it extends to:

- Protection of individual reputation, defamation (positive obligation of the State in relation to obligation of service provider);
- Data protection;
- File or data gathering by security services or other organs of the State;
- Police surveillance (including on the internet and dark web[30]);
- Stop and search police powers;
- Home visits, searches and seizures;
- Interception of telecommunications in a criminal investigation context;
- Correspondence of private individuals, professionals and companies;

30 See more on ECtHR jurisprudence in: CoE, *Mutual Legal Assistance Manual* (Belgrade, 2013), p. 101.

- Secret surveillance of citizens and organizations;
- Retention of subscriber and traffic data.[31]

The Court has also underlined that the right to private and family life places on States both a positive obligation (to protect the right) and a negative obligation (to refrain from interference with the right). For instance, in *K.U. v. Finland*, the Court highlighted the positive obligation of a State to investigate crimes effectively and to enact appropriate legislation on exceptions to service providers' obligation to keep data confidential.[32] The Court emphasized that while freedom of expression and confidentiality of communications are primary considerations, they cannot be absolute. Given the serious nature of the case, the Court held that the State should have established a legal framework for reconciling the confidentiality of internet services with the prevention of disorder or crime and the protection of the rights and freedoms of others.[33]

As with any interference with human rights, limitations to the right to privacy must be provided by law, necessary and proportionate. The jurisprudence of the ECtHR provides guidance on what this means in practice. Similar principles apply to the corresponding provision in the ICCPR (Article 17).[34]

Concerning the **basis in law**, legislation authorizing the use of powers that interfere with the right to private life must be accessible to those liable to be affected and have sufficient clarity so that it gives "individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are entitled to resort to measures affecting their rights under the Convention."[35] This means that the various procedural powers available to investigators (e.g., provisions on requests to preserve or produce data, to allow the real-time collection of traffic data, or to search for and seize computer data, objects or documents) must be clearly defined in national legislation.

With regard to **necessity and proportionality**, any interference must be in pursuit of a legitimate aim – in this case, the investigation of a particular crime – and limited to what is necessary to achieve that aim. This requires consideration of whether less restrictive alternative measures are available. Furthermore, legislation must contain adequate safeguards against arbitrary application and not confer excessive discretion on the officials entrusted with its application.

This means that legislation establishing procedural powers for use in cybercrime investigations should:

- Require the existence of adequate grounds for justifying the use of individual procedural powers;
- Stipulate that the measure is subject to judicial or other independent oversight, especially when it involves particularly invasive acts such as the interception of content data;
- Establish time limits for the preservation of data;

31 ECtHR, *Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence* (Strasbourg, 2020); see also: ECtHR (2023), *Factsheet on Personal Data Protection*, available at https://www.echr.coe.int/Documents/FS_Data_ENG.pdf; ECtHR (2022), *Factsheet on Mass surveillance*, available at https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf.

32 ECtHR, *K.U. v. Finland*, 2 December 2008, No. 2872/02, § 49.

33 Ibid., §§ 48, 49.

34 See UN Human Rights Committee, *CCPR General Comment No. 16: Article 17, Right to Privacy*, 23 March 1988, paras 4, 5.

35 ECtHR, *Fernández Martínez v. Spain* [GC], 12 June 2014, No. 56030/07, § 117.

- Exclude (or specially protect) privileged data from the scope of production orders and search and seizure.

Examples of the application of the principle of proportionality can be found in ECtHR cases related to the interception of content data, which is the most intrusive procedural power set out in the CoE Cybercrime Convention. The ECtHR has held that, in particular, legal provisions governing interception of communications must provide for adequate and effective guarantees against arbitrariness and the risk of abuse inherent in any system of secret surveillance, and has defined specific conditions and safeguards for secret surveillance of communications (see section on "Secret surveillance in cybercrime investigations" below).[36]

PERSONAL DATA PROTECTION IN CYBERCRIME INVESTIGATIONS

Another important aspect of the right to privacy concerns the right to protection of personal data, which is established in a number of international and regional legal instruments (see box 3). Data protection principles must be taken into account when regulating police powers and when collecting and processing personal data in the context of criminal investigations. These principles include:[37]

- **Lawfulness:** personal data must be processed lawfully, either with the consent of the data subject or on the basis of another legitimate ground provided for in data protection legislation.
- **Fairness:** personal data should be processed fairly and data subjects must be informed of the risk.
- **Transparency:** personal data should be processed in a transparent manner. Data subjects should be informed about how their data are being used.
- **Purpose limitation:** any processing of personal data must be done for a specific, clearly defined purpose. Any additional processing must be compatible with the original purpose.
- **Data minimization:** data processing must be limited to what is necessary to fulfil a legitimate purpose.
- **Data accuracy:** data controllers shall ensure that personal data are accurate and up to date, and must take steps to erase or rectify inaccurate data.
- **Storage limitation:** personal data must not be kept for longer than necessary, and must be deleted or anonymized as soon as they are no longer needed for the purposes for which they were collected.
- **Data security (integrity and confidentiality):** appropriate technical or organizational measures must be implemented when processing personal data to protect the data against accidental, unauthorised or unlawful access, use, modification, disclosure, loss, destruction or damage.
- **Accountability:** data controllers and processors must actively and continuously implement measures to promote and safeguard data protection, and must be able to demonstrate compliance with data protection provisions.

36 ECtHR, *Roman Zakharov v. Russia* [GC], 4 December 2015, No. 47143/06; ECtHR, *Breyer v. Germany*, 30 January 2020, No. 50001/12; compare also with CJEU decisions on data retention.

37 EU Agency for Fundamental Rights and CoE, *Handbook on European Data Protection Law* (Luxembourg, 2018).

BOX 3 INTERNATIONAL AND REGIONAL LEGAL INSTRUMENTS ON PROTECTION OF PERSONAL DATA

- **CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** of 28 January 1981, no. 108 (entered into force in 1985).
- **Protocol amending the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** of 10 October 2018, no. 223 (not yet entered into force).
- **EU General Data Protection Regulation:** 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 (entered into force in 2018).
- **EU Law Enforcement Directive:** 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 (entered into force in 2018).

The ECtHR has already examined a wide range of interferences with the right to private life under ECHR Article 8 as a result of the storage, processing and use of personal data. These include: the use of surveillance via GPS in criminal investigations;[38] the disclosure of identifying information to law enforcement authorities by telecommunications providers;[39] the indefinite retention of fingerprints, cell samples and DNA profiles after criminal proceedings;[40] the so-called metering or collection of usage or traffic data;[41] and the storage of data on users of pre-paid SIM cards.[42]

In the case of *Marper v. the United Kingdom*, the ECtHR made clear that the mere storage of data related to the private life of a person amounts to interference with the right to privacy enshrined in ECHR Article 8. The Court held that the protection of personal data is of fundamental importance to the enjoyment of the right to respect for private and family life. Domestic law should ensure that appropriate safeguards are provided, especially when automatic processing of personal data is involved. In particular, domestic law should ensure that such data are relevant and not excessive in relation to the purposes for which they are preserved, and that they are stored in a form which permits identification of the data subjects for no longer than is necessary for the purpose for which those data are kept. It must also afford adequate guarantees that retained personal data are effectively protected from misuse.

