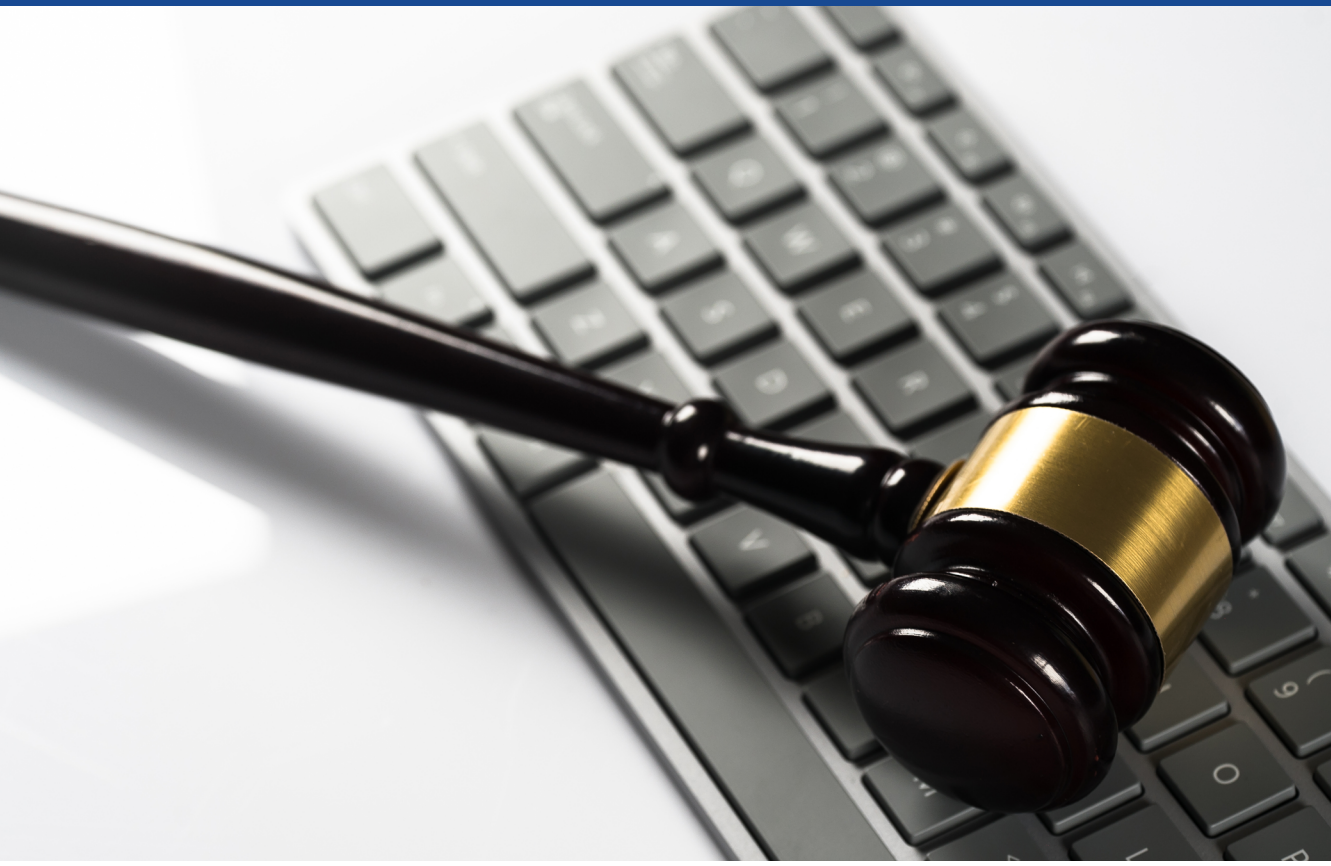
HANDBOOK

ON EUROPEAN COURT OF HUMAN RIGHTS CASE LAW CONCERNING THE USE OF ELECTRONIC EVIDENCE



Co-funded by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Co-funded and implemented by the Council of Europe

HANDBOOK

ON EUROPEAN COURT OF HUMAN RIGHTS CASE LAW CONCERNING THE USE OF ELECTRONIC EVIDENCE

This publication was produced with the financial support of the European Union and the Council of Europe. Its contents are the sole responsibility of the author(s). Views expressed herein can in no way be taken to reflect the official opinion of the European Union or the Council of Europe.

All other correspondence concerning this document should be addressed to the Directorate General of Human Rights and the Rule of Law (DGI),
Avenue de l'Europe F-67075 Strasbourg Cedex, France

Tel. +33 (0)3 88 41 20 00

E-mail: Horizontal.Facility@coe.int

Graphic design:
Studio Heber Podgorica

Cover photo:
Shutterstock

CONTENT

INTRODUCTION

This Handbook sets out the case law that the European Court of Human Rights ("the European Court") has been developing with respect to the gathering and use of electronic evidence in the criminal process in the light of the obligations arising under the European Convention on Human Rights.

Electronic evidence, as the European Court recognised in *Yüksel Yalçınkaya v. Türkiye* [GC], no. 15669/20, 26 September 2023, has become ubiquitous in criminal trials in view of the increased digitalisation of all aspects of life.

It can relate to well-established offences but also to ones specific to the digital environment, such as those required to be established under the Convention on Cybercrime and the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

The fact that crimes may be committed in cyberspace can make the need for cooperation in the gathering and exchange of electronic evidence, giving rise to arrangements such as those under Regulation (EU) 2023/1543 of the European Parliament and of the Council od 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings.

Electronic evidence will relate to data involving images, location, sounds, text and traffic through various forms of communications. It can be gathered and held in many formats, including cameras, computers, storage devices (such as CD-ROMS, DVDs, memory sticks and SIM cards).

It requires special technologies not only for its collection but also for its subsequent securing, processing and analysis. Particular challenges regarding both its gathering and subsequent use arise on account of the volume of data that can be involved, without all of it necessarily being relevant whether to the prosecution or the defence. Moreover, encryption of data may make access difficult but also underlines the encroachment on privacy that can be involved.

There is inevitably concern about its reliability given that the original content can easily be destroyed, damaged, altered and manipulated.

There are no special provisions in the European Convention dealing with electronic evidence. However, the case law of the European Court has had to address the application of the provisions in it to the specificities of gathering and using such evidence, as well as ensuring that this does not lead to unjustified interference with the guaranteed rights and freedoms.

The Handbook deals with the case law that has been elaborated by the European Court under five different chapters, namely, the evidential value of electronic evidence, the gathering of such evidence, its use in connection with pre-trial detention, how it can form the basis for a conviction and a collection of other issues that have arisen with respect to it.

The cases referred to are primarily judgments of the European Court but there also a number of admissibility decisions, which are indicated by "(dec.)" after the name of the case concerned. Although there can be more than only one application number for certain cases, only the first one is cited.

The Handbook reflects the case law up to 27 May 2024. It has been prepared by Mr Jeremy Mcbride, as a part of the Action "Strengthening accountability of the judicial system and enhancing protection of victims' rights in Montenegro", within the European Union/Council of Europe Joint Programme "Horizontal Facility for the Western Balkans and Türkiye".

1. EVIDENTIAL VALUE

The European Court has recognised that electronic evidence may be important when seeking to determine **whether particular facts can be regarded as having been established**, either in national proceedings or in applications to it.

Such facts might, for example, relate to whether:

- *certain persons were in a particular place at the time of a specific event*, such as
  - telephone and geolocation data establishing where named persons were when an alleged poisoning had occurred, as in *Navalnyy v. Russia (No. 3),* no. 36418/20, 6 June 2023;
- *the accused had committed the conduct constituting an element of an offence*, such as
  - a video recording of their involvement in loading drugs into a car, as in *Fejzulla and Mazreku v. "the former Yugoslav Republic of Macedonia",* (dec.), no. 23065/07, 31 May 2011;
- *the complicity of others in particular conduct*, such as
  - a video that showed how police facilitated an attack on certain demonstrators by counter-demonstrators, as in *Women's Initiatives Supporting Group and Others v. Georgia*, no. 73204/13, 16 December 2021;
- *the allegations against the accused might be unfounded*, such as
  - video evidence contradicting the prosecution's version of events said to implicate him, as in *Ilgar Mammadov v. Azerbaijan (No. 2),* no. 919/15, 16 November 2017;
- *there are other circumstances meaning that a conviction would not be warranted*, such as
  - an audio recording which showed that the police had put the accused under pressure to overcome his determination not to take the bribe which he had been offered, as in *Nosko and Nefedov v. Russia,* no. 5753/09, 30 October 2014;
- *there was any resistance to an arrest*, such as
  - a video recording of the applicant's arrest by a group of well-equipped police officers which showed that, from the moment when he was put on his feet until he entered the police station, the police officers' interaction with him consisted in asking whether he would start walking by himself, demanding that he stay still, and threatening to break his arm, as in *Navalnyy and Gunko v. Russia*, no. 75186/12, 10 November 2020

as well as to resolving how a particular outcome had occurred, such as

- the use in *Georgia v. Russia (II),* [GC], no. 38263/08, 21 January 2021 of high-resolution satellite imagery to establish that houses had been damaged by bombing rather than by fire.

The absence of electronic evidence might in some cases be might also be mean that *particular allegations should not be regarded as credible*. See, e.g., *Stojanović v. Croatia*, no. 23160/09, 19 September 2013, in which the absence of an audio recording led the European Court to conclude that the domestic courts' finding that a threat had been made by the applicant during the telephone conversation at issue was not based on an acceptable assessment of the relevant facts.

Nonetheless, there are a number of considerations which should preclude or limit reliance on particular electronic evidence, regardless of its potential evidential value, because this would adversely affect the overall fairness of a conviction based on it. These considerations are examined in the *Basis for conviction* chapter.

2. GATHERING EVIDENCE

Notwithstanding its potential relevance for criminal and other proceedings, electronic evidence must first be gathered and, in doing so, there are certain requirements under the European Convention which will need to be taken into account.

In the first place, electronic evidence may be amongst the forms of evidence that should be gathered in order to fulfil certain obligations under the European Convention to *conduct an effective investigation* where there is an arguable violation of particular rights, with a view to the prosecution of those responsible.

Secondly, although the *exercise of powers to gather evidence* in any criminal proceedings may result in electronic evidence being both found and seized or disclosed, as well as created through the use of various surveillance measures, the scope and use of these powers will also be subject to the need to respect certain rights under the European Convention.

2.1. CONDUCTING AN EFFECTIVE INVESTIGATION

The gathering of certain forms of electronic evidence has been recognised by the European Court as important for the fulfilment of the procedural obligations to conduct an effective investigation, notably those arising under Articles 2 and 3 with respect to deaths and alleged ill-treatment.[1]

Such forms of electronic evidence have included:

- data relating to mobile phone usage (*Enukidze and Girgvliani v. Georgia*, no. 25091/07, 26 April 2011);
- data on specific computers (*Buturugă v. Romania*, no. 56867/15, 11 February 2020);
- digital photos (*X. and Others v. Bulgaria*, no. 22457/16, 2 February 2021);
- geolocation data from mobile phones and vehicles (*Navalnyy v. Russia (No. 3)*, no. 36418/20, 6 June 2023);
- recordings from CCTV and surveillance cameras (*Skorupa v. Poland*, no. 44153/15, 16 June 2022);
- social media files (*Buturugă v. Romania*, no. 56867/15, 11 February 2020);
- USB flash drives (*Başbilen v. Turkey*, no. 35872/08, 26 April 2016);
- use made of an internet service provider's network infrastructure (*Volodina v. Russia (No. 2)*, no. 40419/19, 14 September 2021);
- video-recordings of interviews (*X. and Others v. Bulgaria*, no. 22457/16, 2 February 2021); and
- a video-recording of the force used to effect an arrest (*Sochichiu v. Moldova*, no. 28698/09, 15 May 2012)

Violations of the *procedural obligation to conduct an effective investigation* will arise where either:

- *insufficient efforts are made* to gather such relevant electronic evidence, i.e., by

1 Such an obligation has also been recognised as arising under the prohibition on slavery and forced labour and of discrimination under Articles 4 and 14 respectively.

taking all reasonable and available steps to secure it, or

- there is a *failure to make use* of such evidence gathered in the course of the investigation.

Such failings can be seen to have occurred in cases such as:

- *Enukidze and Girgvliani v. Georgia*, no. 25091/07, 26 April 2011, in which no attempt was found to have been made to establish whom one of the assailants had repeatedly called at the precise time when he and others had kidnapped certain persons and may already have been beating them and the suggestion of a resemblance to another assailant seen in a video recording of an identification parade had not been noted;

- *Balázs v. Hungary*, no. 15529/12, 20 October 2015, in which there was a failure by the prosecuting authorities to explain why the content of certain social media posts by an assailant – in which the Roma origin of the victim and the three men who had helped him get away from the situation - could not be unequivocally linked to the impugned events and why the motives for the attack on the victim could not be validly deduced from those posts. Also ignored were encouraging comments posted by the assailant's acquaintances, with one pointing on the Internet to a film scene containing an overly intolerant and racist message and widely known as such;
- *Ciorap v. Republic of Moldova (No. 5)*, no. 7232/07, 15 March 2016, in which an investigator failed to seek the original video recording of a search during which ill-treatment was allegedly inflicted despite a complaint that the copy viewed was incomplete and its electronic format meant that it was easily editable so as to exclude parts of what had been recorded;
- *X. and Others v. Bulgaria*, no. 22457/16, 2 February 2021, in which the seizure of telephones, computers, cameras, video-cameras or other media used by the persons accused of abusing a child might have made it possible either to obtain proof of that abuse or evidence concerning similar abuse of other children but this was not undertaken;
- *Lapunov v. Russia*, no. 28834/19, 12 September 2023, in which no request was made for geolocation information about the phones of a victim of torture victim and of potential witness, which could have determined their locatiotn at the material time, as well as a failure to examine the phone of a police officer that had allegedly been used to film the applicant while making a statement; and
- *Elibashvili v. Georgia*, no. 45987/21, 22 February 2024, in which the majority of the requests to seize and obtain either road-traffic or private CCTV footage relating to a police chase of another motorist were made belatedly, with potentially important evidence being lost or deleted in the meantime.

It should also be noted that a *failure to seek* electronic evidence could also lead to a finding by the European Court that a substantive, rather than a procedural, violation of those rights had occurred, as in *Olewnik-Cieplińska and Olewnik v. Poland*, no. 20147/15, 5 September 2019. In that case a delay in analysing calls using a known telephone SIM – which would have led to a link with kidnappers and the identification of the location and tracing of the calls made by them - was a contributory factor in its finding that there had been a failure to safeguard the life of a person who had been kidnapped.

Finally, as the evidence obtained during the investigation stage often determines the framework in which the offence charged will be considered at the trial, it was recognised in *Haarde v. Iceland*, no. 66847/12, 23 November 2017 that the *pre-trial collection of evidence could be deficient* to the detriment of an accused and thus give rise to a violation of Article 6(1) of the European Convention. However, that was not found to have occurred in that case, in which the prosecutor had had access to a relevant database and correspondence from the applicant's work email.

2.2. EXERCISING POWERS TO GATHER EVIDENCE

The gathering of evidence – whether through disclosure obligations applicable to those possessing or controlling it, the exercise of search and seizure powers or the surveillance measures (such as through the interception of communication, eavesdropping and audio and video-recording and the use of tracking devices) – where it is non-consensual always has the potential to interfere with the right guaranteed by Article 8 of the European Convention, as well as of the rights to freedom of expression and to property under Article 10 Article 1 of Protocol No. 1 where, respectively, this affects journalists and media organisations and involves the taking of physical items.