38 ECtHR, *Uzun v. Germany*, 2 September 2010, No. 35623/05; ECtHR, *Ben Faiza v. France*, 8 February 2018, No. 31446/12.

39 ECtHR, *K.U. v. Finland*, 2 December 2008, No. 2872/02; ECtHR, *Benedik v. Slovenia*, 24 April 2018, No. 62357/14.

40 ECtHR, *S. and Marper v. The United Kingdom* [GC], 4 December 2008, 30562/04 and 30566/04.

41 ECtHR, *Malone v. the United Kingdom*, 2 August 1984, No. 8691/79; ECtHR, *Copland v. the United Kingdom*, 3 April 2007, No. 62617/00.

42 ECtHR, *Breyer v. Germany*, 30 January 2020, No. 50001/12.

RETENTION AND ACCESS TO SUBSCRIBER OR TRAFFIC DATA

An issue directly related to personal data protection is data retention. Both the ECtHR and the CJEU have addressed this issue in numerous cases. In *Benedik v. Slovenia*, the ECtHR found a violation of ECHR Article 8 in relation to the lack of clarity in the Slovenian constitutional framework on the legal conditions for access to subscriber data relating to (dynamic) IP addresses. It found that users of internet access facilities have a legitimate expectation of privacy, even if they consciously disclose their IP address to the public.

In *Breyer v. Germany*, the Court found no violation of ECHR Article 8, as the conditions and safeguards of the German legislation regulating the obligation of service providers to store personal data of users of pre-paid mobile phone SIM cards and the conditions under which these data are made available to authorities upon request were clear and proportionate. In adjudicating this case, the Court highlighted the fundamental importance of the right to privacy and the need for strong safeguards to prevent the use of personal data contrary to Article 8.

In particular, the Court found that the collection of the applicants' names and addresses as users of pre-paid SIM cards amounted to a limited interference with their rights. The law in question had additional safeguards, and people could also turn to independent data supervision bodies to review the authorities' data requests and seek legal redress if necessary. Therefore, in this case, Germany had not overstepped the limits of its discretion ("margin of appreciation") in applying the law concerned and the data collection did not violate the applicants' rights.

In 2006, the EU adopted the so-called Data Retention Directive, which regulated the retention of certain types of traffic data related to the use of telecommunications networks (phone, mobile phone and internet data) for criminal justice purposes.[43] Traffic data reflects user activity on the network, enabling law enforcement, among others, to see the origin and destination of phone calls on the network, location data (in the cellular network), as well as the IP address of users of internet access services. Specifically in relation to cybercrime, it is important to note that this Directive did not require retention of websites visited or other data that relates to internet usage, but was restricted to retention of the link between the IP address and the subscriber data of users.

In 2014, the CJEU declared the Data Retention Directive incompatible with Articles 7 and 8 of the Charter of Fundamental Rights of the EU (respect for private and family life, and protection of personal data) and therefore invalid.[44] The Court ruled that the retention of traffic data provided for by the Directive was incompatible with the right to privacy due to its generalized nature (it required the retention of data of users who are not suspected of any crime), the lack of safeguards against unlawful access and use of the data, and the lack of purpose limitation (the use would be for serious crime, but this term lacked a clear definition in the Directive).

43 *Directive 2006/24/EC of the European Parliament and of the Council 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*, 13 April 2006, OJEU L 105/54.

44 CJEU, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 8 April 2014, Joined C-293/12 and C-594/12.

The CJEU further clarified its position in several subsequent cases concerning national legislation in EU Member States that was based on the Data Retention Directive.[45] The Court found these national legal frameworks to be in violation of the rights to privacy and data protection, as they required the general and indiscriminate retention of traffic and location data. It clarified that such data retention is permissible only if a serious threat to national security is present or foreseeable, and if the data retention is subject to judicial or other independent scrutiny, and is only for a limited time period. It also stated that EU law does not preclude national legislation that provides for the targeted retention of traffic and location data for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, provided that certain safeguards are in place.[46]

At the same time, the Court clarified that EU law does permit the general and indiscriminate retention of subscriber data, i.e., IP address data and data relating to the civil identity of users, for the same purposes.[47] The need to prosecute (cyber) crime and identify malicious online users was considered to outweigh the interference with the right to privacy caused by the retention of limited data on the source IP addresses of internet users. This has opened the door to legislative measures providing for preventive retention of IP addresses for the purpose of combating crime and safeguarding public security. Without this data, internet use could become entirely anonymous, with significant consequences for the investigation and prosecution of (cyber) crime.

SECRET SURVEILLANCE IN CYBERCRIME INVESTIGATIONS

Different overt and covert methods of gathering information present various degrees of interference with the right to privacy. Some of these methods, such as the use of special investigation techniques and other covert investigation measures, including surveillance on private premises or in homes, interception of communications, the use of undercover agents and informants as well as accessing bank accounts and other confidential information, are explored in further detail in the OSCE manual *Human Rights in Counter-Terrorism Investigations*.[48]

As opposed to targeted surveillance, which is commonly based on prior suspicion and subject to judicial or executive authorization, mass surveillance programmes do not allow for an individualized case-by-case assessment of proportionality before such measures are taken. As such, they risk undermining the very essence of the right to privacy. Information gathered for intelligence purposes is sometimes also used as evidence in criminal proceedings. However, the original purpose of gathering such information is different from the purpose of prosecution of cybercrimes or other crimes involving electronic evidence, and often different legal rules and conditions apply to its collection. Therefore, caution is clearly required when using such

45 CJEU, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 8 April 2014, Joined C-293/12 and C-594/12; CJEU, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* [GC], 21 December 2016, Joined C-203/15 and C-698/15; CJEU, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others* [GC], 6 October 2020, C-623/17; CJEU, *La Quadrature du Net and Others v Premier ministre and Others* [GC], 6 October 2020, Joined C-511/18, C-512/18 and C-520/18; CJEU, *SpaceNet and Telekom Deutschland GmbH* [GC], 27 October 2022, Joined C-793/19 and C-794/19.

46 CJEU, *SpaceNet and Telekom Deutschland GmbH* [GC], 27 October 2022, Joined C-793/19 and C-794/19.

47 CJEU, *La Quadrature du Net and Others v Premier ministre and Others* [GC], 6 October 2020, Joined C-511/18, C-512/18 and C-520/18; CJEU, *SpaceNet and Telekom Deutschland GmbH* [GC], 27 October 2022, Joined C-793/19 and C-794/19.

48 See also OSCE/ODIHR, *Human Rights in Counter-Terrorism Investigations: A Practical Manual for Law Enforcement Officers* (Warsaw, 2013).

information in criminal proceedings. The use of intelligence obtained by unlawful means in criminal proceedings will be contrary to human rights.