In addition, a compulsion to disclose information that would entail self-incrimination would be inconsistent with the right to a fair trial under Article 6(1).

2.2.1 Consent

The existence of this can be seen in a case such as *Posevini v. Bulgaria*, no. 63638/14, 19 January, where the police were only able to go through the applicant's email account because he had given them his password and invited them to do so and there was no evidence that he had done so under overt or implied coercion.

However, *co-operation* in the provision of information will not make it consensual where the person doing so has been made to understand that there was no choice but to allow access to the material concerned. This was found to have occurred in, e.g., *Saint-Paul Luxembourg S.A. v. Luxembourg*, no. 26419/10, 18 April 2013, where police officers had made it clear that they could carry out a search by force in the event of a refusal to cooperate.

The gathering of evidence that is *non-consensual* can be regarded as an admissible interference with the rights under the European Convention **only** where this:

- has a *basis in law*;
- that basis meets the criteria of *accessibility* and *foreseeability*;
- has *a legitimate aim*; and
- is *necessary in a democratic society*.

Furthermore, these requirements should have been respected whenever the gathering of material that could become evidence occurs in another country. This is both as regards a Party to the European Convention itself gathering such evidence in the absence of a request for international legal assistance in criminal matters(as was found to have occurred in *Bosak and Others v. Croatia*, no. 40429/14, 6 June 2019 with respect to the use of surveillance measures) and to the requesting from and receipt of such material from a State that is not a party to the European Convention (as was considered to be the case in *Big Brother Watch and Others v. United Kingdom* [GC], no. 58170/13, 25 May 2021 with respect to intercept material that had been gathered by a foreign intelligence service).

2.2.2 A basis in law

The gathering of evidence which has no basis at all in law for undertaking it will necessarily amount to a violation of Article 8.

This will be so whether the evidence is gathered by law enforcement officials or by private individuals who act either under their direction (as in *M.M. v. Netherlands*, no. 39339/98, 8 April 2003, in which telephone conversations had been recorded at the suggestion of the police on equipment that they had installed) or with their technical assistance (as in *Van Vondel v. Netherlands*, 38258/03, 25 October 2007, where the recordings of conversations had been made by the individual on a voluntary basis but the police had given instructions as to what should be recorded).

Such a basis can be provided by *any provision having the force of law* under the legal system of the State concerned. It is not necessary that it take the form of legislation adopted by the legislature but can extend to a provision adopted under powers delegated to administrative bodies.

However, *a mere practice* will be insufficient for this purpose, as was the situation found to exist in *Heglas v. Czech Republic*, no. 5935/02, 1 March 2007, relating to the recording of a conversation as the relevant power had not yet entered into force.

3.1. ABSENCE OF A BASIS IN LAW

This will be the situation where:

- there is *no legal provision* that actually allowed a particular measure to be undertaken, such as was the case regarding the interception of communications, the use of covert listening devices and the monitoring of email and internet usage considered respectively in *Malone v. United Kingdom*, no. 8691/79, 2 August 1984. *Bykov v. Russia* [GC], no. 4378/02, 10 March 2009and *Copland v. United Ki*ngdom, no. 62617/00, 3 April 2007; or
- there is a *failure to observe the limits specified* in the authorisation given under a specific provision, such as

- who could provide that authorisation,
- the procedures to be followed, its duration,
- those covered by it and
- the proceedings to which it could be given

as seen respectively in *A. v. France*, no. 14838/89, 23 November 1993, *Perry v. United Kingdom*, no. 63737/00, 17 July 2003, *Kvasnica v. Slovakia*, no. 72094/01, 9 June 2009, *Mikhaylyuk and Petrov v. Ukraine*, no. 11932/02, 10 December 2009 and *Karabeyoğlu v. Turkey*, no. 30083/10, 7 June 2016.

Moreover, no reliance can be placed on a legal provision *coming into effect only after the particular measure has occurred*, as was the situation in *Heglas v. Czech Republic*, no. 5935/02, 1 March 2007.

In all cases, it will be important to check *whether certain requirements in a law are actually applicable to a specific situation*. This was not the case in, e.g., *Blagajac v. Croatia*, no. 50236/16, 9 May 2023, in which the European Court accepted the respondent government's submission that a search of the laptop and mobile phones belonging to a lawyer that had been seized following a search of his premises was not unlawful as a legal requirement for an investigating judge and a representative of the bar association to be present only applied in the case of the search of the lawyer's person or law office.

Furthermore, *limits on the ability to use particular powers* in respect of certain persons must also be observed, as did not occur in *Aydin Sefa Akay v. Türkıye*, no. 59/17, 23 April 2024 when the premises of a international judge enjoying diplomatic immunity were searched.

3.2. ACCESSIBILITY

This *requirement* will normally be satisfied by the publication of the legal provisions concerned.

Thus, in *Mikhaylyuk and Petrov v. Ukraine*, no. 11932/02, 10 December 2009, it found this requirement not to be fulfilled where instructions on dealing with correspondence by the organs of the interior ministry and a penitentiary service were internal and unpublished and, thus, not accessible to the public.

However, the European Court has sometimes considered that it will be fulfilled if the legal provisions are *in practice accessible*, even if not officially published.

This was, e.g., the situation in *Roman Zakharov v. Russia* [GC], 47143/06, 4 December 2015 concerning a ministry's order relating to interception of communications, which was published in its official magazine that was distributed through subscription, making it available only to communications specialists rather than to the public at large. However, the text of the order, with the addendums, could be accessed through a privately-maintained internet legal database, which reproduced it from the publication in the official magazine. The European Court concluded that, taking into account the fact that it has been published in an official ministerial magazine, combined with the fact that it could be accessed by the general public through an internet legal database, it was not necessary to pursue further the issue of compliance with the accessibility requirement.

3.3. FORESEEABILITY

A legal provision relating to *disclosure obligations* and *powers of search and seizure* will be considered by the European Court to be "foreseeable" if it is formulated with sufficient precision to enable individuals – if need be, with appropriate advice – to regulate their conduct.

This will not be the case where there:

- is *disagreement as to the legal basis*, such as

- initial legal basis for inspection and seizure measures relating to a computer and a computer hard drive had been found to have been altered in *Bože v. Latvia*, no. 40927/05, 18 May 2017 and there had then been disagreement among the authorities as to which specific provision of the relevant legislation had regulated the police actions concerned;

- is *imprecision regarding important safeguards or these are absent*[2], such as

- where there was found in *Petri Sallinen v. Finland*, no. 50882/99, 27 September 2005, to be no applicable regulations specifying with an appropriate degree of precision the circumstances in which legally privileged material on the hard disk of a lawyer's computer could be subject to search and seizure, meaning that the applicants were deprived of the minimum degree of protection to which they

2 However, where legislation permitting secret surveillance is contested before the European Court, it sees the lawfulness of the interference as being closely related to the question of whether the test of being "necessary in a democratic society has been complied with so that it tends to address both requirements jointly. In its view, the "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application but must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing adequate and effective safeguards and guarantees against abuse; see *Roman Zakharov v. Russia* [GC], 47143/06, 4 December 2015, at para. 236. As a result, the safeguards required for gathering evidence by secret surveillance measures are considered in the "Necessary in a democratic society" segment below.

were entitled under the rule of law in a democratic society

- where, after the seizure of a lawyer's mobile phone and laptop, the law was seen in *Särgava v. Estonia*, no. 698/19, 16 November 2021 to be unclear as to how any potential disputes between the investigative authorities and the lawyer concerned over the keywords to be used or any other methods of filtering the electronic content would be resolved. Indeed, the law did not seem to have any specific rules about the procedure to be followed in the event that either the lawyer or his representative objected to the seizure or content examination with reference to lawyer-client confidentiality and

- where there was some legal basis for a search, the law concerned was seen in *Taraneks v. Latvia*, no. 3082/06, 2 December 2014 not to provide sufficient judicial safeguards, either before the grant of a search warrant or after a search so that the applicant was thus deprived of the minimum degree of protection to which he was entitled under the rule of law in a democratic society

- where, as was found in *Sanoma Uitgevers B.V. v. Netherlands* [GC], no. 38224/03, 14 September 2010, there was no procedure attended by adequate legal safeguards in order to enable an independent assessment as to whether the interest of the criminal investigation overrode the public interest in the protection of journalistic sources, where the company owning a magazine was required to surrender photographs on a CD-ROM of illegal car races. In urgent cases, the European Court considered that a procedure should exist to identify and isolate, prior to the exploitation of the material by the authorities, information that could lead to the identification of sources from information that carries no such risk.

- where rather than there being any rules by which to determine when it might be and when it might not be permissible to breach the confidentiality of legally privileged documents, it was found in *Kruglov and Others v. Russia*, no. 11264/04, 4 February 2020, the courts seemed to imply that lawyer-client confidentiality could be breached in every case as long as there was a criminal investigation, even where such investigation was not against the lawyers but against their clients;

- *Kadura and Smaliy v. Ukraine*, no. 42753/14, 21 January 2021, where there were no safeguards in place against the authorities accessing, improperly and arbitrarily, information subject to legal professional privilege on a lawyer's mobile phone that was searched as an incident of his arrest while representing a client at the police station;

• has been an *interpretation that could not be anticipated*, such as

- where the reference to "goods" in customs legislation as being movable property that is being transferred across the customs border was found in *Ivashchenko v. Ukraine*, no. 61064/10, 13 February 2018 to have been construed to cover such items as laptops, flash memory cards, cameras, video-cameras, printed material and the like. This served as a basis for then asserting that such "goods" could be lawfully subjected to the sampling procedure, without any further consideration of the context in which the customs control concerned the non-material digital contents (electronic data amounting to information or images, for instance) accessed by way of "opening" a "container" (the laptop) The European Court did not consider that the reading given to the relevant legal provisions constituted a foreseeable interpretation of national law, thereby providing a legal basis for the copying of electronic data contained in electronic documents located in such a "container" as a laptop.

Nonetheless, the necessary precision can also be provided by *a substantial body of case-law* relating to the provision concerned, as was the situation in *K.S. and M.S. v. Germany*, no. 33696/11, 6 October 2016 regarding the possibility of a search warrant being based on data despite the fact that this may have been acquired in breach of the law.

In the case of surveillance, the European Court in *Roman Zakharov v. Russia* [GC], 47143/06, 4 December 2015 confirmed that "foreseeability" in the special context of secret measures of surveillance, such as the interception of communications, could not mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly.

Rather, as the risks of arbitrariness were evident, especially where a power vested in the executive is exercised in secret, it was essential to have *clear, detailed rules on interception of conversations*, especially as the technology available for use was continually becoming more sophisticated. Thus, the must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures.

Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, *it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power*. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

This has led the European Court to elaborate *certain minimum safeguards*, the observance of which is relevant to whether the interference with the right under Article 8 is kept to what is "necessary in a democratic society". As a result, these safeguards are discussed in the sub-section below concerned with that issue.

3.4. LEGITIMATE AIM

This requirement will be met where the measures taken are for th*e prevention of disorder of crime*, which includes ones to secure evidence for a prosecution (as recognised by the European Court in, e.g., *Nagy v. Hungary*, no. 6437/02, 20 December 2005, at para. 26) or to *facilitate the investigation of future crimes* (as found by it in *P.N. v. Germany*, no. 74440/17, 11 June 2020, at para. 68).

At the same time, the nature of the offences involved may mean that other legitimate aims are also served by measures to gather evidence, notably, t*he economic well-being of the country* (such as the search relating to observance of competition rules considered in *Naumenko and Sia Rix Shipping v. Latvia*, no. 50805/14, 23 June 2022), the *fight against corruption*, such as the search of the laptop and mobile phone examined in *Blagajac v. Croatia*, no. 50236/16, 9 May 2023) and *national security* (such as the interception of telephone conversations considered in *Draksas v. Lithuania*, no. 36662/04, 31 July 2012).

3.5. NECESSARY IN A DEMOCRATIC SOCIETY

The specific elements involved in achieving compliance with this requirement will vary according to the particular measure involved.

4. DISCLOSURE OBLIGATIONS

In the case of obligations to provide information or documents in an electronic format, this is likely to be satisfied where the information sought from those possessing or controlling it is *strictly limited*, as in *P.G. and J.H. v. United Kingdom,* in which there was a requirement to disclose specific billing information about telephone calls that had been made but this had only concerned the telephone numbers called from a suspect's flat between two specific dates and thus did not include any information about the contents of those calls or who had made or received them.

4.1. TELECOMMUNICATION COMPANIES AND INTERNET SERVICE PROVIDERS

Furthermore, the European Court is likely to accept some obligation being imposed on telecommunication companies and internet service providers to disclose the identity of their users where this can be shown to be necessary for the alleged perpetrator of offences such as those threatening a person's physical or moral integrity or involving the use of as hate speech to be identified and brought to justice.

Thus, a violation of Article 8 was found in *K.U. v. Finland*, no. 2872/02, 2 December 2008 as a result of the absence of a remedy for a 12-year-old who had been the subject of an advertisement of a sexual nature on an Internet dating site where the law did not provide for the possibility of obtaining the identity of the person who had placed it from the Internet service provider.

See also *Delfi AS v. Estonia* [GC], no. 64659/09, 16 June 2005, in which a factor in concluding that the imposition of civil liability on the owner of a news portal for hate speech posted on it was its failure to assist in identifying the author concerned. See also the requirements under the Convention on Cybercrime that obliges the States party to it to make measures such as the real-time collection of traffic data and the issuing of production orders available to the authorities in combating crimes such as those relating to child pornography.

However, in imposing such obligations, the general retention of communications data by communications service providers and its access by the authorities in individual cases must be accompanied, *mutatis mutandis*, by the same safeguards as secret surveillance (as to which, see ***Surveillance measures*** below).

As regards safeguards against abuse by officials in the procedure for access to and transfer of such data, it was found in *Benedik v. Slovenia*, no. 62357/14, 24 April 2018 that the police, could have identified an author by merely asking the ISP provider to look up that information and there was no independent supervision of the use of these powers, despite the fact that those powers, as interpreted by the courts, compelled the ISP to retrieve the stored connection data and enabled the police to associate a great deal of information concerning online activity with a particular individual without his or her consent.

Similarly, in *Podchasov v. Russia*, no. 33696/19, 13 February 2024, the European Court concluded that legislation providing for the retention of all Internet communications of all users, the security services' direct access to the data stored without adequate safeguards against abuse and the requirement to decrypt encrypted communications, as applied to end-to-end encrypted communications, could not be regarded as necessary in a democratic society as it impaired the very essence of the right to respect for private life under Article 8 of the Convention.

Nonetheless, the European Court in both *Podchasov* and *Yüksel Yalçınkaya v. Türkiye* [GC], no. 15669/20, 26 September 2023[3] has acknowledged that encryption could also be used by criminals, thereby complicating criminal investigations. In that connection, it noted in the former case that there were calls for alternative solutions to decryption which did not weaken the protective mechanisms, both in legislation and through continuous technical evolution.[4] It also referred to some of the alternatives that had been cited by a third-party intervener, namely, the use of live forensics on seized devices, guessing or obtaining private keys held by parties to the communication, the use of vulnerabilities in the target's software or the sending of an implant to targeted devices.