The ECtHR has found violations of ECHR Article 8 in several cases related to secret surveillance regimes, including bulk interception of communications and intelligence sharing, for example, *Roman Zakharov v. Russia*,[49] *Szabó and Vissy v. Hungary*,[50] and *Big Brother Watch and Others v. the United Kingdom*.[51] The *Vissy v. Hungary* judgment made clear that judicial oversight of secret surveillance is of particular importance. An independent judicial body should oversee their use; a body directly linked to the executive (the Minister of Interior, in this case) does not meet this requirement. The judgment also highlighted the issue with regard to the scope of the surveillance measures and considered the safeguards provided in legislation insufficiently precise, effective and comprehensive on the ordering, execution and potential redressing of such measures.

In *Big Brother Watch and Others v. the United Kingdom*, the Court stated that any bulk interception regime must be subject to "end-to-end safeguards" at the domestic level, meaning: an assessment of the necessity and proportionality of the measures taken should be made at each stage of the process; bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are defined; and that the operation should be subject to supervision and independent *ex post facto* review.[52]

In the connected case of *Centrum För Rättvisa v. Sweden*, the Court highlighted shortcomings in the domestic legal framework that were not sufficiently compensated by other safeguards.[53] These included: the absence of a clear rule on the destruction of intercepted material that does not contain personal data; the absence of an obligation to take the privacy of individuals into account when deciding whether to transmit intelligence material to foreign partners; and the absence of an effective *ex post facto* review, such as the possibility for members of the public to obtain reasoned decisions in response to inquiries regarding bulk interception of communications.

These cases provide clear guidance on some of the safeguards required in the context of secret surveillance of communications. The ECtHR has indicated that it expects there to be a regime of independent supervision of the use of such covert and intrusive powers, and that the more independent an authorizing or reviewing body is, the more likely the authorizing and reviewing regime is to be appropriate. Indeed, in *Klass v. Germany*, the ECtHR noted that judicial control of the authorization procedure provides "the best guarantees of independent, impartial and a proper procedure."[54] The use of specialized commissioners and tribunals at the national level can also satisfy the requirements of ECHR Article 8.

49 ECtHR, *Roman Zakharov v. Russia* [GC], 4 December 2015, No. 47143/06.

50 ECtHR, *Szabó and Vissy v. Hungary*, 12 January 2016, No. 37138/14.

51 ECtHR, *Big Brother Watch and Others v. The United Kingdom* [GC], 25 May 2021, No. 58170/13, 62322/14 and 24960/15.

52 Ibid.

53 ECtHR, *Centrum För Rättvisa v. Sweden* [GC], 25 May 2021, No. 35252/08.

54 ECtHR, *Klass and Others v. Germany*, 6 September 1978, No. 5029/71.

5.2 RIGHT TO A FAIR TRIAL

Cybercrime investigations involve a number of processes that relate to the main elements of the right to a fair trial, including:

- Access to data stored on electronic devices;
- Maintenance of the integrity of seized electronic evidence in the context of the search, seizure and management of electronic data;
- Access to evidence and its inspection by the accused in relation to seized electronic evidence;
- The exclusion or limitations imposed on searches of privileged communications and information (such as communications with lawyers, medical records, or communications of journalists with their sources).

Presumption of innocence is closely linked to the right not to incriminate oneself and to remain silent.[55] The right to remain silent is particularly important in the context of searching and investigating electronic data. While national legislation might impose (administrative) sanctions on a witness who is not willing to provide information, such as a password to access a computer during a search of electronic devices, sanctioning a suspect would be problematic, as the suspect can invoke his or her right to remain silent. It is therefore important that a suspect is informed of his or her rights before being asked to voluntarily provide a password or access code to a computer or other electronic device.[56]

A storage device, such as an internal or external computer disk, USB drive or a mobile device, might contain a vast quantity of data that cannot be searched during a house search. Therefore, it often has to be seized and searched at a later stage.[57] Domestic legislation, including specific rules on search and seizure (or more precisely: access and copying[58]) of electronic evidence, must guarantee that the right to an effective defence is preserved in the same way as for tangible evidence. Relevant procedural provisions include: the obligation to seize an electronic device and create an accurate copy; the obligation to inform and invite the suspect and his/her lawyer to the search of a seized electronic device; and the obligation to disclose the evidence seized to the defence. Putting in place such procedural safeguards helps to ensure that the principles of equality of arms and an adversarial procedure, which are important components of a fair trial, are implemented in practice.

The large volume of data involved in some investigations also presents a challenge in terms of data disclosure. An important safeguard is to ensure that the defence has the opportunity to participate in establishing the criteria used to determine which data may be relevant for disclosure.[59] This is particularly important in cases involving data stored online. Moreover, any refusal to allow the defence to conduct further searches of identified or tagged case data (e.g., data resulting from a

55 ECtHR, *Guide on Article 6 of the European Convention on Human Rights: Right to a fair trial (criminal limb)* (Strasbourg, 2022), para 197 and 373.

56 *Convention on Cybercrime*, 23 November 2001, CETS No. 185, Article 32(b).

57 CoE, *Explanatory Report to Cybercrime Convention* (Budapest, 2001), § 187.

58 Ibid. §§ 137, 191 and 197.

59 ECtHR, *Sigurður Einarsson and Others v. Iceland*, 4 June 2019, No. 39757/15, § 90; see also ECtHR, *Rook v. Germany*, 25 July 2019, No. 1586/15, §§ 67, 72.

search) raises the issue of providing adequate facilities for the preparation of the defence.[60] Wherever possible, the defence should be informed of the search criteria for large data sets, be given equal access, and have every opportunity to search the data sets for pertinent (exculpatory) data. The privileged nature of communications between lawyers and their clients should also be respected when searching through electronic evidence.

In short, the right to a fair trial requires a fair and balanced procedure, especially when electronic evidence is searched in relation to criteria identified by criminal justice authorities. It is not acceptable to exclude the defence from this process, and adequate safeguards and opportunities to find exculpatory evidence should be provided.

Finally, the concept of a "tribunal established by law," together with the concepts of "independence" and "impartiality" of the tribunal, form part of the "institutional requirements" of ECHR Article 6. In the ECtHR case law, there is a very close interrelationship between these concepts.[61] While they each serve specific purposes as distinct fair trial guarantees, there is a common thread running through the institutional requirements, in that they are guided by the aim of upholding the fundamental principles of the rule of law and the separation of powers.[62]

In *Szabo and Vissy v. Hungary*, the ECtHR reiterated the link between the independence of a judicial oversight body and the right to a fair trial.[63] Similarly, the CJEU has identified the oversight of data retention mechanisms as an important safeguard in its case law.

5.3 RIGHT TO FREEDOM OF EXPRESSION

The ECtHR has repeatedly recognized that user-generated content on the internet provides an unprecedented platform for the exercise of freedom of expression.[64] The Court has, however, also underlined the dangers presented by illegal online content, including child pornography, hate speech and speech inciting violence.[65]

The right to freedom of expression may be directly or indirectly affected by cybercrime investigations:

- Direct interference with the right to freedom of expression occurs when blocking or taking down websites and making content unavailable due to its illegal nature (e.g., child pornography, online marketplaces with illegal goods and services, hate speech);
- Indirect hindrance of the freedom of speech can take place if service providers or internet users are pressured into censoring content by threat of sanctions or criminal procedure.

60 ECtHR, *Sigurður Einarsson and Others v. Iceland*, 4 June 2019, No. 39757/15, § 91; see also: CoE, *Explanatory report to Cybercrime Convention* (Budapest, 2001), § 179.

61 ECtHR, *Guðmundur Andri Ástráðsson v. Iceland* [GC], 1 December 2020, No. 26374/18, § 218.

62 Ibid., §§ 218, 232, 233; see also: CoE, *Explanatory Report to Cybercrime Convention* (Budapest, 2001), § 70.

63 ECtHR, *Zabó and Vissy v. Hungary*, 12 January 2016, No. 37138/14.

64 See ECtHR, *Guide on Article 10 of the European Convention on Human Rights, Freedom of expression* (Strasbourg, 2022), §§ 588–632.

65 ECtHR, *Delfi AS v. Estonia* [GC], 10 October 2013, No. 64569/09, § 110; ECtHR, *Annen v. Germany*, 20 September 2018, No. 3682/10, § 67.

In addition, investigators must balance the protection of personality rights (e.g., defamation) and the need to uphold public security, with the obligation to ensure freedom of speech.

BLOCKING ACCESS TO THE INTERNET

International human rights bodies have repeatedly emphasized that state-mandated blocking of entire websites, IP addresses, ports or network protocols is an extreme measure that is only permissible as a measure of last resort and if minimum due process guarantees are respected.[66] Website blocking measures can only be compatible with international standards on the freedom of expression if they are provided for by law and are necessary and proportionate to protect legitimate aims.[67]

In its case law, the ECtHR has underlined that blocking access to the internet may be in direct conflict with paragraph 1 of ECHR Article 10, which guarantees freedom of expression "regardless of frontiers."[68] The case of *Bulgakov v. Russia* concerned the blocking of an entire website by a court order on account of the presence of illegal material (even after that material had been removed). In its ruling, the Court found that there had been no legal basis for the blocking order, as the legislation on which the order was based did not permit the authorities to block access to an entire website. The Court also held that its finding of unlawfulness applied in particular to the continued blocking of the website after the prohibited material had been removed.

In a separate case, *Cengiz and Others v. Turkey*, concerning the blocking of the video-hosting site YouTube, the ECtHR held that the applicants, who were users of the site, could legitimately claim that the measure had affected their right to receive and impart information or ideas. In view of the platform's unique characteristics, its accessibility and, above all, its potential impact, and given that no alternatives were available to the applicants, the Court found that the blocking infringed their freedom of expression.[69]

LIABILITY FOR ONLINE CONTENT

While acknowledging the important benefits of the internet for the exercise of freedom of expression, the ECtHR has held that liability for defamatory or other types of unlawful speech must, in principle, be retained and constitutes an effective remedy for violations of personality rights.[70]

In assessing in the case *Delfi AS v. Estonia* whether an owner of an internet news portal is required to remove comments posted by a third party, the Court identified four aspects relevant

66 See UN OSCE Representative on Freedom of the Media and Others, *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda*, 3 March 2017, FOM.GAL/3/17.

67 See, e.g., OSCE, *International Standards and Comparative Approaches on Freedom of Expression and Blocking of Terrorist and "Extremist" Content Online* (Vienna, 2018), para 47; see also: OSCE/ODIHR, *Comments on Certain Legal Acts Regulating Mass Communications, Information Technologies and the Use of the Internet in Uzbekistan* (Warsaw, 2019), para 86–89.

68 ECtHR, *Ahmet Yıldırım v. Turkey*, 18 December 2012, No. 3111/10, § 67.

69 ECtHR, *Cengiz and Others v. Turkey*, 1 December 2015, No. 48226/10 and 14027/11, §§ 52, 53, 55; see also: ECtHR, Ahmet Yıldırım v. Turkey, 18 December 2012, No. 3111/10, §§ 49, 55 about a similar case concering access to a website hosted on a Google Sites hosting service.

70 ECtHR, *Delfi AS v. Estonia* [GC], 10 October 2013, No. 64569/09, § 110.

to determining the liability of service providers for content on their platforms:[71]

- The context of the comments;
- The measures applied by the applicant company in order to prevent or remove defamatory comments;
- The liability of the actual authors of the comments as an alternative to the applicant company's liability;
- The consequences of the domestic proceedings for the applicant company.

Applying these considerations, the Court held that a notice-and-take-down system, if accompanied by effective procedures allowing for rapid response, can offer a sufficiently balanced approach to the rights of third parties.[72] Service providers can thus rely on such a system without directly attracting liability for user-generated content such as defamatory comments.[73] However, the Court also underlined that in cases such as *Delfi AS v. Estonia*, where comments by third party users take the form of hate speech and direct threats against the physical integrity of individuals, the rights and interests of others and of society as a whole might entitle States to impose liability on internet news portals if they fail to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or third parties.

BOX 4 THE "CHILLING" EFFECT ON FREEDOM OF EXPRESSION

If a video website, for example, is confronted with unclear legislation, it may overly censor users in order to stay out of trouble with the authorities. This effect, often referred to as a "chilling" effect, can be prevented by having clear rules, as well as regimes limiting the liability of service providers in cases where there is potentially illegal content on their platforms without their knowledge or permission. A chilling effect on freedom of expression can also occur if people self-censor themselves as a result of surveillance or out of fear of being targeted by wrongful suspicion. This, in turn, is often the result of vague or arbitrary norms.

BALANCING THE RIGHT TO FREEDOM OF EXPRESSION, PRIVACY AND PREVENTION OF CRIME

The ECtHR has also addressed the need to balance the rights to freedom of expression and privacy with the responsibility of States to prevent and investigate crimes. In *K.U. v. Finland*, the Court held that it was incompatible with ECHR Article 8 not to oblige a service provider to disclose the identity of a person wanted for placing an indecent advertisement about a minor on an internet dating site, referring in this context to the potential threat to the minor's physical

71 ECtHR, *Delfi AS v. Estonia* [GC], 10 October 2013, No. 64569/09, §§ 142–143; see also: ECtHR, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, 2 February 2016, No. 22947/13, §§ 60 et seq.

72 ECtHR, *Delfi AS v. Estonia* [GC], 10 October 2013, No. 64569/09, § 159.

73 ECtHR, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, 2 February 2016, No. 22947/13, § 91; see also: ECtHR, *Rolf Anders Daniel Pihl v. Sweden*, 7 February 2017, No. 74742/14, § 32; ECtHR, *Tamiz v. the United Kingdom*, 19 September 2017, No. 3877/14, § 84; ECtHR, *Høiness v. Norway*, 19 March 2019, No. 43624/14, §§ 73–74 concerning the importance of timely reaction after notification of the illegality of content.

and mental well-being and the vulnerability caused by his or her young age.[74] The Court stated that although freedom of expression and confidentiality of communications are primary considerations and internet users must have a guarantee that their own privacy and freedom of expression will be respected, such a guarantee cannot be absolute. It must 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.[75]

To sum up, freedom of expression can only be limited by law. Legislation should define precise rules and conditions for blocking and taking down websites or content and limit the responsibility of service providers for content generated by users. When the police propose a measure in relation to illegal content on the internet and a court considers its authorization, the impact on the freedom of expression needs to be throughly assessed to avoid excessive interference. A balance must be struck, particularly in relation to the freedom of media and in cases of defamation or hate speech, where boundaries between allegedly illegal content and the expression of an opinion, criticism or political views are not always clear. The chilling effect that censorship has on society is another important aspect (see box 4). The blocking of websites should be limited strictly to criminal content and should not impact content that is not illegal.