Moreover, where access was obtained to communications data that had been retained in breach of privacy requirements because of its systemic, indiscriminate and general manner, it was held in *Škoberne v. Slovenia*, no. 19920/20, 15 February 2024 that access to such data – and its subsequent processing and storage by the authorities – could not, for the same reason, comply with Article 8.

On the other hand, in *Breyer v. Germany*, no. 50001/12, 30 January 2020, there was considered to be protection against excessive or improper information requests regarding the stored data relating to users of pre-paid SIM cards by the retrieval being limited to necessary data involving at least an initial suspicion of an offence, with this necessity requirement being safeguarded by a general obligation for the respective authorities retrieving the information to erase, without undue delay, any data they do not need. Moreover, there existed possibilities of review and supervision of information requests, with also independent supervision by data protection authorities and the ability to seek legal redress against information retrieval under general rules.

In addition, there should also be an effective remedy to alleviate the suspicion among the general public that retained communications data is being abusively accessed and used, which was not established in *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, 11 January 2022

4.2. PERSONS OTHER THAN SUSPECTS

The width of an order for disclosure is likely to be seen as problematic by the European Court in situations where this relates to banking information where this affects an individual who was not subject to the ongoing investigation in relation to which the letters rogatory for assistance had been made and in respect of whom no clear suspicions had been advanced. In that case, the fact that this had been decided by a judicial authority was considered insufficient by the European Court in *M.N. v. San Marino*, no. 28005/12, 7 July 2015 given that it could not, or in any event, had failed to make any assessment as to the need for such a wide-ranging order, or its impact on the multiple third parties concerned.

Furthermore, where - as in the case of *M.N. v. San Marino* - criminal proceedings are involved, there will be a need for affected persons to have "effective control" over the disclosure requirement in the sense of being able to challenge the measure to which they have been subjected and thus, subsequent to the implementation of the order concerned, to have available to them some means for reviewing it. In that case, unlike persons who were accused, there was no such possibility that would enable them to restrict the interference in question to what was "necessary in a democratic society".

3 At para. 312.

4 It cited, in that regard a Joint Statement by Europol and the European Union Agency for Cybersecurity (ENISA) of 20 May 2016 on lawful criminal investigation that respects 21st Century data protection and the *Report on the right to privacy in the digital age* by the Office of the United Nations High Commissioner for Human Rights, (4 August 2022, A/HRC/51/17), paras. 21-26.

4.3. JOURNALISTS

A requirement for a journalist to disclose research material that does not entail the possible identification of his or her sources where this could assist the investigation and production of evidence in a case will not be incompatible with Article 10, so long as this was not disproportionate to that legitimate aim. This was the situation in, e.g., *Nordisk Film & TV A/S v. Denmark* (dec.), no. 40485/02, 8 December 2005, where the material sought concerned film taken by a journalist working undercover by a journalist of two persons known to the police who were unaware that they were being recorded, as well as various notes. The disclosure requirement specifically excluded material concerning journalistic sources in the traditional sense.

Moreover, a requirement to hand over a letter to a magazine from a person claiming to have carried out three bomb attacks, the contents of which it had subsequently published, was not regarded by the European Court in *Stichting Ostade Blade v. Netherlands* (dec.), no. 8406/06, 27 May 2014 as either affecting a journalistic source or as being incompatible with Article 10 given that the original document was sought as a possible lead towards identifying a person or persons unknown who were suspected of having carried out a plurality of bomb attacks.

However, it will be very hard to justify the imposition of a disclosure requirement on journalists which might lead to the identification of a source since the European Court is concerned that such compulsion might lead to the vital public-watchdog role of the press being undermined and the ability of the press to provide accurate and reliable information being adversely affected.

As a result, an order for disclosure – which might, e.g., affect photographs and video and voice recordings - will not be regarded as compatible with Article 10 of the European Convention unless it is justified by an overriding requirement in the public interest.

This will not be regarded as having been established where its objective is to guard the integrity of the police (*Voskuil v. Netherlands*, no. 64752/01, 22 November 2007), to prevent the disclosure of confidential information by a disloyal employee (*Financial Times Ltd. and Others v. United Kingdom*, no. 821/03, 15 December 2009) or to recover copies of illegally disclosed documents where their destruction could be supervised (*Telegraaf Media Nederland Landelijke B.V. and Others v. Netherlands*, no. 39315/06, 22 November 2012).

Nonetheless, a disclosure requirement affecting journalists might be capable of being justified where it can be demonstrated that the disclosure of the source is necessary to secure the fair trial for an accused person, which was not established in *Voskuil v. Netherlands*, no. 64752/01, 22 November 2007, where the court was apparently able to substitute the evidence of other witnesses for that which it had attempted to extract from the applicant.

4.4. LAWYERS

Lawyers should not be required to disclose information covered by legal professional privilege or professional secrecy as the European Court has made it clear in *Michaud v. France*, no. 12323/11, 6 December 2012 that that would strike at the very essence of their defence role.

However, as that case made clear, a requirement - supported by the liability to disciplinary action - for lawyers to report suspicious operations by people who come to them for advice is not necessarily incompatible with Article 8.

In particular, this would not be so where:

- the lawyers are themselves taking part in money-laundering activities,
- their legal advice is provided for money-laundering purposes,
- they know that the client is seeking legal advice for such purposes or
- this requirement concerns tasks other than those relating to the defence of their clients

and sufficient safeguards are in place, such as the filter in that case whereby the Chairman of the Bar could first determine which information is covered by lawyer-client privilege and would then only transmit a report of suspicions after having ascertained that the relevant conditions had been met.

5. SEARCH AND SEIZURE

A non-consensual search will only be regarded as necessary in a democratic society and thus not a violation of Article 8 where the reasons adduced to justify such a measure were *"relevant" and "sufficient"* and the *proportionality principle* has been respected.

This will necessitate:

- A *reasonable suspicion* that an offence has been committed by the person under investigation or that there has been an infringement of legislation governing economic activities so that the interference with the right under Article 8 can be regarded as pursuing the legitimate aim concerned, such as in *Lindstrand Partners Advokatbyrå AB v. Sweden*, no. 18700/09, 20 December 2016 (concerning the need to search two premises to determine the ownership and declared business costs of a number of named, interrelated companies and referring to a particular individual's involvement in all of them) but not in *Aliyev v. Azerbaijan*, no. 68762/14, 20 September 2018 (in which the search was justified merely by referring in vague terms to the criminal investigation into "breaches of legislation discovered in the activities of a number of non-governmental organisations" without asserting any specific facts related to the suspected crimes of abuse of power and forgery);

- A *particularly strong justification* where the person affected is not her or himself suspected of the offence in respect of which the investigation is being undertaken, as was the case with the managers and employees in the search of the organisation considered in *International Research and Exchange Board v. Azerbaijan*, no. 7668/15, 2 March 2023;

- The offence for which the search is undertaken being of *sufficient gravity* to justify the interference with the right guaranteed by Article 8, something not satisfied in *Buck v. Germany*, no. 41604/98, 28 April 2005, where the offence involved was the mere contravention of a road traffic rule;

- The inability of achieving the search's objective through *less intrusive means*, as in *Zubal v. Slovakia*, no. 44065/06, 9 November 2010 (in which there was actually a willingness to cooperate with the investigation) and *Kruglov and Others v. Russia*, no. 11264/04, 4 February 2020 (in which there was the possibility of obtaining the information from the clients of lawyers rather than the lawyers themselves);

- *Judicial control*, which should normally take the form of prior authorisation where the judges duly examine the existence of a reasonable suspicion, draw up the search warrant in such a way as to keep its impact within reasonable bounds and satisfy themselves that a search in the place in respect of which the warrant was sought could yield relevant evidence (*Vinks and Ribicka v. Latvia*, no. 28926/10, 30 January 2020, at para. 104) **but** in urgent cases (e.g., to prevent the destruction or concealment of documents, the need for which was not demonstrated in *Nagla v. Latvia*, no. 73469/10, 16 July 2013), *ex post facto* judicial review will be acceptable so long as those affected are not precluded from seeking it, there are clear rules as to its scope, there is then a genuine consideration of the actual need to act without first seeking judicial authorisation and the actual review carried out can be considered efficient (see respectively, *Kruglov and Others v. Russia*, no.

11264/04, 4 February 2020, *Prezhdarovi v. Bulgaria*, no. 8429/05, 30 September 2014, *Taraneks v. Latvia*, no. 3082/06, 2 February 2014 and *Stefanov v. Bulgaria*, no. 73284/13, 16 November 2021);

- An *order or warrant* for the search that

  (a) contains information about the ongoing investigation, the purpose of conducting it or why it was believed that it would enable evidence of any offence to be obtained, as well as adequate record-keeping of the authorisation given (see *Iliya Stefanov v. Bulgaria*, no. 65755/01, 22 May 2008 for deficiencies in this regard),
  (b) is not broadly drawn (unlike in *Aleksanyan v. Russia,* no. 46468/06, 22 December 2008, in which neither the application for the warrant nor the warrant itself specified what items and documents were expected to be found in the office to be searched or how they would be relevant to the investigation),[5]
  (c) covers the person, premises or item to be searched (see *Avaz Zeynalov v. Azerbaijan*, no. 37816/12, 22 April 2021 in which the warrant applied to the applicant's home and workplace but not to the vehicle being parked in the courtyard of the latter) and
  (d) is reasonably limited in time (as in *Cacuci and S.C. Virra & Cont Pad S.R.L. v. Romania*, no. 27153/07, 17 January 2017);

- The *serving of the order or warrant* on those affected so as to give them precise information about the scope of the search (as did not occur in *Imakayeva v. Russia*, no. 7615/02, 9 November 2006);

- The *presence of the persons* whose premises or items such as phones are being searched when this occurs so that they can contest that particular items being seized are covered by the order or warrant (a point made in *Modestou v. Greece*, no. 51693/13, 16 March 2017);[6]

- A *record or description* being made of any item seized (as could not be produced in, e.g., *Imakayeva v. Russia*, no. 7615/02, 9 November 2006);

- Appropriate consideration being given to the *potential impact of searches* affecting the media and lawyers on the respective rights to freedom of expression and to a fair trial, with (a) special authorisation being required for the search and seizure of their professional materials (as was not given in *Taner Kılıç v. T*urkey, no. 70845/01, 24 October 2006), (b) either a prohibition on removing material covered by lawyer-client privilege (As was found lacking in *Aleksanyan v. Russia*, no. 46468/06, 22 December 2008) or the supervision of the search by an independent observer capable of identifying, independently of the investigation team, which material was covered by legal professional privilege and professional secrecy and could not, therefore, be removed (as occurred in *Tamosius v. United Kingdom* (dec.), no. 62002/00, 19 September 2002 but not in *Močuļskis v. Latvia*, no. 71064/12, 17 December 2020), which may entail a sifting procedure in respect

5 However, when assessing whether a particular order or warrant is too broad, account can be taken of the nature of the allegations involved; see *Sher v. United Kingdom*, no. 5201/11, 20 October 2015 (in connection with terrorist attacks) and *Vinks and Ribicka v. Latvia*, no. 28926/10, 30 January 2020 (in connection with large-scale tax evasion and money laundering).

6 However, a refusal to take part in the search will probably be taken as a waiver of this particular safeguard, as occurred in *Cacuci and S.C. Virra & Cont Pad S.R.L. v. Romania*, no. 27153/07, 17 January 2017.

of electronic data that has been indiscriminately collected (a procedure followed in *Naumenko and Sia Rix Shipping v. Latvia*, no. 50805/14, 23 June 2022 but not in *Sergey Sorokin v. Russia*, no. 52808/09, 30 August 2022) and (b) suitable safeguards to ensure that any later examination of material removed does not infringe this privilege (as occurred in *Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal*, no. 27013/10, 3 September 2015, where the computer files and emails that were seized had been sealed and sent to the President of the Court of Appeal and had subsequently been opened and examined by its Vice-President. This also means that the investigative body should not have access to the material before this procedure is duly completed, something emphasised in *Lindstrand Partners Advokatbyrå AB v. Sweden*, no. 18700/09, 20 December 2016 as having been respected. Furthermore, the possibility of appealing against any decision allowing material to be examined by investigators or prosecutors was emphasised in *Wolland v. Norway*, no. 39731/12, 17 May 2018 and *Mirmotahari v. Norway* (dec.), no. 30149/19, 8 October 2019 as ensuring compatibility with the rule of law). Also, a judge undertaking a sifting exercise after material has been seized must, when presented with reasoned submissions as to precisely identified material being unrelated to the investigation or falling within the scope of confidentiality of the lawyer-client relationship, rule on their fate following a concrete control of proportionality and, if necessary, order their restitution, as was found not to have occurred in *Vinci Construction and GMT genie civil and services v. France*, no. 63629/10, 2 April 2015 but to have done so in *Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal*, no. 27013/10, 3 September 2015. In addition, the inadequacy of the legislative framework may render ineffective particular supervision arrangements, as was the situation in *Särgava v. Estonia*, no. 698/19, 16 November 2021 regarding the resolution of disputes as to the filtering of the electronic content being examined on lawyer's mobile phone and laptop subsequent to the seizure of them in a search; and

- Making arrangements to *limit access to unrelated personal data* (see, e.g., *Kent Pharmaceuticals Limited and Others v. United Kingdom* (dec.), no. 9355/03, 11 October 2005, relating to computer stored images of the wife of the person subjected to the search).

All such *safeguards must actually prove effective* in the particular circumstances of the search concerned.

This was found not to be so in *Wieser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, 16 October 2007 as regards the examination of electronic data in the course of a search.

Thus, the member of the Bar Association, though temporarily present during the search of the computer facilities, was mainly busy supervising the seizure of documents and could therefore not properly exercise his supervisory function as regards the electronic data. Secondly, the report setting out which search criteria had been applied and which files had been copied and seized was not drawn up at the end of the search but only later the same day.

Furthermore, the remedy against the examination of the electronic data seized from a lawyer's office under a broadly drawn warrant was unsatisfactory in *Robathin v. Austria*, no. 30457/06, 3 July 2012 where the court gave only very brief and rather general reasons when authorising the search of all the data and, in particular, did not address the question whether it would be sufficient to search only those discs which contained data relating to

the two persons under investigation and did not give any specific reasons for its finding that a search of all data was necessary for that investigation. Moreover, the officers apparently left once they had finished their task without informing the first applicant or the representative of the Bar Association of the results of the search.

See also *Kruglov and Others v. Russia*, no. 11264/04, 4 February 2020, where the safeguard of having recourse to legal assistance during a search was unavailable to at least one applicant on the pretext that her lawyer had arrived at the scene belatedly when the search had already begun. In that case, it was difficult see how the lawyer could have appeared at the beginning of a search, given that the applicant had not been notified about the search in advance and the time at which the search had started had not been chosen by her.

In addition, the *independent observer* should:

(I) have the requisite legal qualification in order to effectively participate in the procedure;

(II) be bound by the lawyer-client privilege to guarantee the protection of the privileged material and the rights of the third persons; and

(III) be vested with the requisite powers to be able to prevent, in the course of the sifting procedure, any possible interference with the lawyer's professional secrecy, which was the case, e.g., in *Lindstrand Partners Advokatbyrå AB v. Sweden*, no. 18700/09, 20 December 2016 but not *Kruglov and Others v. Russia*, no. 11264/04, 4 February 2020, where the observers had no legal qualification.