5.4 RIGHT TO THE PROTECTION OF PROPERTY

Cybercrime investigations often involve virtual assets, which may be seized as evidence of a crime and/or confiscated as proceeds of crime. The most common virtual assets in this context are cryptocurrencies, which are often used as a payment method for illegal goods offered on dark net marketplaces or for ransom in cases of ransomware. Cryptocurrencies have a market value and can thus be considered as “property” according to international standards.

The use of cryptocurrencies or other virtual assets is not in itself illegal, even if it is unregulated in many countries. The Financial Action Task Force’s (FATF) anti-money laundering standards, however, require regulation of certain aspects of cryptocurrencies, and a growing number of countries are implementing rules for cryptocurrency service providers, for example regarding the creation of a wallet, storage, exchange to fiat currency or to other cryptocurrencies or virtual assets.

Forfeiture and confiscation are generally regarded by the ECtHR as control of the use of property, to be considered under Article 1 (2) of Protocol No. 1 to the ECHR. The Court examined various measures taken to combat unlawful enrichment from the proceeds of crime. States have a wide margin of appreciation in implementing policies to fight crime, including by confiscation of:

- Property that is presumed to be of unlawful origin;[76]
- Property purchased with illicit funds;[77]

74 ECtHR, *K.U. v. Finland*, 2 December 2008, No. 2872/02, § 41.

75 Ibid., § 49.

76 ECtHR, *Raimondo v. Italy*, 22 February 1994, No. 12954/87; *Riela and Others v. Italy*, 4 September 2001, No. 52439/99; ECtHR, *Arcuri and Others v. Italy*, 5 July 2001, No. 52024/99; ECtHR, *Gogitidze and Others v. Georgia*, 12 May 2015, No. 36862/05 concerning a confiscation applied in civil proceedings; ECtHR, *Balsamo v. San Marino*, 8 October 2019, No. 20319/17 and 21414/17 concerning money laundering proceedings.

77 ECtHR, *Milorad Ulemek v. Serbia*, 2 February 2021, No. 41680/13.

- Proceeds of a criminal offence;[78]
- Property that was the object of the offence;[79]
- Property that had served, or had been intended to serve, for the commission of the crime.[80]

How much can be seized by police and confiscated by a court depends on the national confiscation regime, which can also be applied to virtual assets in an individual criminal case.

The ECtHR has considered several cases addressing proportionality and due process in confiscation proceedings. In *Todorov and Others v. Bulgaria*,[81] the Court held that there had been a violation of Article 1 of Protocol 1 to the ECHR in four out of seven applications. Domestic courts had failed to establish a link between the goods forfeited and criminal activity, or between the value of the property and the difference between income and expenditure. Ordering forfeiture had thus been disproportionate.

In *Balsamo v. San Marino*,[82] the Court accepted that the confiscation measures were proportionate, even in the absence of a conviction establishing the guilt of the accused and if also imposed on the children due to their father's previous criminal record. For the proportionality test, the high probability of illicit origin combined with the owner's inability to prove the contrary, was considered sufficient.

The case of *Gogitidze and Others v. Georgia*[83] concerned a court-imposed measure of confiscation of property belonging to a former deputy minister of the interior. The Court found that a fair balance had been struck between the means employed for forfeiture of the applicants' assets and the general interest in combating corruption in the public service. The applicants had not been denied a reasonable opportunity to put forward their case and the domestic courts' findings had not been arbitrary.

78 ECtHR, *Phillips v. the United Kingdom*, 5 July 2001, No. 41087/98; ECtHR, *Welch v. the United Kingdom*, 9 February 1995, No. 17440/90; ECtHR, *Silickienė v. Lithuania*, 10 April 2012, No. 20496/02; ECtHR, *Gogitidze and Others v. Georgia*, 12 May 2015, No. 36862/05.

79 ECtHR, *Agosi v. the United Kingdom*, 24 October 1986, No. 9118/80.

80 ECtHR, *Andonoski v. the former Yugoslav Republic of Macedonia*, 17 September 2015, No. 14464/11; ECtHR, *Todorov and Others v. Bulgaria*, 13 July 2021, No. 50705/11 and 6 others.

81 ECtHR, *Todorov and Others v. Bulgaria*, 13 July 2021, No. 50705/11 and 6 others.

82 ECtHR, *Balsamo v. San Marino*, 8 October 2019, No. 20319/17 and 21414/17.

83 ECtHR, *Gogitidze and Others v. Georgia*, 12 May 2015, No. 36862/05.

6

Conclusion

Respect for human rights and the rule of law is an important aspect of every democratic society and can also be a condition for the legality of evidence and the fairness of a criminal procedure. It also affects the trust that citizens have in public institutions, and in many cases is a prerequisite for securing the international co-operation that is critical for effective cybercrime investigations. It is therefore important that criminal justice practitioners know and understand the human rights standards that apply to the different stages and processes of a cybercrime investigation.

Many human rights, including the rights to privacy, a fair trial, freedom of expression and protection of property, can be affected in the course of cybercrime investigations. Any interference with human rights that allow for limitations in the course of cybercrime investigations must be **based in law, necessary and proportional**, and pursue a **legitimate aim**, such as protecting the human rights of victims or other interests of society.

International and regional human rights standards, as well as the jurisprudence of international courts such as the ECtHR, provide important guidance to States on how to implement in practice their human rights obligations regarding cybercrime investigations. This includes putting in place domestic legislation to regulate the use of investigative powers in line with international human rights standards and safeguards, and ensuring that practitioners have the knowledge and skills necessary to uphold these standards throughout cybercrime investigations.

7

Annexes

ANNEX 1 RELEVANT ICCPR AND ECHR ARTICLES

ANNEX 2 SELECTED ECTHR JURISPRUDENCE

ANNEX 1 RELEVANT ICCPR AND ECHR ARTICLES

RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

ICCPR Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

ECHR Article 8

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. 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 for the protection of the rights and freedoms of others.

RIGHT TO A FAIR TRIAL

ICCPR Article 14

1. All persons shall be equal before the courts and tribunals. In the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law. The press and the public may be excluded from all or part of a trial for reasons of morals, public order (ordre public) or national security in a democratic society, or when the interest of the private lives of the parties so requires, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice; but any judgement rendered in a criminal case or in a suit at law shall be made public except where the interest of juvenile persons otherwise requires or the proceedings concern matrimonial disputes or the guardianship of children.
2. Everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law.
3. In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality:
   a. To be informed promptly and in detail in a language which he understands of the nature and cause of the charge against him;
   b. To have adequate time and facilities for the preparation of his defence and to communicate with counsel of his own choosing;
   c. To be tried without undue delay;
   d. To be tried in his presence, and to defend himself in person or through legal assistance of his own choosing; to be informed, if he does not have legal assistance, of this right;

and to have legal assistance assigned to him, in any case where the interests of justice so require, and without payment by him in any such case if he does not have sufficient means to pay for it;

e. To examine, or have examined, the witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

f. To have the free assistance of an interpreter if he cannot understand or speak the language used in court;

g. Not to be compelled to testify against himself or to confess guilt.

4. In the case of juvenile persons, the procedure shall be such as will take account of their age and the desirability of promoting their rehabilitation.

5. Everyone convicted of a crime shall have the right to his conviction and sentence being reviewed by a higher tribunal according to law.

6. When a person has by a final decision been convicted of a criminal offence and when subsequently his conviction has been reversed or he has been pardoned on the ground that a new or newly discovered fact shows conclusively that there has been a miscarriage of justice, the person who has suffered punishment as a result of such conviction shall be compensated according to law, unless it is proved that the non-disclosure of the unknown fact in time is wholly or partly attributable to him.

7. No one shall be liable to be tried or punished again for an offence for which he has already been finally convicted or acquitted in accordance with the law and penal procedure of each country.

ECHR Article 6

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

3. Everyone charged with a criminal offence has the following minimum rights:

a. to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;

b. to have adequate time and facilities for the preparation of his defence;

c. to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;

d. to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

e. to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

FREEDOM OF EXPRESSION

ICCPR Article 19

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

   a. For respect of the rights or reputations of others;

   b. For the protection of national security or of public order (ordre public), or of public health or morals.

ECHR Article 10

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

RIGHT TO PROTECTION OF PROPERTY

Article 1 of Protocol 1 to ECHR

1. Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.
2. The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.

ANNEX 2 SELECTED ECTHR JURISPRUDENCE

Benedik v. Slovenia[84]

The case concerned a violation of the right to respect for private life under ECHR Article 8. In 2006, the Slovenian police received information from the Swiss police about an exchange of files containing child pornography through a peer-to-peer file-sharing website. Among the IP addresses recorded by the Swiss police was a certain dynamic IP address in Slovenia. In August 2006, the Slovenian police, without a court order, requested a Slovenia-based Internet service provider (ISP) to disclose data on a user to whom the dynamic IP address had been assigned at a particular time. The request was based on the provision of the Criminal Procedure Act which allowed the police to request information from an electronic communication provider about the user of a certain means of electronic communication whose details were not available in the relevant directory.

The ISP provided the name and address of the subscriber relating to the respective IP address. Subsequently, in December 2006, a court order was issued requiring the ISP to disclose both the personal data and the traffic data of the subscriber associated with the IP address in question. On the basis of the received data, a district court ordered a search of the applicant's family home in January 2007. During the search, computers containing pornographic material involving minors were seized.

In December 2008, the applicant was found guilty of the criminal offence of displaying, manufacturing, possessing and distributing pornographic material. He was sentenced to a suspended prison term of eight months with a probation period of two years. In November 2009, on appeal, the Ljubljana Higher Court converted the applicant's suspended sentence into a prison term of six months.

The applicant unsuccessfully pursued legal recourse before the domestic courts, claiming that the privacy of correspondence and other means of communication could only be suspended on the basis of a court order and therefore any unlawfully obtained information should be excluded as evidence. The applicant's complaint concerned the first request by the police to the ISP for identification of the IP address user on the basis of the Criminal Procedural Act.

In this respect, the Constitutional Court concluded in February 2014 that the Constitution also protected traffic data, i.e., any data processed for the transmission of communications in an electronic communications network. It considered that IP addresses were included in such traffic data and that a court order would normally be required. However, the applicant, who had not hidden in any way the IP address through which he had accessed the internet, had consciously exposed himself to the public and had thus waived the legitimate expectation of privacy. As a result, though the data concerning the identity of the user of the IP address were in principle protected as communication privacy under the Constitution, the Constitutional Court ruled that no court order was required to disclose them in the applicant's case.

When the case was brought to the ECtHR, the Court concluded that the police request to the ISP and the use of the subscriber information leading to the applicant's identification had amounted to

84 ECtHR, *Benedik v. Slovenia*, 24 April 2018, No. 62357/14; summarized in: ECtHR, Information Note on the Court's caselaw 217.

interference with his rights under Article 8 of the ECHR. The Court noted that the police measures had some basis in domestic law. As the relevant legislation was not coherent with regard to the level of protection afforded to the applicant's privacy interest, the Court relied on the Constitutional Court's interpretation, according to which the disclosure of subscriber information associated with a certain dynamic IP address in principle required a court order, as the traffic data fell within the protection of the Constitution. As to the Constitutional Court's position that the applicant in the concrete case had waived the legitimate expectation of privacy as he had not hidden in any way the IP address through which he had accessed the internet, the ECtHR did not find it reconcilable with the scope of the right to privacy under the ECHR. Therefore, a court order was necessary in the present case, and nothing in the domestic law prevented the police from obtaining it.

The ECtHR found the legislation, namely the relevant provisions of the Criminal Procedure Act (which did not contain specific rules as to the association between the dynamic IP address and subscriber information), the Electronic Communications Act (which specifically regulated the secrecy and confidentiality of electronic communication), and the Constitution (which required a court order for any interference with privacy of communication), not coherent about the level of protection afforded to the applicant's privacy interest.

In this context, the Court also noted that, at the relevant time, there was no regulation specifying the conditions for the retention of data obtained under the Criminal Procedure Act and that the procedure for accessing and transmitting such data did not contain safeguards against abuse by State officials. No independent supervision of the use of police powers in relation to obtaining information from ISPs had existed at the relevant time.

The ECtHR therefore concluded that the law on which the contested measure was based and the way it was applied by the domestic courts lacked clarity and did not offer sufficient safeguards against arbitrary interference with Article 8 of ECHR. The Court found that the interference with the applicant's right to respect for his private life was not "in accordance with the law," as required by Article 8 (2) of the Convention.

Following the judgment, Slovenian police and prosecutors changed their practice immediately. In 2019, the Criminal Procedure Act was amended to specify that subscriber data can be obtained without a court order only if no traffic data is analysed. In practice, this means that a court order is needed to access the data on the user of a specific dynamic IP address. This is not the case when the subscriber data is included in a contract with a service provider, for example for a mobile phone number or a static IP address.

In June 2018, Mr. Benedik filed a request for protection of legality before the Supreme Court. In June 2020, the Supreme Court granted the applicant's request for protection of legality, annulled the final judgement and returned the case to the Kranj District Court for retrial. In May 2021, the Kranj District Court discontinued the criminal procedure against Mr. Benedik after the Kranj District Prosecutor's Office withdrew the indictment.