Where lawyer-client confidentiality or professional secrecy is not involved, the presence of non-lawyers as observers may be considered a sufficient safeguard against abuse, as in *Koval v. Bulgaria* (dec.), no. 38482/11, 1 October 2019, where they were cadets in the city's military school.

Any seizure during a search of material that was not covered by the authorisation for it, as well as of material seized during a search that has no legal basis, would constitute violations of Article 8 and of 1 of Protocol No. 1; such as in *Bagiyeva v. Ukraine*, no. 41085/05, 28 April 2016 (which concerned the seizure of mobile telephones when these did not come within the scope of the warrant concerned) and *Zaurbekova and Zaurbekova v. Russia*, no. 27183/03, 22 January 2009 (in which a computer central processing unit and compact discs when there was no warrant at all).

In all cases, the conduct of searches and seizures should not involve the *use of unnecessary force*.

Thus, the European Court was not convinced in *Anzhelo Georgiev and Others v. Bulgaria*, no. 51284/09, 30 September 2014 that the legitimate aim of preventing the destruction of electronic evidence in the applicant company's computers could not be achieved by more appropriate and less intrusive means which did not require using physical force after entering the offices. The authorities were held to have failed to discharge the burden satisfactorily to disprove the applicants' version that there was no necessity for the use by masked of force, as well as handcuffs and electroshock batons, against some employees of the company who had sustained injuries, leading to a finding of a violation of the prohibition of ill-treatment in Article 3 of the European Convention in both its substantive and procedural aspects.

See also *Vinks and Ribicka v. Latvia*, no. 28926/10, 30 January 2020, in which it was held that there were insufficient safeguards against abuse, and thus a violation of Article 8, where

a search and seizure in respect of digital passwords, several laptops and hard drives, CDs and USB flash drives, several cell phones and SIM cards was carried out by a heavily-armed anti-terrorism unit that forced its entry by breaking through the windows into the applicants' home and used restraint measures and guns on them and teenage daughter of one of them in the early hours of the morning.

Moreover, a search should not be carried out in a way that *damages the reputation* of the person or entity concerned, which was not established in either *Lindstrand Partners Advokatbyrå AB v. Sweden*, no. 18700/09, 20 December 2016 or *Kolev v. Bulgaria* (dec.), no. 38482/11, 1 October 2019.

There also need to be appropriate *safeguards regarding access* to, and further handling of, any material that has been retained. None were found in respect of privileged information in *Stefanov v. Bulgaria*, no. 73284/13, 16 November 2021, concerning the whole content of a memory key that had been copied, initially on a computer, from where it was transferred onto at least two digital carriers (disks). No legal requirements were cited as regards the keeping of such data or their destruction and they appears to have been deleted from an expert's computer because of lack of storage space or as a result of internal practice, without any rules or guarantees about how the information had to be handled in the process. Moreover, it also appeared that a digital copy might have been additionally kept in the institute conducting the expertise and no guarantees were shown to exist in relation to access and further handling of the data.

Furthermore, any material seized should be *returned where it is not required*, or is no longer required, for the relevant proceedings and there should not be any lack of diligence in determining what may be needed for this purpose. Thus, a violation of Article 1 of Protocol No. 1 was found in *Gration Treyd, TOV v. Ukraine*, no. 9166/14, 22 February 2024, where the prosecution authorities failed to comply with the applicable safeguards under the applicable legislation and the investigating ordered that the relevant property be withheld without giving any explanation despite having held the day before that its retention was unlawful and that it should be returned.

There was not considered to be any such lack of diligence in *Wolland v. Norway*, no. 39731/12, 17 May 2018 as regards the year taken by a court to review 2,309 electronic documents, having regard to its efforts to expedite the process after a delay in their transmission to it by the prosecution and an interruption in the review by the applicant's appeals to two higher courts. In this connection, it was also material that the hard disk and the laptop concerned had been returned to the applicant two days after the initial search at his premises. The last point can be contrasted unfavourably with the keeping of a computer and peripherals for more than a month after being checked, which contributed to the finding of a violation of Article 8 in *Iliya Stefanov v. Bulgaria*, no. 65755/01, 22 May 2008.

Where electronic documents have been copied for the purpose of the investigation, such copies should be *deleted when no longer required*.

Thus, in *Bernh Larsen Holdings AS and Others v. Norway*, no. 24117/08, 14 March 2013, the European Court was satisfied with the procedure requiring that, after the review had been completed, the copy would either be deleted or destroyed and all traces of the contents would be deleted from the tax authorities' computers and storage devices. Moreover, they would not be authorised to withhold documents from the material that had been taken away unless the tax subject accepted the measure. On the other hand, in *Stefanov v.*

Bulgaria, no. 73284/13, 16 November 2021, it was not informed of any legal requirements as regards the keeping of data or their destruction.

The European Court did not consider in *UAB Kesko Senukai Lithuania v. Lithuania*, no. 19162/19, 4 April 2023that Article 8 of the European Convention can be interpreted as requiring an *ex post facto* judicial review in all cases concerning an inspection carried out in the premises of a commercial company where prior authorisation for this had been given by a court. However, it did indicate that the availability of such review may be taken into account when assessing the compliance with that provision in a particular instance. In particular, the European Court considered such review particularly important where a large number of physical and electronic documents, including the entire mailboxes of five of the applicant company's employees had been seized or copied and the investigation had been discontinued so that the company could not raise its complaints concerning the impact of the action involved on commercial secrets or personal information unrelated to that investigation.

6. SURVEILLANCE MEASURES

As already noted, the European Court is concerned regarding such measures that the relevant provisions ensure both that there is *sufficient clarity as to the scope or manner* in which any discretion conferred may be exercised and that there are *sufficient safeguards against abuse*.

In order for this to be achieved, that the legislation authorising the interception of communications and the gathering of other data without consent must specify:

- the *categories of persons and communications or data affected*, which must be clearly defined, which they were not in *Iordachi and Others v. Moldova,* no. 25198/02, 10 February 2009, since it was unclear who – and under what circumstances – risked having the measure applied to them;
- the *offences for which the measure may be used*, which should be all or even the majority of them, unlike in the *Iordachi* case where interception warrants could be sought in respect of more than one half of offences in the Republic of Moldova;
- the *basis for applying such measures*, which should only be where these should be authorised only where there are very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity;
- the *maximum duration of any measure*, which should not be overly long, such as in *Volokhy v. Ukraine*, no. 23543/02, 2 November 2006, in which interception was not subject to any time-limit or any review at reasonable intervals and lasted for more than one year;
- the *procedure for examining, using and storing the data gathered*, unlike in the *Iordachi* case where the law did not require investigating judges to review whether requirements in the law concerning these matters had been complied with or provide for acquainting them with the results of the surveillance;
- the permitted use of and access to the material gathered, such as the provisions considered in *Roman Zakharov v. Russia* [GC], 47143/06, 4 December 2015, which stipulated that the data collected constituted a State secret and were to be sealed and stored under conditions excluding any risk of unauthorised access. Moreover, they could only be disclosed to those officials and prosecuting authorities who genuinely needed the data for the performance of their duties and who had the appropriate level of security clearance, with just the amount of information needed by the recipients to perform their duties being disclosed;
- the *circumstances in which the material will be destroyed or erased*, such as the requirement in the *Roman Zakharov* case that intercept material must be destroyed after six months of storage, if the person concerned has not been charged with a criminal offence and that the judge, after the completion of criminal proceedings makes a decision on its further storage or destruction. The European Court considered that time-limit to be reasonable in such cases. However, it also deplored in that case the lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained and held that the automatic storage for six months of clearly irrelevant data could not be considered justified under Article 8. In addition, the retention of data from surveillance without any external control and under rules

that were not accessible was found in *Haščák v. Slovakia*, no. 58359/12, 23 June 2022 to afford no protection against arbitrary interference with the right to respect for private life and was thus not "in accordance with the law". Also, the lack of sufficient clarity in the legal framework and the absence of procedural guarantees relating specifically to the destruction of the communications of a person who was not the subject of the surveillance operation concerned was held in *Kaczmarek v. Poland*, no. 16974/14, 22 February 2024 mean that the interference with her rights under Article 8 was similarly not "in accordance with the law";

- the *arrangements for record-keeping* (which found in *Shimovolos v. Russia*, no. 30194/09, 21 June 2011 not to be open to public scrutiny and knowledge) and independent supervision (this was by prosecutors under the legislation considered in the *Roman Zakharov* case but there was considered to be doubts about their independence both from the executive and their prosecutorial responsibilities and the scope and effectiveness of their supervision was limited);and
- a *remedy to ensure examination of the justification of surveillance* the dedicated remedy, which was found unsatisfactory in *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, 11 January 2022 as it was not available in practice in all possible scenarios, did not ensure examination of the justification of each instance of surveillance (by reference to reasonable suspicion and proportionality), was not open to legal persons, and was limited in terms of the relief available.

In addition, *prior judicial authorisation*:

- should generally be required for prior judicial authorisation where the surveillance involves criminal proceedings, with the scope of the review being capable of ensuring that the measures are not ordered haphazardly, irregularly or without due and proper consideration, which was not, e.g., the case in *Roman Zakharov v. Russia* [GC], 47143/06, 4 December 2015, in which the bar on materials containing information about undercover agents or police informers or about the organisation and tactics of operational-search measures being submitted to the judge and therefore being excluded from a court's scope of review meant that it was deprived of the power to assess whether there was a sufficient factual basis to suspect the person in respect of whom operational-search measures were requested of a criminal offence;
- is always required for any interception of communication undertaken to discover journalistic sources (as underlined in *Telegraaf Media Nederland Landelijke Media BV v. Netherlands,* no.39315/06, 22 November 2012, at paras. 89-102); **but**
- will not be insisted upon in genuinely urgent cases, with judicial authorisation being subsequently needed 48 or 72 hours after the commencement of the surveillance being seen as acceptable in respectively *Roman Zakharov v. Russia* [GC], 47143/06, 4 December 2015 and *Szabó and Vissy v. Hungary*, no. 37138/14, 12 January 2016.

Conversations and other communications with an accused person's lawyer should not generally be subject to surveillance since the European Court considers that the right to the assistance of a lawyer under Article 6(3)(c) would lose much of its usefulness if the lawyer concerned was unable to confer with his or her client and receive confidential instructions from him or her without such surveillance; *Khodorkovskiy and Lebedev v. Russia*, no. 11082/06, 25 July 2013, para. 627. Such surveillance could, however, be regarded as

compatible with these rights where the lawyer is a participant in the commission of an offence, as in *Versini-Campinchi and Crasnianski v. France,* no. 49176/11, 16 June 2016.

Moreover, even if the surveillance does not affect the fairness of criminal proceedings, the European Court found in *Canavci and Others v. Türkıye*, no. 24074/19, 14 November 2023 that the monitoring of the conversations of detained persons conversations with their lawyers in the context of legal assistance fell within the scope of private life since the purpose of such interaction was to allow individuals to make informed decisions about their life and such an interference could not be regarded as constituting an "insignificant" disadvantage for the purpose of Article 35(3)(b) of the European Convention.

Furthermore, whenever surveillance measures are undertaken, there should always *be effective protection for communications covered by legal professional privilege or professional secrecy*, such as clear rules defining what should happen when, for example, a phone call made by a client to his lawyer is intercepted, which were found to be lacking in *Iordachi and Others v. Moldova,* no. 25198/02, 10 February 2009 and, specifically relating to the destruction of the conversations concerned, in *Vasil Vasilev v. Bulgaria*, no. 7610/15, 16 November 2021.

Moreover, even where the foregoing safeguards do exist, a surveillance operation will certainly not be regarded as necessary in a democratic society unless it can be shown that:

- the *basis for undertaking it was substantiated*, which was the case in *Karabeyoğlu v. Turkey*, no. 30083/10, 7 June 2016 (in which the surveillance was based on suspicion after the discovery of evidence during a search) but not in *Kvasnica v. Slovakia*, no. 72094/01, 9 June 2009 (in which the measure had not been based on any specific suspicion against the applicant and had not been for any specific purpose) nor in *Potoczká and Adamčo v. Slovakia*, no. 7286/16, 12 January 2023 (in which the warrant contained no reasoning beyond a reference to the prosecution request and an offhand finding that, in view of that request, obtaining the necessary evidence by other means was ineffective or impossible);
- *other less intrusive means could not have been used* for the purpose of the investigation, which seemed to have been the case in *Matanović v. Croatia*, no. 2742/12, 4 April 2017 as no relevant reasoning had been provided in that case but just a formulaic statement to that effect in the authorisation;
- they *were effectively applied* in the particular circumstances of a case, as was not the case in *Bălteanu v. Romania*, no. 142/04, 16 July 2013, in which – despite the legal provisions governing supervision of surveillance measures, the courts did not offer a comprehensive answer to the applicant's repeated objections concerning the lawfulness of the authorisation given for such measures and the accuracy of the transcripts of the recordings made. Rather, they merely noted that the report made by the prosecutor concerning the recordings, together with the tapes, had been attached to the court file and they accepted without questioning the prosecutor's refusal to present the authorisation; and
- the particular use of an authorisation for surveillance *should not be disproportionate*, as was found to be the case in *Uzun v. Germany,* no. 35623/05, 2 September 2010, in which GPS surveillance had been carried out for a relatively short period of time (some three months) and had affected the applicant essentially only at weekends and when he was travelling in a particular car whereas it was not in *Sedletska v. Ukraine*, no. 42634/18, 1 April 2021, in which there had been (a) one authorisation to collect a wide range of a journalist's protected

communications data concerning her personal and professional contacts over a sixteen-month period, including the time and duration of her communications and the telephone numbers of her contacts which could possibly include identifiable information concerning her confidential sources which had no relevance to the criminal proceedings regarding the alleged misconduct of a suspect and (b) another authorisation allowing access to her posted geolocation data for the same period which could have been registered there on a number of occasions which had no relevance to the case under investigation and there remained considerable uncertainty that any information pertinent to the proceedings against the suspect.

(b) drugo ovlašćenje koje dozvoljava pristup njenim objavljenim podacima o geolokaciji za isti period koji su tamo mogli biti registrovani u više navrata, a koji nisu bili relevantni za predmet koji je bio pod istragom . Ostala je značajna neizvjesnost da li su bilo kakve informacije bile relevantne u vezi sa postupkom protiv osumnjičenog.

The use in criminal proceedings of video recordings made spontaneously and without any intervention or assistance by the authorities was found not to give rise to a violation of Article 8 in *Sarbu v. Romania*, no. 34467/15, 28 March 2023 where these had involved two one-off incidents, they had been found during a search and those proceedings had offered the applicant sufficient guarantees.

There is *no obligation to give advance warning* to anyone that might become subject to surveillance since this could seriously jeopardise the success of a surveillance operation by being liable to reveal the resources of those undertaking it and the scope of information had already been gathered; *Mersch and Others v. Luxembourg* (dec.), no. 10439/83, 10 May 1985.

However, the *notification of those who have been the subject of surveillance after its occurrence after the event is required* for the purpose of ensuring an effective remedy against any abuse of the powers concerned; *Roman Zakharov v. Russia* [GC], 47143/06, 4 December 2015, at para. 298. This applies not only to the parties to the criminal proceedings concerned but also to those individuals whose communications had been intercepted but had not been parties to the proceedings since they were not suspected or accused of involvement in an offence concerned. In the absence of such notification, the European Court held in *Contrada v. Italy (No. 4)*, no. 2507/19, 23 May 2024 that there would not be adequate and effective guarantees against abuse to such persons who had been subjected to an interception measure because they could not apply to a judicial authority for an effective review of the lawfulness and necessity of the measure and to obtain appropriate redress, as applicable.

Furthermore, the *collection and storage of the digital images of persons and their use to extract and process the biometric personal data of those persons with the aid of facial recognition technology* to (a) identify them from photographs and a video published on a messaging application and (b) to locate and arrest them was not considered to be necessary in a democratic society in *Glukhin v. Russia*, no. 11519/20, 4 July 2023 when this concerned proceedings in respect of a minor offence that consisted of holding a solo demonstration without a prior notification that was entirely peaceful.

In addition, the European Court doubted in *Glukhin* that the legal provision involved met the *quality of law requirement* as it:

(I) was *widely formulated* without any instances of restrictive interpretation and application;

(II) *allowed the processing of biometric personal data* – including with the aid of facial recognition technology – in connection with any judicial proceedings;

(III) had *no limitations* on the nature of situations which might give rise to the use of such technology, the intended purposes, the categories of people who might be targeted, or on the processing of sensitive personal data; and

(IV) there did not appear to be any *procedural safeguards* such as ones regarding authorisation, examination, use and storage of the data obtained, supervisory control mechanisms and remedies, i.e., the requirements generally applicable to surveillance measures.

6.1. SUBSEQUENT USE

The European Court did not consider it material in *Škoberne v. Slovenia*, no. 19920/20, 15 February 2024 that, for the purpose of finding a violation of Article 8, only very limited use had been made in subsequent criminal proceedings of all the data that had been acquired by law-enforcement authorities and then processed, kept and examined by them.

However, in *Aydin Sefa Akay v. Türkıye*, no. 59/17, 23 April 2024, the European Court did say that it could not disregard the fact that the search of the house of a person enjoying diplomatic immunity had yielded certain materials, such as computers and mobile phones, which were later used in the criminal proceedings against, forming part of the bill of indictment. In that case, the applicant was an international judge and the European Court emphasised that his house was subject to a heightened protection, similar to the protection afforded to searches of a lawyer's office in the Court's case law under Article 8.

6.2. SELF-INCRIMINATION

A requirement to provide information or material should not be imposed where this would breach the right not to incriminate oneself, which the European Court considers to "lie at the heart of the notion of a fair procedure under Article 6", even though it is not specifically mentioned in it; *Saunders v. United Kingdom* [GC], no. 19187/91, 17 December 1996, at para. 68.

Persons will be regarded as incriminating themselves not only where the statement or document concerned involves *an admission of wrongdoing or is otherwise directly incriminating* but also where it is *exculpatory or provides information which can then be later deployed* in criminal proceedings in support of the prosecution cases, e.g., to contradict or cast doubt upon other statements of the accused or evidence given by him or her during the trial or to undermine his or her credibility in some other way; *Ibrahim and Others v. United Kingdom* [GC], no. 50541/08, 13 September 2016, at para. 268.

Moreover, the right not to incriminate oneself *will not be extinguished by the public interest* in tackling complex frauds (as had been claimed in *Saunders v. United Kingdom* [GC], no. 19187/91, 17 December 1996), addressing security and public order concerns (as had been claimed in *Heaney and McGuinness v. Ireland*, no. 34720/91, 21 December 2000) or seeking to recover debt (as had been claimed in *Marttinen v. Finland*, no. 19235/03, 21 April 2009).

The right not to incriminate oneself will be *breached by any requirement to hand over evidence, or to provide information that is backed by criminal penalties for non-compliance* with it, such as:

- *accumulation of liability* in *Funke v. F*rance, no. 10828/84, 25 February 1993 to pay fines for refusing to produce statements for bank accounts held by the applicant outside the country;

- *imprisonmen*t in *Heaney and McGuinness v. Ireland*, no. 34720/91, 21 December 2000 for failure to provide information about the applicants' whereabouts at a particular time;

- *accumulation of liability* in *J.B. v. Switzerland*, no. 31827/96, 3 May 2001 to pay fines for refusing to submit documents which would have provided information as to the applicant's income with a view to the assessment of his taxes in connection with tax-evasion proceedings instituted against him; and

- imprisonment or fine in *Shannon v. United Kingdom*, no. 6563/03, 4 October 2005 for failure to attend to give information to financial investigators seeking to trace the proceeds of crime in connection with events in respect of which the applicant had already been charged with offences.

7. PRE-TRIAL DETENTION

Electronic evidence has been invoked for the purpose of establishing the existence of the *reasonable suspicion* of an offence having been committed that is required whenever a decision is taken to detain persons before any trial. This sets a *threshold* that cannot be assumed to have been met. Access to it and its availability have also been material when determining whether certain *procedural guarantees* relating to a deprivation of liberty had been observed.

7.1. REASONABLE SUSPICION

Article 5(1)(c) of the European Convention requires that there be a reasonable suspicion of persons having committed an offence when they are arrested or detained for the purpose of bringing them before the competent legal authority.

A suspicion will - as the European Court has made clear on many occasions - be "reasonable" where there exist *facts or information which would satisfy an objective observer* that the persons concerned may have committed the offence, having regard to all the circumstances; see, e.g., *Ilgar Mammadov v. Azerbaijan*, no. 15172/13, 22 May 2014, at paras. 87-88.

However, it has also emphasised that that evidence *does not have to be sufficient to enable charges to be brought or to justify a conviction* as the purpose of questioning during detention under Article 5(1)(c) is to further the criminal investigation by confirming or dispelling the concrete suspicion grounding the arrest; *Murray v. United Kingdom* [GC], no. 14310/88, 28 October 1994, at para. 55.

Such a reasonable suspicion is also required if the imposition of any preventive measure involving deprivation of liberty (i.e., remand in custody/pre-trial detention) is to be compatible with Article 5(3) and that is also the case for the imposition of any less exacting form of preventive measure, as well as where the imposition of any of these measures is continued after their initial imposition.

However, *the longer any pre-trial detention is continued, so more exacting will become the evidence required to demonstrate that such a reasonable suspicion still exists*; *Labita v. Italy* [GC], no. 26772/95, 6 April 2000.

The European Court noted in *Svetina v. Slovenia*, no. 38059/13, 22 May 2018, at para. 50 , without expressing any concern, the possible role played by unlawfully obtained data from a person's mobile telephone in the initial stage of proceedings that led to his arrest. However, its focus in that case was only on the fairness of his conviction and the unlawfully obtained data had not been used to secure that.

7.2. MEETING THE THRESHOLD

So far, the substance of the electronic evidence invoked – involving messaging applications, recordings of telephone conversations and social media posts - has not been regarded as sufficiently strong to satisfy the threshold set by the foregoing considerations.

Thus, there has been just one case, *Ahmet Hüsrev Altan v. Turkey*, no. 13252/17, 13 April 2021, in which the European Court acknowledged that the mentioning of a person's name as amongst those involved in an illegal organisation – which occurred in a transcript of a conversation on a messaging application – *could potentially be capable of giving rise to suspicions* justifying the continued detention of that person. However, this could not amount to a determining factor in that case as it appeared that this evidence had not been specifically taken into consideration when the relevant decisions concerning that person's detention were actually delivered.

On the other hand, there have been a number of instances in which the evidential standard required for the purposes of for the purpose of Article 5(1)(c) has *definitely not been met*.

Thus, in two cases - *Sabuncu and Others v. Turkey*, no. 23199/17, 10 November 2020 and *Şik v. Turkey (No. 2)*, no. 36493/17, 24 November 2020 - the content of posts on social media were considered by the European Court to fall within the legitimate bounds of freedom of suspicion and could not amount to anything other than a mere suspicion that the persons concerned had committed the offences of disseminating propaganda on behalf of terrorist organisations or assisting those organisations.

Moreover, in another case - *Selahattin Demirtaş v. Turkey (no. 2)* [GC], no. 14305/17, 22 December 2020 – the records of intercepted telephone conversations were viewed by the European Court as not capable of constituting a fact justifying a suspicion that the applicant was in charge of the political wing of an illegal organisation. This was especially so as regards the purported giving in those conversations of instructions to take part in a programme organised within the Council of Europe many years before his pre-trial detention.

Also, the European Court found a deprivation of liberty unlawful in *Mehmet Hasan Altan v. Turkey*, 13237/17, 20 March 2018, thereby effectively endorsing the view of the Turkish Constitutional Court that the contents of the messages exchanged by suspected members of an illegal organisation via a messaging application could not in themselves be regarded as significant indications that someone else had committed that offence. In view of that finding, the European Court did not consider it necessary to rule on the applicant's complaint of a lack of a reasonable suspicion that he had committed an offence.

In *Baş v. Turkey*, no. 66448/17, 3 March 2020, which concerned the same messaging application, the European Court did not find it necessary to address the ruling of the Turkish Constitutional Court that its use or the installation of it with a view to using it should have been treated by the investigating authorities as evidence of a link to the illegal organisation concerned since there had been no explanation as to how such evidence obtained several months after the applicant's initial pre-trial detention could have formed a basis for a reasonable suspicion that he had committed the offence of which he was accused.[7]

---

7 Similarly, in *Başer and Özçelik v. Türkiye*, no. 30694/15, 13 September 2022, the initial detention of the applicants could not be justified by reference to a document on a USB stick found during a search as that evidence had not been adduced until long afterwards.

However, the European Court has subsequently emphasised in *Akgün v. Turkey,* no. 19699/18, 20 July 2021 that, as a matter of principle, *the mere fact of downloading or using a means of encrypted communication* (or indeed the use of any other method of safeguarding the private nature of exchanged messages) could not in itself amount to evidence capable of satisfying an objective observer that an illegal or criminal activity was being engaged in.

As a result, it will only be when the use of an encrypted communication tool is supported by other evidence about that use - e.g., the content of the exchanged messages or the context of such exchanges – that the European Court considers that it would then be possible to speak of evidence that could satisfy an objective observer that there were reasonable grounds to suspect the individual using that communication tool of being a member of a criminal organisation.

This approach is consistent with the acceptance by the European Court in *Engels v. Russia*, no. 61919/16, 23 June 2020, at para. 30 that information technologies are *a means of storing and accessing content and cannot be equated with content itself*, whatever its legal status happens to be.

Furthermore, in the *Akgün case,* the European Court also underlined that the information submitted about such use had to be *sufficiently precise* to allow it to be concluded that the messaging system in question had in reality been intended for use only by members of a criminal organisation.

However, this requirement was found not to be met in that case. In particular, the European Court considered that the document concluding that the applicant had used a particular secure messaging application had not specified and had not set out any illegal activity on his part since it had not identified either the dates of this presumed activity or its frequency, and had not contained any additional details. Furthermore, the European Court pointed out that neither this document nor the pre-trial detention order had explained how this presumed activity by the applicant would indicate his membership of a terrorist organisation.

Electronic evidence might also be important in *disproving the existence of a reasonable suspicion*, as can be seen in *Ayyubadze v. Azerbaijan*, no. 6180/15, 2 March 2023. This concerned the applicant's apprehension for supposedly committing the offence of resistance to or violence against a public official. However, in concluding that there was no reasonable suspicion of him having committed this offence, the European Court noted that the prosecution had accepted without question the assertion that there were no memory storage systems on the surveillance cameras which might have supported the applicant's version of the events in question.

Moreover, whenever the authenticity of electronic evidence is relied upon to extend a person's pre-trial detention, the judicial authorities will then be under *an obligation to demonstrate its credibility*. This was emphasised by the European Court in *Selahattin Demirtaş v. Turkey (no. 2)* [GC], no. 14305/17, 22 December 2020, in which it noted that the domestic courts did not appear to have sought to verify the authenticity of the records of the intercepted telephone conversations presented to them by the public prosecutor, even though it found them insufficient on the assumption that they were trustworthy.

7.3. PROCEDURAL GUARANTEES

It is well-established that *equality of arms* is required where the lawfulness of detention at the pre-trial stage is challenged pursuant to Article 5(4) of the European Convention.

7.3.1 Access to evidence

Equality of arms will not, however, be ensured if *access is denied to those documents in the investigation file* which are essential for this purpose. Although the need for criminal investigations to be conducted efficiently may mean that part of that information may be kept secret in order to prevent suspects from tampering with evidence and undermining the course of justice, this goal cannot be pursued at the expense of substantial restrictions on the rights of the defence.

The requirement of such access applies equally to electronic evidence.

Thus, in *Akgün v. Turkey*, no. 19699/18, 20 July 2021, there was found to be a violation of Article 5(4) where the applicant had not, throughout his pre-trial detention been provided to him about his name appearing on the red list of users of a particular messaging application. As this was the single item of evidence on which the order for his pre-trial detention had been based, neither the applicant nor his lawyer had had sufficient knowledge of the substance of this evidence, available exclusively to the prosecution, which had been of crucial importance for challenging his detention

Nonetheless, there will not be a violation of Article 5(4) if it cannot be demonstrated both that this evidence was relevant for calling into question the basis for a suspect's deprivation of liberty and that access had actually been denied for the purpose of challenging its lawfulness.

This was found to be the situation in *Falk v. Germany* (dec.), no. 41077/04, 11 March 2008. Thus, in the first place, the material presented by the applicant's counsel to challenge an arrest warrant after having full access to certain confiscated data stored on CD-ROMs, a server and a computer hard drive was considered did not contain any elements calling into question the suspicion against the applicant. Secondly, the applicant was considered to have failed to demonstrate that any such material to which access had been delayed because of a defect in the hard drive would have called into question the suspicion against him if he had received it earlier and would thus have played a role in his challenge to the arrest warrant

7.3.2 Providing reasons

Moreover, the European Court has accepted in *Ugulava v. Georgia*, no. 5432/15, 9 February 2023 that, where national law required written reasons for imposing or continuing pre-trial detention, the availability of, and access to, an audio recording in which a person's application for release was rejected could compensate for the lack of a written decision where the grounds which, in the eyes of the court judge, justified the imposition of pre-trial detention were clearly discernible. This was because the applicant and his lawyers could, in proceedings to seek his release, have access to and use that recording in proceedings.

8. BASIS FOR A CONVICTION

This chapter considers first the general requirements arising from the right to a fair trial Article 6(1) of the European Convention to the use of evidence to support a conviction before considering specific aspects relating to its probative value, admissibility, disclosure and examination of witnesses, as well as the use of electronic evidence acquisition to address deficiencies relating to other evidence or show that such evidence has not been improperly gathered.

8.1. EVIDENCE IN GENERAL

A *failure to properly assess the probative value of evidence relied upon* will give rise to a violation of Article 6(1) of the European Convention.

However, this provision, although guaranteeing the right to a fair trial, does not lay down any rules on the admissibility of evidence. As the European Court reiterated in *Yüksel Yalçınkaya v. Türkiye* [GC], no. 15669/20, 26 September 2023, at para, 302, this is primarily a matter for regulation by national law and the national courts.

As a result, *the consistent approach of the European Court as to whether particular types of evidence may be admissible, and thus provide some or the sole basis for a conviction, is for it to be concerned only with whether the proceedings as a whole were fair and thus compatible with the guarantee of a fair trial*.

The admission into evidence of *statements obtained as a result of torture or of other ill-treatment* in breach of Article 3 of the European Court for the purpose of establishing the relevant facts in criminal proceedings *will automatically render the proceedings as a whole unfair*. This is irrespective of the probative value of the statements and irrespective of whether their use was decisive in securing a person's conviction.