In conclusion, it needs to be highlighted that the condition of a court order to obtain user data of a (dynamic) IP address stems from the Slovenian Constitution and jurisprudence of the Slovenian Constitutional Court and is not an international standard. The case also shows the importance of the right to respect for private life and sufficient legal clarity and adequate practice when interfering with human rights. Because of a violation of the ECHR in this case, the electronic evidence was excluded and the renewed criminal procedure was stopped.

Breyer v. Germany[85]

Under the 2004 amendments to the German Telecommunications Act, telecommunications companies were required to collect and store the personal details of all their customers, including users of pre-paid SIM cards, even when not necessary for billing purposes or other contractual reasons, and to make them available to the authorities upon request. Customers had to register personal details such as their name and address, telephone numbers and date of birth with their service providers. They complained about the storage of their personal data as users of pre-paid SIM cards.

The ECtHR held that there had been no violation of ECHR Article 8 (right to respect for private life). The Court found that, overall, Germany had not overstepped the limits of its discretion ("margin of appreciation") in the choice of means to achieve the legitimate aims of protecting national security and fighting crime, and that the storage of the applicants' personal data had been proportionate and "necessary in a democratic society." There had thus been no violation of the Convention.

The Court considered in particular that collecting the applicants' names and addresses as users of pre-paid SIM cards amounted to a limited interference with their rights. It noted, however, that the law in question had additional safeguards, and that people could also turn to independent data supervision bodies to review authorities' data requests and seek legal redress if necessary.

In respect of the use of stored data, the data could be requested by various public authorities without the need for a court order or notification of the persons concerned. Requests for data retrieval could under certain conditions be automated and result in lists based on mere similarity (partial-data queries) in names or numbers. Such information requests were permissible where considered necessary "to prosecute criminal and administrative offences, to avert danger and to perform intelligence tasks."

In particular, the Court reviewed two main aspects. First, whether the interference was necessary in a democratic society and proportionate, including the question of foreseeability and sufficient detail of the relevant provisions. The Court acknowledged that the storage at issue was, from a general point of view, a suitable response to changes in communication behaviour and in the means of telecommunication:

- Pre-registration of mobile telephone subscribers greatly simplified and accelerated investigation by law enforcement agencies, and could thereby contribute to effective law enforcement and prevention of disorder or crime.
- The existence of possibilities to circumvent legal obligations could not be a reason to call into question their overall utility and effectiveness.
- Besides the lack of consensus, the fact that national security concerns were at stake also justified a certain margin of appreciation.

The second aspect addressed by the Court concerned the question of whether the interference with the right to private life was proportionate. Unlike in cases previously examined by the Court, the data storage at issue did not include any highly personal information or allow the creation of

85 ECtHR, *Breyer v. Germany*, 30 January 2020, No. 50001/12; summarized in: ECtHR, Information Note on the Court's case-law 236.

personality profiles or the tracking of movements of subscribers. Moreover, no data concerning individual communication events was stored. While not trivial, the interference was thus rather limited in nature.

On safeguards as to the data registration and storage *per se*, the Court noted that:

- The applicants had not alleged that this storage had been subject to any technical insecurities.
- The duration of the storage was limited to the calendar year following the year in which the contractual relationship had ended; this did not appear excessive, given that investigations into criminal offences might take some time and extend beyond the end of the contractual relationship.
- The stored data had been limited to the information necessary to clearly identify the relevant subscriber.
- Automated requests under the Telecommunications Act are limited to specific authorities in the field of law enforcement and national security. Manual requests, on the other hand, are not explicitly listed but are determined based on the authorities' tasks (e.g., preventing dangers, prosecuting crimes, enforcing regulations). This level of detail is adequate, despite the lack of an explicit enumeration of the authorities concerned.

The German Federal Constitutional Court also considered the question of whether there were sufficient safeguards for future possible access to and use of the stored data, in particular with regard to the following aspects:

- Competence for issuing information requests: the fact that the existing law stipulates that information may only be given in so far as it is necessary for the performance of the duty does create an objectively limiting factor already. This ensures that retrievals are only permitted when information actually needed for the performance of duties cannot be obtained more easily but equally effectively in another way. As a result, there is no requirement at the non-constitutional level for the entitled authorities to be expressly specified in the law.
- Purpose of information requests: the requesting authorities had to have an additional legal basis to retrieve the data (double-door system analogy[86]).
- Extent of information requests: retrieval was limited to necessary data under a general obligation to erase any data the requesting authority did not need without undue delay. Besides, the requirement of "necessity" was not only inherent in the specific legal provisions subject to this complaint but also to German and European data-protection law.
- Review and supervision of information requests: even if the responsibility for the legality of the information request lay with the retrieving agencies themselves, the Federal Network Agency was considered competent to independently examine the admissibility of the transmission of data when it saw reasons to do so. Legal redress against information retrieval might also be sought under general rules. Given those avenues for review, the lack of notification of the retrieval procedure did not raise an issue under the Convention.

86 A data exchange takes place through the encroachments of retrieval and transfer, which correspond to each other and each of which requires an idependent legal basis. Figuratively speaking, the legislature must open not only the door for the transmission of data, but also the door for their retrieval. It is only both legal bases together, which must operate together like a double door, which give authority to exchange personal data.

The ECtHR confirmed the decision of the German Federal Constitutional Court that there had been no violation of human rights and highlighted the importance of legal limitations and safeguards in the framework of national margin of appreciation in order to satisfy the principles of proportionality and necessity in a democratic society. In particular, it found that the legal obligation on service providers to store personal data of users of pre-paid mobile telephone SIM cards and make them available to the authorities upon request was proportionate to the legitimate aims of protecting national security and fighting crime, and that data retrieval by the authorities was accompanied by adequate safeguards.

Roman Zakharov v. Russia[87]

The applicant, who was the editor-in-chief of a publishing company, brought judicial proceedings against three mobile network operators, complaining about interference with his right to privacy of his telephone communications. He claimed that, pursuant to the relevant domestic law, the mobile network operators had installed equipment which enabled the Federal Security Service to intercept all telephone communications without prior judicial authorization. He sought an injunction ordering the removal of the equipment and ensuring that access to telecommunications was given to authorized personnel only.

The domestic courts rejected the applicant's claim, finding that he had failed to prove that his telephone conversations had been intercepted or that the mobile operators had transmitted protected information to unauthorized persons. Domestic courts also found that the installation of the equipment to which he referred did not in itself infringe the privacy of his communications.