However, as regards the admissibility of any evidence which has not been so obtained, the European Court's focus will thus be on whether the rights of the defence have been respected and, in particular, on factors such as:

a. any *unlawfulness* in the way in which particular evidence might have been obtained;
a. the *quality* of the evidence, including whether the circumstances in which it was obtained cast doubts on its *reliability or accuracy*;
b. the *opportunity to challenge* the authenticity and reliability of the evidence and to oppose its use;
c. the *opportunity to examine* any relevant witnesses; and
d. the v*oluntariness of any admissions* made by the defendant.

The issue of fairness will not necessarily arise where evidence, the admissibility of which is contested, is *unsupported by other material*. In such cases, the European Court has repeatedly emphasised that, where the evidence is very strong and there is no risk of its being unreliable, the need for supporting evidence is correspondingly weaker; see, e.g., *Bosak and Others v. Croatia*, no. 40429/14, 6 June 2019, at para. 83.

Nonetheless, this does not mean that the European Court will not emphasise the existence of other supporting evidence where it has not found unjustified a rejection of a challenge to certain evidence that is decisive. For example, in *Fejzulla and Mazreku v. "the former Yugoslav Republic of Macedonia"* (dec.), no. 23065/07, 31 May 2011, it pointed to the existence of corroborative evidence against the accused other than the video that had been impugned.

The need to assess the probative value of evidence and to address the different factors that may make reliance on it unfair applies to electronic as much as any other form of evidence. Failings in this respect have thus led the European Court to find a violation of Article 6(1) in a number of cases.

8.2. PROBATIVE VALUE

Although the potential probative value of electronic evidence in particular instances has already been noted, this does not mean that it is always *capable of establishing anything material to the issues to be determined in particular proceedings or of even contributing to so doing*.

The defence should thus be able to challenge the probative value of any electronic evidence being invoked in support of a conviction, even if its admissibility is not contested. See, e.g., *Shuvalov v. Estonia* (dec.), no. 39820/08, 30 March 2010, in which the playing of audio recordings in the court gave the defence the opportunity to argue that the offence had been committed as a result of incitement

Moreover, it is essential that a court make a *proper assessment of the probative value of any electronic evidence* adduced in support of a prosecution. This cannot be assumed from the fact of a conviction being rendered in a particular case but must be demonstrated in the reasoning that led to it.

This was not the situation found in *Ilgar Mammadov v. Azerbaijan (No. 2)*, no. 919/15, 16 November 2017 with respect to view taken by the national courts that certain posts made on a blog and social media demonstrated an intent to organise mass disorder. This was entirely inconsistent with the full content of the posts, which merely conveyed what the applicant had seen and heard, offering an interpretation of events from his own perspective, with nothing in them to suggest that he had overstepped the limits of protected political speech on a question of significant public interest.

Similarly, there was no adequate explanation in *Üçdağ v. Turkey,* no. 23314/19, 31 August 2021 as to the reasons why the sharing of a social media post of two photographs had to be interpreted as praising, condoning and encouraging the methods entailing coercion, violence and threats used by a terrorist organisation.

Moreover, in *Yüksel Yalçınkaya v. Türkiye* [GC], no. 15669/20, 26 September 2023, the European Court noted the lack of any meaningful discussion in the relevant judgments as to how the use of a bank account – a seemingly lawful act that benefited from the presumption of legality - could be evidence of criminal conduct, even in an ancillary manner. As a result, it considered that there should have been clarification as to how this had reinforced their finding regarding the applicant's membership of an armed terrorist organisation, noting in particular that the explanation provided by him to account for his banking transactions was never verified or otherwise addressed by the courts.

Furthermore, making a proper assessment will also *necessitate showing that full account has been taken of any submissions by the defence regarding the conclusions to be drawn from any electronic evidence which it had adduced*.

This did not occur in *Ilgar Mammadov v. Azerbaijan (No. 2)*, no. 919/15, 16 November 2017 since an appeal court had essentially ignored the fact that the images on a video did not show any clashes between protestors and the police, contradicting the specific factual claims made against the applicant, and had created what was a purely hypothetical version of the events which had never been argued by the prosecution and which was unsupported by any existing evidence. In dismissing the evidence favourable to the applicant in such a manner, the European Court considered that the domestic court had placed an extreme and unattainable burden of proof on the applicant, contrary to the basic requirement that the prosecution has to prove its case and one of the fundamental principles of criminal law, namely, *in dubio pro reo.* As such its assessment of the evidence was manifestly unreasonable and contributed to the conclusion that the criminal proceedings against the applicant did not comply with guarantees of a fair trial.

It was also notable in that case that a first instance court had relied upon a different video showing clashes between protestors and the police, ignoring the defence's submission that this concerned events when the applicant was not even present in the town concerned.

Similarly, in *Yüksel Yalçınkaya v. Türkiye* [GC], no. 15669/20, 26 September 2023, it was considered it primordial for the courts to have addressed the applicant's objections regarding the veracity of allegations as to the exclusive use of the messaging application by the members of the illegal terrorist organisation or as to his use of it for "organisational" purposes. In this regard, such use by him was not supported by specific findings of fact but subsumed with the exclusivity argument, supported mainly by the technical features of the application – such as its encrypted nature, the special arrangements required to enter into communication with other users, the requirement to use a VPN and the automatic deletion of content, as well as the decrypted user profiles and content, notwithstanding that it had been possible to download the application for approximately two years without any control mechanism , the number of times this had occurred and the technical features being common to other applications. Moreover, the findings regarding the allegedly exclusive and organisational nature of the messaging application had been made primarily in an extrajudicial context by the national intelligence agency and had not been thoroughly scrutinised by the courts.

Reliance on a lost video of the special operation concerning an accused's apprehension in finding him guilty of requesting a bribe, notwithstanding that the crucial moment – the passing of the money - had not been filmed anyway was held in *Dan v. Republic of Moldova (No. 2*), no. 57575/14, 10 November 2020 to have *exacerbated the deficiencies in the overall assessment* of the evidence in the case.

8.3. ADMISSIBILITY

The issues relevant to admissibility of electronic evidence in a manner consistent to the right to a fair trial concern any possible use of ill-treatment, its unlawful acquisition, its quality and reliability, the ability to challenge and oppose its use and its voluntariness.

8.3.1 Ill-treatment

Although the use of ill-treatment contrary to Article 3 of the European Convention might not generally be associated with reliance on electronic evidence, it was a situation that had to be considered by the European Court in *Ćwik v. Poland*, no. 31454/10, 5 November 2020.

In that case, the transcript of recorded utterances by a person had been relied on by the prosecution in the trial of the applicant. This transcript had been admitted in evidence by the e trial court, which then referred to it in making the factual findings and determining the applicant's guilt. The utterances had been recorded while the person concerned was being subjected to ill-treatment contrary to Article 3 by the members of an organised criminal group.

The fact that the *ill-treatment was inflicted by private individuals rather than public officials* made no difference to the conclusion that the admission of the impugned transcript had automatically rendered the proceedings as a whole unfair, in breach of Article 6(1).[8]

8.3.2 Unlawfulness

The European Court has not found reliance on electronic evidence for the purpose of a conviction where that evidence was gathered *without a basis for doing so under national law* should then lead to the trial being considered unfair in cases concerned with:

- the recording of telephone conversations (*Schenk v. Switzerland*, no. 10862/84, 12 July 1988);
- the use of listening devices to record conversations (*Khan v. United Kingdom*, no. 35394/97, 12 May 2000 and *P.G. and J.H. v. United Kingdom*, no. 44787/98, 25 September 2001);
- the making of a video-recording (*Perry v. United Kingdom* (dec.), no. 63737/00, 26 September 2002).

Although there was no legal provision authorising the gathering of evidence in these ways, only in *Schenk* was there a specific legal prohibition on doing so. However, the gathering of evidence in this way was contrary in all the other cases to official practice or guidelines.

Nonetheless, in the *Khan* and *P.G. and J.H.* cases, there was some emphasis on the fact that – unlike in the *Schenk* case - the recordings were *not unlawful in the sense of being contrary to the criminal law*. It is possible that this might prove to be relevant for an assessment in the future by the European Court of the fairness of relying on electronic evidence where the means used to gather it did amount to a criminal offence.

In assessing the fairness of reliance on the evidence, the importance of there being an *opportunity of challenging its authenticity or reliability* was emphasised in all the cases other than *Khan*, in which this was not contested. In all of them, there was also the possibility of

8 There was a dissent in this regard by Judges Wojtyczek and Pejchal.

opposing the use of the evidence, albeit that this was unsuccessful.

In the *Perry* case, it was also possible to challenge the quality of the video-recording.

In both the *Schenk* and *P.G. and J.H.* cases, some emphasis was also placed on the fact that some reliance had been placed on other evidence but this was not seen as important in *Khan* given that the recording was acknowledged to be very strong evidence and there was no risk of it being unreliable.

In *Škoberne v. Slovenia*, no. 19920/20, 15 February 2024, the European Court reiterated its long-standing position that the admission and use in judicial proceedings of evidence obtained in breach of Article 8 does not necessarily lead to the finding of a violation of Article 6.

Indeed, the European Court has not so far considered unfair any trial in which reliance on evidence gathered in a manner contrary to the requirements of Article 8 had led to a conviction.

Thus, although it found in *Dumitru Popescu v. Romania (No. 2)*, no. 71525/01, 26 April 2007 that the safeguards required under Article 8 for the recording of telephone conversations had not been met, it only addressed the issue of the fairness of the trial from the perspective of the alleged failure to comply with the requirements of the national law concerned. In this regard, it simply noted that the applicant had never denied the content of the disputed recordings or contested their authenticity, whether before the national courts or even before it. Furthermore, it considered it appropriate, as in the *Schenk* case, to attach weight to the fact that the disputed recordings did not constitute the only means of proof.

8.3.3 Quality and reliability

Electronic evidence ought to be regarded as deficient for the purpose of proving anything, for example, where:

- it is of *poor quality or incomplete*, such as
  - the nature of the audio recording invoked in *Mikhaylova v. Ukraine,* no. 10644/08, 6 March 2018. Apart from these deficiencies, the applicant – who had sought to rely on the recording to support her allegations about the judge's conduct in a trial – had failed to provide a transcript of the recording or even of the parts that she purported to rely on. Moreover, she had failed to explain under what conditions the recording had been made and its legal status under domestic law. As a result, the European Court declined to take it into account;

- there has been some *editing or manipulation* of its content, such as
  - where the expert report considered in *Botea v. Romania*, no. 40872/04, 10 December 2013 had found the audio tapes adduced as evidence were not original and could be copies, mixings done with or without the intent to present a false reality, or fabricated and had pointed out that voice identification could only be carried out on original recordings using the same equipment as that used for the recording;
  - the editing of recordings that was alleged in *Taraneks v. Latvia*, no. 3082/06, 2 December 2014 but was disproved by an expert report;
  - the manipulation was actually found to have occurred in *Batiashvili v. Georgia*, no. 8284/07, 10 October 2019 with respect to an audio recording in order to create a suspicion in respect of the applicant;

- there is *a lack of clarity as to its provenance*, such as:
  - where the circumstances in which an audio recording was found were unclear and

there was no explanation as to the purpose of making it or those responsible for doing so, as in *Adzhigitova and Others v. Russia,* no. 40165/07, 22 June 2021. This led the European Court to conclude that an audio recording of unknown men did not seem to constitute sufficiently credible evidence as to overturn the presumption of an abduction having taken place;

- there are *other shortcomings affecting the way it was gathered*, such as
- the allegation that was not substantiated in *Khodorkovskiy and Lebedev v. Russia,* no. 11082/06, 25 July 2013 regarding both possible discrepancies in the documents describing the amount of data contained on certain hard drives and inaccuracies as to the exact location of the computer servers concerned;
- the serious doubt that was considered in *Ayetullah Ay v. Turkey*, no. 29084/07, 27 October 2020 to have been thrown on the reliability and accuracy of evidence allegedly found during a search where (a) it had been carried out in disregard of a statutory procedural safeguard – the presence of two independent witnesses -which was particularly important where the accused alleged that it had been planted and (b) that evidence had not been mentioned as having been seized in the search-and-seizure record submitted to a court afterwards but was cited in another record of the search.

Moreover, the European Court underlined in *Yüksel Yalçınkaya v. Türkiye* [GC], no. 15669/20, 26 September 2023 that in cases where the collection or processing of intelligence information is *not subject to prior independent authorisation or supervision, or a post factum judicial review*, or where it is not accompanied by other procedural safeguards or corroborated by other evidence, its reliability may be more likely to be called into question.

This case was concerned with whether the applicant had used a particular encrypted messaging application considered to be used by members of an armed terrorist organisation. The fact that in that case the domestic courts had not engaged in any assessment of the forensic precautions to ensure the integrity and reliability of the relevant data relied upon to show that he had used that application meant that the European Court was not itself in a position to assess whether the measures concerned – namely, obtaining the raw data from the application's server as a file automatically created by an open-source relational database management system without any human intervention, which was copied by two appointed experts in accordance with the digital forensics standards, in the presence of a judge and recorded by camera, with the retrieval of the raw data limited to rendering it intelligible in order to be able to extract meaningful information from them - presented sufficient guarantees of integrity and reliability.

On the other hand, objections in the *Yüksel Yalçınkaya* case to the lawfulness, accuracy and reliability of certain other complementary means of verifying the applicant's use of the application were not seen as decisive since (a) being outside a statutory time limit did not have a bearing on technical accuracy and (b) the applicant did not advance any claims of manipulation or any tangible ones of personal data indicating the connection from his telephone to the application's IP addresses.

Nonetheless, as the circumstances in which the data concerning the application had been retrieved did *prima facie* raise doubts as to their "quality" in the absence of specific procedural safeguards geared to ensuring their integrity until the handover to the judicial authorities, it then became important to consider whether the applicant had a genuine opportunity to challenge the evidence against him and conduct his defence in an effective manner and on an equal footing with the prosecution

8.3.4 Challenging and opposing use

Whenever the prosecution seeks to rely on electronic evidence, there should always be **an opportunity both to challenge its authenticity and reliability and to oppose its use**.

Certainly, as in some cases the reliability or accuracy of electronic evidence may not be contested (e.g., *Pejkić v. Croatia*, no. 49922/16, 17 January 2023), there may still be reasons why the accused may want to argue that it should not be used in the proceedings against them on account of its unlawfulness or for other reasons.

Thus, the *existence of fair procedures for both purposes* will normally be seen by the European Court as of fundamental importance when assessing the overall fairness of a trial.

However, a failure by the court to address the admissibility of certain electronic evidence or the probative value of other such evidence may not, however, always be sufficient for the European Court to conclude that the overall fairness of the proceedings had been undermined.

This will certainly be so where there was *other compelling evidence of the accused's guilt* that it would be difficult to imagine that, even if those issues had been addressed, the conclusion of the court would have been different.

Such a situation can be seen in *Victor Savitchi v. Moldova*, no. 81/04, 17 June 2008, in which there was a failure by the courts in the prosecution of a police officer for bribery to address submissions by the defence concerning the admissibility of certain audio recordings, as well as the probative value of one of the recordings and of one of two videos of the *flagrante delicto*. However, the finding of his guilt was based on:

- The officer's involvement in the investigation of a case involving one of two persons from whom the bribe was requested;
- The testimony of the two bribers that the officer had requested the bribe; and
- The other video of the *flagrante delicto* clearly showing the officer dipping his fingers in a mug of beer, apparently attempting both to wash away traces of the powder used to mark the banknotes handed over to him and to expel from his shirt pocket the banknotes which had been powder-marked, with the contested video also clearly showing that, during the officer's arrest, his shirt pocket had not been checked.