The ECtHR found that the mere existence of the contested legislation on interception of mobile telephone communications amounted in itself to an interference with the exercise of the applicant's rights under Article 8. The Court considered several aspects of the interference with Article 8:

- **Legality:** The interception of mobile telephone communications had a basis in the domestic law and pursued the legitimate aims of protecting national security and public safety, the prevention of crime and the protection of the economic well-being of the country.
- **Accessibility:** legal provisions had been officially published and were accessible to the public.
- **Scope of application of secret surveillance measures:** the nature of the offences which could give rise to an interception order was sufficiently clear. However, the range was too wide, and the interception could be ordered not only for individuals who were suspects or accused.
- **Duration of secret surveillance measures:** the law contained clear rules on the duration and renewal of interceptions, but not on discontinuation of the surveillance.
- **Procedures** for, inter alia, storing and destroying intercepted data: the automatic storage for six months of clearly irrelevant data could not be considered justified under Article 8.
- **Authorization of interceptions:** interception had to be authorized by a court, but Russian judges were not instructed to verify the existence of "reasonable suspicion" against the person concerned or to apply the "necessity" and "proportionality" tests. The law did not contain any requirements with regard to the content of interception requests or authorizations. Some orders

87 ECtHR, *Roman Zakharov v. Russia*, 4 December 2015, No. 47143/06; summarized in: ECtHR, Information Note on the Court's caselaw 191.

did not mention a specific person or telephone number or the duration of surveillance. There was no obligation under the domestic law to show judicial authorization to the communications service provider before obtaining access to communications.

- **Supervision:** it was impossible for the supervising authority to discover interceptions carried out without proper judicial authorization which, combined with the law enforcement authorities' technical ability to intercept communications directly, renders supervision arrangements ineffective. Supervision by prosecutors was limited.
- **Notification of interception and available remedies:** persons whose communications were intercepted were not notified.

The judicial remedies invoked by the government were available only to persons in possession of information about the interception of their communications. Their effectiveness was therefore undermined by the absence of a requirement to notify the person subject to the interception or of an adequate possibility to request and obtain information about the interception from the authorities. Accordingly, Russian law did not provide for an effective judicial remedy against secret surveillance measures in cases where no criminal proceedings were brought against the person subject to the interception.

As such, the domestic legal provisions governing the interception of communications did not provide adequate and effective guarantees against arbitrariness and the risk of abuse. The domestic law did not meet the "quality of law" requirement and was incapable of limiting the "interference" to what was "necessary in a democratic society." Through its judgement, the ECtHR set precise standards and a compliance test for legislation in the case of mass surveillance.

K.U. v. Finland[88]

In this case, the ECtHR discussed the positive obligations of States Parties in relation to the effective protection of private life (privacy) and the use of communications data in cases related to electronic evidence and cybercrime. The case concerned a 12-year-old Finnish boy whose data was shared against his will on a dating site and who was approached by an adult. It is clear that such a (sexual) approach was illegal at the time, especially since the perpetrator remained anonymous.

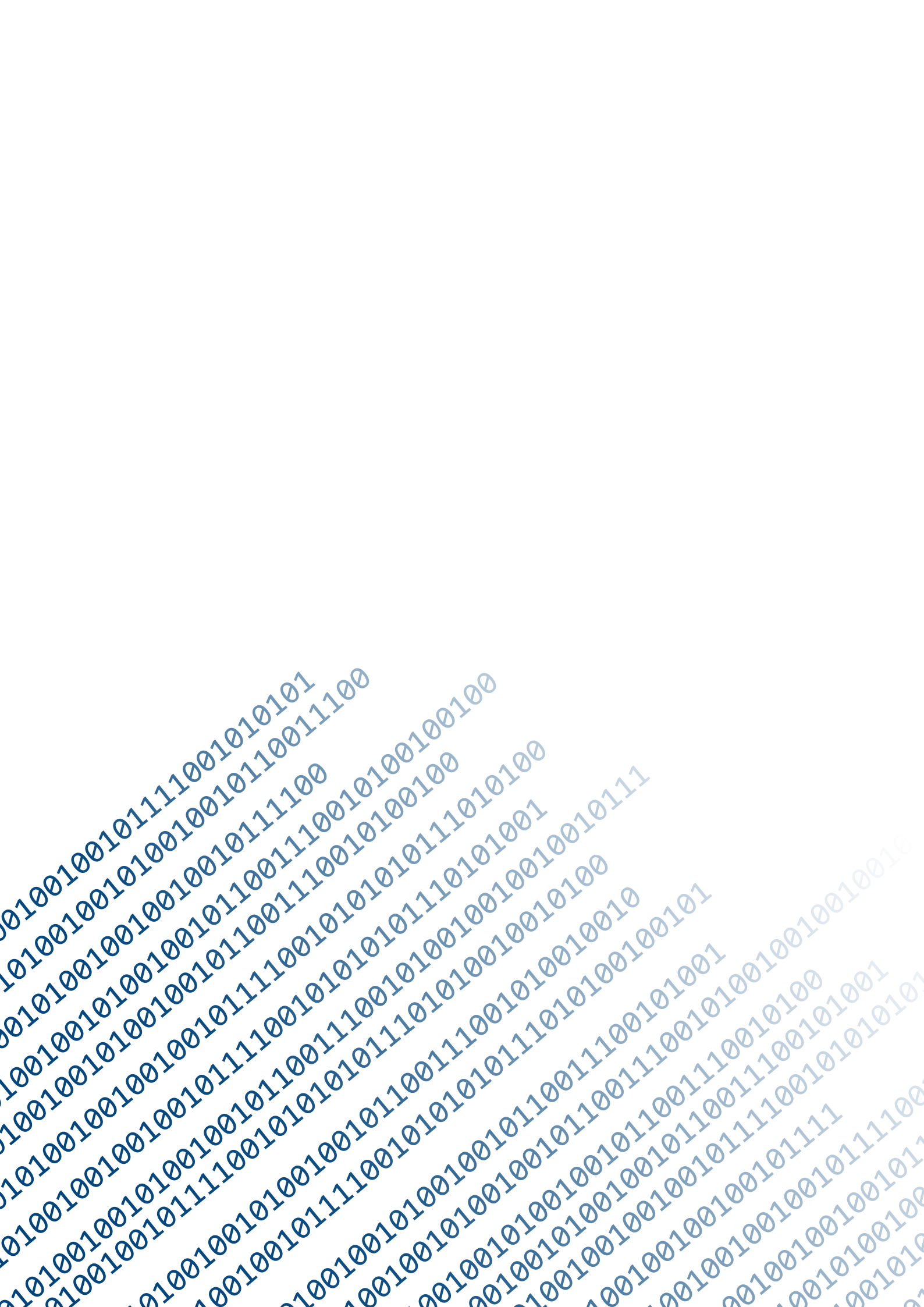
When the Finnish authorities tried to prosecute the case, they could not get the perpetrator's details from the service provider of the dating site. The service provider was not able under Finnish legislation to divulge the identity of the user upon request by the police. The Court assessed this outcome and found that the Finnish legislator had not taken sufficient measures to address such a situation.

The judgement read: "The Court considers that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case, such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality.

88 ECtHR, *K.U. v. Finland*, 2 December 2008, No. 2872/02; summarized in: ECtHR, Information Note on the Court's caselaw 114.

Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must 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."

The Court therefore concluded that the case of K.U. could not be treated effectively under the existing legal framework, leading to an infringement of the positive duty of the State to protect K.U. from this type of behaviour. The State had failed to protect K.U.'s right to respect for his private life by giving precedence to the confidentiality requirement over his physical and moral welfare.



Organization for Security and
Co-operation in Europe