Moreover, where such procedures exist but have not been used, a complaint to the European Court that the proceedings leading to a conviction were unfair on account of the reliance on evidence that lacked the integrity, reliability and authenticity or should not otherwise have been relied upon will be dismissed for having failed to exhaust domestic remedies as required by Article 35(1) of the European Convention, as occurred, e.g., in *Knaggs and Khachik v. United Kingdom* (dec.), no. 46559/06, 30 August 2011.

However, *a failure to disclose certain electronic evidence or the existence of limits on access to it* – which is considered further below - may affect the ability to challenge the integrity of particular evidence, as was recognised in *Yüksel Yalçınkaya v. Türkiye* [GC], no. 15669/20, 26 September 2023.

It will be important that there is not just an opportunity to challenge the authenticity of particular electronic evidence but that

(a) *submissions with substantiated argumentation* concerning that issue are actual-

ly examined, which did not seem to occur in *Ilgar Mammadov v. Azerbaijan (No. 2)*, no. 919/15, 16 November 2017, at para. 236, since the domestic courts had remained entirely silent about the allegations that the prosecution had tampered with certain video evidence. On the other hand, in *Bosak and Others v. Croatia*, no. 40429/14, 6 June 2019, at para. 81, all the defence's doubts as to the accuracy of certain audio recordings were duly examined and addressed by the trial court and also examined and confirmed by the Supreme Court, which considered that all the relevant circumstances of the case had been properly established by the trial court

(b) those submissions are *only dismissed by a reasoned decision*, as occurred in *Fejzulla and Mazreku v. "the former Yugoslav Republic of Macedonia"* (dec.), no. 23065/07, 31 May 2011.

Reliance on electronic evidence despite there being doubts about its integrity and authenticity which are not resolved will undoubtedly lead the European Court to conclude that the proceedings did not comply with the requirements of a fair trial. This was the situation in *Nițulescu v. Romania*, no. 16184/06, 22 September 2015, in which there could not be an expert examination of recordings of conversations, where important parts of them were claimed to be missing, because neither the tapes nor the equipment used to make the recordings were submitted to the court. These failings were compounded by the person who had made the recordings herself challenging the integrity of the transcripts and the reliance of the courts on written statements of persons who had not actually been present at one of the conversations concerned.

In some cases, *the court may be able to resolve a challenge to the authenticity or reliability of electronic evidence through its own examination of it or through a simple test*, such as was used in *Fejzulla and Mazreku v. "the former Yugoslav Republic of Macedonia"* (dec.), no. 23065/07, 31 May 2011. In that case, there had been a challenge to the authenticity of the VHS reproduction of the original video material recorded by digital cameras of events in a car park where drugs had been loaded into a truck. The European Court did not find fault with the trial court's refusal of the accused's request to admit the original video material, finding no grounds to suspect the authenticity of the reproduction. In this connection the European Court noted that the length of the video material recorded on the VHS tape and admitted at trial corresponded to the length of the original video material recorded by the digital cameras.

Moreover, doubts as to the content of recorded conversations might also be resolved where the defendant has had *an ample opportunity in the course of the trial to question and cross-examine* those persons with whom they had been held, as occurred in *Taraneks v. Latvia*, no. 3082/06, 2 December 2014.

Nonetheless, resolving a challenge may necessitate *being able to obtain expert examination* of the electronic evidence adduced in a case.

This will be, particularly so where, e.g., reliance is placed only on transcripts that are alleged not to cover this in its entirety, as was the situation in *Văduva v. Romania*, no. 27781/06, 25 February 2014, in which it was alleged that the prosecutor had (a) failed to present all the transcripts of certain recorded conversations in court and so concealed the fact that the applicant had been incited to sell drugs and (b) refused to allow an expert examination of the tapes concerned. These considerations led the European Court to conclude that there had been a failure to ensure, in practice, adequate safeguards to counterbalance any difficulties caused to the defence by the limitation on its rights, notably, the inability

to question certain witnesses on whose reports and statements on which the applicant's conviction had been based to a significant extent.

Where it is submitted that the assessment of electronic evidence requires the assistance of experts (such as for voice identification in respect of recordings or to establish whether it is authentic), there should be not be an unreasoned or arbitrary refusal to undertake such an assessment, such as in:

- *Groza v. Romania*, no. 12889/19, 21 December 2021, where this was the consequence of the court refusing to order a social media company to disclose information about the circumstances surrounding an account, which was required so that an expert could determine that it was a fake one created in the name of the applicant. The reasons for rejecting the request for a court order appear to secure this information merely contradicted the essence of the reasons behind a previous decision to allow the expert to repeatedly request it from the company in the first place and to ignore points raised by the applicant with a decisive implication for the case; and

- *Beraru v. Romania*, no. 40107/0418 March 2014, in which the domestic courts had based their decision on recordings of contested authenticity and the first instance court had changed its initial position concerning the necessity of a technical report in order to establish the authenticity of the recordings, considering this to be superfluous despite a technical report by a national forensic institute stating that there were doubts about the authenticity of the recordings.

Nor should there be a failure to respond to a request for an independent examination – even if only to explain why such independent examination was not deemed necessary – as was considered problematic in *Yüksel Yalçınkaya v. Türkiye* [GC], no. 15669/20, 26 September 2023, given in particular the absence of any concrete information in the case file to suggest that the data in question had at any point been subjected to examination for verification of their integrity, whether at the time of their submission to the judicial authorities or subsequently. This was important, in view of the crus of the applicant's concern being as to whether the data's integrity had been kept intact before the handover rather than afterwards. In addition, certain other concerns about securing the integrity of the data were not addressed.

Moreover, where a technical report casts doubt on the authenticity or reliability of electronic evidence, it should not be simply ignored as occurred in *Botea v. Romania*, no. 40872/04, 10 December 2013.

In that case, despite the importance of certain audio recordings – which were, if not the sole, at least the decisive evidence against the applicant, without which securing his conviction would either not have been possible or the possibility would have been remote – the court changed its initial position concerning the necessity of a technical report in order to establish the authenticity of the recordings. Moreover, despite receiving a technical report stating that there were doubts about the authenticity of the recordings before the delivery of its judgment, the court relied on the transcripts instead of re-opening the proceedings in order to allow the parties to submit their observations on the report. In addition, it did not reply to the applicant's submissions that he had not been presented with the transcripts and was thus unaware of their content. Also, the court neither played the audio tapes at the hearings in the presence of the accused nor provided any answer to his repeated complaints concerning the unlawfulness of the recordings.

Indeed, whenever there is doubt about the reality or reliability of electronic evidence, there should be a clear and effective possibility of having it assessed by a public or private centre independent of the one which gathered it.

This was not the situation in *Dumitru Popescu v. Romania (No. 2)*, no. 71525/01, 26 April 2007, in which the independence of the Romanian intelligence service - the very authority responsible for intercepting communications, putting them in writing and certifying their authenticity - could be doubted

Furthermore, there should *be no unfairness in way in which the experts are chosen or resulting from either their partiality or one or more of them being able to play a special or dominant role in the proceedings*.

This was alleged to have occurred in *Mirilashvili v. Russia*, no. 6293/04, 11 December 2008 but the European Court concluded that this had not been the case regarding any of the experts appointed to assess whether the voice on recordings of telephone conversations was that of the applicant. Indeed, it pointed out that the defence had had an opportunity to participate in the process of appointing and questioning of experts and submissions by its own experts had led the court to commission another examination of the audiotapes concerned. The fact that a particular expert sought had not been appointed was not significant as she had not been claimed to be irreplaceable as the only expert in the field of phonetic studies and an alternative had been appointed.

However, it may be open to the court to conclude that there are *other ways than an expert assessment to test the reliability of particular evidence*, as was the situation in, e.g., *Saçak v. Türkiye* (dec.), no. 18815/18, 30 August 2022. In that case, the European Court was unable to conclude that the applicant had laid the basis of a *prima facie* claim such as to cast doubt on the domestic courts' conclusion that a particular mobile telephone had been used by him and could not accept that its rejection of a comparative voice analysis of the intercepted calls was in and of itself sufficient to conclude that the applicant was deprived of all the means necessary to subject this matter to meaningful scrutiny. Thus, it pointed out that, even though he and his lawyer had access to the audiotapes of the intercepted telephone calls, there was no indication that they had attempted to obtain copies thereof or had asked the trial court to play those recordings during the trial with a view to shedding light on the question whether the calls in question were made by him or not.

In opposing the use of particular electronic evidence, there may also need to be a possibility of contesting its lawfulness where that would be relevant for the proceedings in the jurisdiction concerned, as was possible in *Fejzulla and Mazreku v. "the former Yugoslav Republic of Macedonia"* (dec.), no. 23065/07, 31 May 2011 and *Svetina v. Slovenia*, no. 38059/13, 22 May 2018.

8.3.5 Voluntariness

A lack of voluntariness in the way electronic evidence has been obtained will, where that evidence is the basis for a conviction, will lead to the trial being considered unfair.

Thus, the *use of psychological pressure Allan v. United Kingdom*, no. 48539/99, 5 November 2002 to obtain an audio-recording of an admission meant that the information thereby obtained was to be regarded as having been obtained in defiance of the suspect's will and so its use at the trial impinged on his right to silence and privilege against self-incrimination. In that case, the admissions had been obtained through the persistent questioning by an informer who had, at the instance of the police, channelled conversations

with the defendant into discussions of the alleged offence in circumstances which could be regarded as the functional equivalent of interrogation, without any of the safeguards which would attach to a formal police interview, including the attendance of a lawyer and the issuing of the usual caution.

8.3.6 Disclosure

The *right to an adversarial trial includes a requirement for the prosecution authorities to disclose to the defence all material evidence in their possession for or against the accused and that includes electronic evidence*. Such disclosure will be important for the defence to be able to test its admissibility, integrity, reliability, completeness and evidential value as part of preparing an effective defence, not least where the material concerned might include exculpatory material.

However, as the European Court emphasised in *Yüksel Yalçınkaya v. Türkiye* [GC], no. 15669/20, 26 September 2023, *electronic evidence may be withheld from the defence* in order, e.g., to protect information about the details of undercover police operations, sensitive information relevant to national security and the rights of others.

Nonetheless, there must always be an *appropriate procedure by which both the relevance of evidence obtained by the prosecuting authorities and the necessity of its disclosure or it being withheld can be properly assessed*.

Such a procedure was found not to exist in *Matanovič v. Croatia*, no. 2742/12, 4 April 2017, with the result that the European Court concluded that the applicant had been prevented from establishing that evidence in the possession of the prosecution – CD recordings – that had been excluded from the case file might have reduced his sentence or put into doubt the scope of his alleged criminal activity.

Any decision to withhold evidence should be taken by a judge in a process that affords the defence an opportunity to participate to the maximum extent possible. decision-making process involving the defence The judge must perform a balancing exercise between the public interest in non-disclosure and the importance of the documents to the issues of interest, or likely to be of interest, to the accused. This requires the judge to analyse the content of the materials, rather than their type, and determine whether the materials concerned would be of any assistance for the defence, and whether their disclosure would, at least arguably, have harmed any identifiable public interest.

This was found not to have occurred in *Mirilashvili v. Russia*, no. 6293/04, 11 December 2008, in which court's decision to withhold particular material was based on its type – i.e., material relating to operational and search activities - and not on an analysis of its content. Thus, it appeared not analyse whether those materials would have been of any assistance for the defence, and whether their disclosure would, at least arguably, have harmed any identifiable public interest. This was a consequence of the applicable legislation, which prohibited in absolute terms the disclosure of documents relating to these activities and did not provide for any "balancing exercise" by a judge.

The non-disclosure in this case of material relating to the manner in which the electronic evidence was obtained was considered a factor in concluding that the defence had been placed at a serious disadvantage *vis-à-vis* the prosecution in respect of the examination of a very important part of the case file so that, having regard to the importance of appearances in matters of criminal justice the proceedings in question, taken as a whole, could

not be regarded as satisfying the requirements of a "fair hearing".

In the case of surveillance recordings, Article 6 of the European Convention does not require the accused actually to have *access to copies of them*. Nonetheless, there would be a problem in complying with this provision if s/he could not effectively obtain either the transcripts or a copy of the recordings of the tapped phone calls used as evidence in the proceedings.

Moreover, the *production of the transcript of the recordings* by an independent and impartial expert and the *playing back of the recordings* at the trial is likely to be regarded by the European Court as a counterbalance to the impossibility for the defence to obtain the copies of the recordings, particularly if an ample opportunity is provided for the accused to compare the transcripts against the played material. Such transcripts should be made available in sufficient time to ensure that the accused can adequately prepare her/his defence.

These requirements were all found to be satisfied in *Matanovič v. Croatia*, no. 2742/12, 4 April 2017 so that the European Court did not find any unfairness in the proceedings in connection with the fact that the applicant was not provided with copies of the secret surveillance recordings which were relied upon for his conviction.

However, in *Beraru v. Romania*, no. 40107/0418 March 2014, the accused's lawyers could not obtain a copy of the transcripts of the recordings of the tapped phone calls or a taped copy of them that were used as evidence in the file, which was a factor in the European Court concluding that the proceedings in question, taken as a whole, did not satisfy the requirements of a fair trial.

See also the similar ruling *in Cevat Soysal v. Turkey*, no. 17362/03, 23 September 2014, in which the inability of the applicant to have access to the originals of audiotapes of telephone conversations prevented him from effectively challenging the reliability of the transcripts with which he had been provided.

On the other hand, in *İnal v. Turkey*, no. 28359/08, 18 January 2022, the applicant was provided with a copy of the CDs containing the audio recordings and the transcripts of the intercepted telephone conversations and in *Blagajac v. Croatia*, no. 50236/16, 9 May 2023, an assertion that the applicant was not aware of a file containing all the surveillance material was not considered credible by the European Court, which also found that there was no evidence of him seeking access to this material or of him complaining about his inability to access it

Insofar as any part of the electronic evidence has been *lost or destroyed* and thus cannot be disclosed to the defence, there will be a need to establish - in so far as possible - whether this was deliberate. This was not considered to have been the situation in *Mirilashvili v. Russia*, no. 6293/04, 11 December 2008. Moreover, where, as in *Natunen v. Finland*, no. 21022/04, 31 March 2009, a decision to destroy undisclosed evidence – such as the recordings of telephone conversations which could possibly have supported the accused's innocence - was made in the course of the pre-trial investigation without providing the defence with the opportunity to participate in the decision-making process, there will be a violation of Article 6(1) taken together with Article 6(3)(b).

Furthermore, where it is complained that certain electronic evidence could not be adduced to support a particular defence, *it will need to be established that that evidence actually existed*. See, e.g., *Lyubchenko v. Ukraine* (dec.), no. 34640/05, 31 May 2016, in which the investigating authorities had consistently denied the existence of an audio recording of a

conversation involving the accused and there was no proof to the contrary.

The particular approach to disclosure required where *a mass of electronic data* involved has been addressed in *Sigurður Einarsson and Others v. Iceland*, no. 39757/15, 4 June 2019. The European Court reaffirmed that the prosecution authorities should disclose to the defence all material evidence in their possession for or against the accused. However, it indicated that there would be no withholding of it were it was not in fact aware of what was contained in the mass of electronic data – such as that seized in that case during a search - and thus, to that extent, did not hold any advantage over the defence.

On the other hand, it took a different view as regards data that had been "tagged", i.e., through it being searched by means of key words and then reviewed by the investigators in order to determine which material should be included in the investigation file. Where such a selection is made by the prosecution alone, without the defence being involved and without any judicial supervision of the process – as had occurred in this case - any attempted assessment by the prosecution of the importance of concealed information to the defence and to weigh this against the public interest in keeping the information secret could not comply with the requirements of Article 6(1).

Moreover, although there was no obligation on the prosecution to create documents which did not already exist, it found in that case that further searches in the data would have been technically rather straightforward and in principle it would been appropriate for the defence to have been *afforded the possibility of conducting – or having conducted – a search for potentially disculpatory evidence*, particularly where any obstacles to securing privacy interests were not insurmountable obstacles.

As a result, it considered that a refusal to allow the defence to have further searches of the "tagged" documents carried out would in principle raise an issue under Article 6(3)(b) with regard to the provision of adequate facilities for the preparation of the defence.

However, in that particular case, the lack of access to the data in question was not considered to be such that the applicants were denied a fair trial overall as they had not appeared at any stage to have formally sought a court order for access to the "full collection of data" or for further searches to be carried out nor to have suggested further investigative measures, such as a fresh search using keywords suggested by them.

Where there is a substantial amount of telecommunication data that has been gathered, it was recognised in *Rook v. Germany*, no. 1586/15, 25 July 2019 that *support may have to be provided in use of the software required to analyse it*, as well as possibly the assistance of a judicial employee in examining the data. However, the defence may also be expected to narrow down the search by looking for specific telephone lines, for connections between specific telephones lines, within a certain frame of time, overall allowing for substantial reduction of the data with potential relevance and also to engage substantially in the analysing, listening and reading exercise. In this regard, it was also made clear by the European Court that, where the accused are the ones who have been the subject of the surveillance generating the data concerned particular account can be taken of the fact that they would know best what specific telecommunicationsurveillance data to look for.

That case also showed that it may not be enough to provide the defence with the entirety of the electronic files that have been gathered as it may not be readable without a special forensic-data-analysis program or the provision of a copy in a format readable with freely available software. The latter was eventually requested and provided in the Rook case. The delay in getting this was not shown in that case to have been prejudicial to the

defence and, as with the telecommunication data, the European Court considered that defence was well-placed to develop the search parameters needed to identify relevant material and could have engaged more in undertaking the analysis in the time available.

Finally, where it may not be possible to share particular electronic evidence with the accused, it should not be overlooked that – as the European Court emphasised in *Yüksel Yalçınkaya v. Türkiye* [GC], no. 15669/20, 26 September 2023 - *the requirement of "fair balance" between the parties might have implications for other aspects of the way in which the proceedings are conducted*.

Thus, in that case an opportunity for the applicant to acquaint himself with the decrypted material concerning his exchanges on the messaging application and information concerning the individuals with whom he had communicated might have constituted an important step in preserving his defence rights. However, although the appeal court had requested that this be provided to the applicant, it had delivered its judgment without waiting for this to happen and the cassation court had concluded that this had not affected the outcome, leading the European Court to conclude that this had been at the expense of the procedure leading to it.

8.3.7 Examining witnesses

Where reliance is placed on an electronic recording of a statement by a person other than an accused, the possibility of cross-examining the persons with whom the conversations had occurred was one of the factors that led the European Court to conclude in *Taraneks v. Latvia*, no. 3082/06, 2 December 2014 that the use of this evidence obtained through procedures not in accordance with requirements under the European Convention had not rendered the proceedings as a whole unfair

That ruling did not address the question of *whether the person whose statements form part of the electronic evidence, or allegedly do so, should be regarded as a witness* within the meaning of Article 6(3)(d), giving rise to a potential need to be able to cross-examine them in the proceedings concerned.

However, the European Court proceeded on this assumption in *Arlewin v. Sweden* (dec.), no. 32814/11, 2 February 2016 with respect to the interviews of certain anonymous persons on a television programme that had been admitted in evidence in a prosecution for fraud.

Although the programme was thus viewed during the trial, the European Court also doubted whether these anonymous persons could be considered sufficiently connected to the proceedings to be regarded as "witnesses" since the prosecutor had not specifically referred to or invoked any of the statements made by them.

In any event, the applicant had the opportunity to oppose the use of the programme as evidence and indeed did so. Moreover, the national courts had been aware of his opposition to the evidence being used as well as his grounds for why the programme and the statements made therein should be given very little, if any, value as evidence. Furthermore, the statements had been given to a journalist and not to the police during the investigation and, while the prosecution relied on the programme as evidence, it was neither the sole evidence nor the decisive evidence against the applicant.

In addition, there was nothing to indicate that the programme, or the statements made therein, was used by the courts to support their conclusion that the applicant had committed the offences of which he was convicted.

As a result, the European Court concluded that the criminal proceedings against the applicant as a whole were fair and the fact that he had not been able to cross-examine the anonymous persons in the television programme had not restricted his defence rights to an extent incompatible with the guarantees provided by Article 6(1) and 3(d) of the European Convention.

8.3.8 Support for other evidence

Electronic evidence may be an important contribution to establishing that the pre-trial statement of a witness who did not appear at the trial was not the sole or decisive basis for an accused's conviction so that, given the availability to the defence of some procedural safeguards capable of counterbalancing, at least in part, the absence of this witness at trial, the admission of the statement would not be regarded as resulting in a breach of Article 6(1) read in conjunction with Article 6(3)(d) of the European Convention.

Thus, the telephone records of a Sim card were among the pieces of collaborative evidence in *Štefančič v. Slovenia*, no. 18027/05, 25 October 2012 confirming the whereabouts and contacts made by the person whose pre-trial statement was admitted as evidence so that this testimony was not to be regarded as the sole or decisive evidence against the applicant in that case, but rather one of the elements which, examined in their individual probative value as well as in relation to the other available pieces of parallel evidence, led the Slovenian courts to convict him for drug-trafficking.

Similarly, in *Rastoder v. Slovenia*, no. 50142/13, 28 November 2017, telephone and GPS data contributed to establishing that the applicant had had a motive to attack the victims, had been prepared for the fight as he had been armed and accompanied by his sons, who had likewise been armed, and had inflicted a number of serious injuries on the victims so that a pre-trial statement by a witness could not be regarded as the sole or decisive basis for his conviction.

However, this will not always be the case:

- *Martirosyan v. Armenia*, no. 18550/13, 6 December 2018, at paras. 65-66, where number plate recognition report and transcripts of telephone calls were not, along with certain other evidence, enough to displace the fundamental relevance of certain absent witnesses in a prosecution for attempted murder and illegal possession of firearms; and

- *Avaz Zeynalov v. Azerbaijan*, no. 37816/12, 22 April 2021, at para. 122, in which an audio recording of conversations on a CD-ROM could not alter the decisive nature of statements by absent witnesses in a conviction for bribery-related offences.

It should also be noted that the European Court has welcomed in *Strassenmeyer v. Germany*, no. 57818/18, 2 May 2023, at para. 85 - a case in which the applicant was unable to cross-examine his co-accused as he had refused to testify – the adoption of a legislative reform allowing for video-recordings of pre-trial statements given by an accused.

Electronic evidence may also be enough to outweigh some weaknesses in the way in which other evidence has been gathered:

Thus, the fact that a conviction had partly relied on incriminating evidence in the form

of audio and video recordings and computer data which multiple expert examinations confirmed to have been authentic contributed to the conclusion in *Mamaladze v. Georgia*, no. 9487/19, 3 November 2022 that, despite some failings with respect to handling of other evidence, it was within the domestic courts' remit to consider whether, overall, sufficiently strong evidence existed to demonstrate that the applicant had been guilty of "preparation of murder."

8.3.9 Safeguards for using other evidence

The availability of electronic evidence could sometimes have been *important in demonstrating that there has been no abuse in the gathering of evidence*. Such situations can be seen in:

- *Layijov v. Azerbaijan*, no. 22062/07, 10 April 2014, where a time lapse in carrying out a search after an arrest raised legitimate concerns about the possible "planting" of the evidence, because the applicant was completely under the control of the police during that time. In that case, the investigating authorities had failed to submit in the course of the domestic proceedings a copy of the video-recording of the search of the applicant and his and, despite an explicit request, a copy of it had not been submitted to the European Court;
- *Ayetullah Ay v. Turkey*, no. 29084/07, 27 October 2020, in which the Government, having been invited by the European Court to submit a video recording of a search, had stated that they were unable to obtain it.[9] Some photographs which they did submit were found not to be sufficient to rule out any doubts surrounding the circumstances in which that evidence was obtained, although that would not necessarily be so in all cases.

9 Observations about the recording by a judge on an earlier panel dealing with the cases were not addressed by the court convicting the accused.

9. SOME OTHER ISSUES

Other issues that have arisen with respect to electronic evidence have concerned the ability of the defence to adduce it, the possible impact on the presumption of innocence, its use in challenging court rulings, its contribution to the length of proceedings, its use for purposes other than for which it was gathered and its use in civil proceedings.

9.1. ADDUCING EVIDENCE BY THE DEFENCE

There may be a *need to secure electronic evidence which the defence considers necessary* to adduce in particular proceedings.

The domestic courts' refusal to order the retrieval of the video recordings of airport security cameras in the context of an accused's allegation that poison found in his suitcase had been planted on the basis that his application had not been supported by the appropriate supporting documents and that, more importantly, no information had been indicated as to where the recordings – which were not kept by the airport – were to be retrieved from was considered in *Mamaladze v. Georgia*, no. 9487/19, 3 November 2022 to be reasoning that was arbitrary or unreasonable.

9.2. PRESUMPTION OF INNOCENCE

The *public dissemination of electronic evidence that creates the impression that persons have committed the crimes with which they are charged before their guilt is proved* in court will be in violation of the presumption of innocence where there was no public interest for having done so.

Such a violation was found in *Batiashvili v. Georgia*, no. 8284/07, 10 October 2019 in respect of the dissemination to the media by the interior ministry of an edited recording of an accused's telephone conversation, whereby it was insinuated – four days before being charged - that he had covered up the preparation of a crime, owing to his failure to inform the relevant authorities of the possible involvement of certain separatist forces in a rebellion and had aided and abetted high treason aimed at overthrowing the constitutional order by force. The dissemination was considered by the European Court not to have been justified by the public interest in obtaining information on events planned by the separatists to which the applicant had referred in the conversation concerned.

9.3. PAPER COPIES OF PROCEDURAL DOCUMENTS

The European Court held in *Patricolo and Others v. Italy*, no. 37943/17, 23 May 2024 the absence of an attestation that the paper copies of the notice of service were true copies of the original electronic documents which had been served on them by certified email did not prevent the Court of Cassation from assessing compliance with the short time limit for filing an appeal at the earliest stage of the proceedings. Furthermore, it considered that declaring the appeals inadmissible, moreover without giving the applicants a fair chance to submit the attestation at a later stage – especially in a transitional phase from paper-based to electronic proceedings – therefore went beyond the aim of ensuring legal certainty and the proper administration of justice and created a barrier preventing the applicants from having their case determined on the merits by the Court of Cassation.

As to the *risk that the paper copies might be inconsistent with the electronic originals*, the European Court noted in that case that, under the national law concerned, the integrity of documents filed with a court is generally ensured by the criminal and disciplinary sanctions available in case of a breach of duty. Moreover, it stated that whether paper copies were true copies of electronic originals could easily be checked by inviting the applicants to file the appropriate attestation at a later stage in the proceedings. In its view, this was particularly true in the context of the transition from paper-based to electronic proceedings, where the need to adapt formal requirements designed for paper documents called for some flexibility in their application to electronic ones.

9.4. CHALLENGES TO THE CONDUCT OF TRIAL PROCEEDINGS

An audio recording of the conduct of proceedings can be used as *evidence of the treatment of a party by a judge* in them, such as in :

- *Sidlova v. Slovakia* (dec.), no. 50224/99, 22 February 2005, in which the European Court noted that the applicant's complaint concerning the treatment received from the judge presiding over her case, which relied upon an audio recording made by her of a hearing, had been accepted;

  Dmitriyevskiy v. Russia, no. 42168/06, 3 October 2017, in which the European Court found admissible a complaint alleging that a judge had disallowed applications to have the transcript amended in line with the audio recording of the hearings which had been submitted by the applicant on the sole ground that that recording had not been authorised. However, having regard to its finding of a violation of Article 10 in relation to the applicant's conviction in the proceedings concerned, the European Court considered that it was not necessary to examine it.

See also *Zhvayy v. Ukraine*, no. 6781/13, 22 September 2022, in which a court had treated as irrelevant an applicant's request to consider an audio recording of an alleged conversation with a judge in support of his allegations against the chairman of the High Council of Justice that were the subject of defamation proceedings brought by the latter against him. This response to the applicant's request contributed to the finding by the European Court that the defamation proceedings had resulted in an excessive and disproportionate burden being placed on him, contrary to his right to freedom of expression under Article 10.

However, it *must be possible to attribute the impugned remarks to the judge concerned*, which was found not to be possible in *Pavlov v. Russia* (dec.), no. 31430/05, 26 January 2015, no examination of the recording having ever been carried out and none seeming to have ever been requested, Moreover, the original of the audio tape had been lost.

Moreover, in such efforts, the *audio recording relied upon should not be of poor quality or incomplete*, factors in *Mikhaylova v. Ukraine*, no. 10644/08, 6 March 2018, which led the European Court to consider that it was not appropriate to take such a recording into account when determining a complaint about a judge's alleged lack of impartiality.

Furthermore, an audio-recording of a court hearing was, however, sufficient in *Shkirya v. Ukraine*, no. 30850/11, 24 June 2021 to refute a submission that the applicant's arguments and his supporting documents had not been duly considered by the national courts.

9.5. LENGTH OF PROCEEDINGS

The complexity of computer software created which was allegedly used for fraudulent accounting and tax evasion by a company was recognised by the European Court as a factor in the time taken by the tax inspectorate to assess whether its accounting documents had been in order and, if not, how much tax may have been avoided. However, it was not considered enough to justify the inspectorate taking nearly twenty months to reach a conclusion on this issue and this delay was a contributing element to the finding in *Gančo v. Lithuania*, no. 42168/19, 13 July 2021 that the criminal proceedings had, contrary, to Article 6(1), been unduly prolonged.

9.6. BEING USED FOR OTHER PURPOSES

Where material that had been lawfully obtained through the interception of a person's telephone conversation as part of a criminal investigation was then used in disciplinary proceedings against him, this was held in *Karabeyoğlu v. Turkey*, no. 30083/10, 7 June 2016 to be an interference with the exercise of his right to respect for his private life that was not in accordance with the law, as required by Article 8(2) since such use was contrary to the purposes for which surveillance measures was authorised under the constitution and the law and since the material had not been destroyed within the deadline applicable following the decision not to prosecute him.

No violation of Article 8 has, however, been found in *Terrazzoni v. France*, no. 33242/12, 29 June 2017 and *Starkevič v. Lithuania*, no. 7512/18, 29 March 2022 where the transcript of telephone conversations intercepted in the course of a criminal investigation was subsequently used in disciplinary proceedings and this was neither precluded by national law nor obtained in a manner inconsistent with the requirements under that provision governing such interceptions.

Moreover, in. *Versini-Campinchi and Crasnianski v. France*, no. 49176/11, 16 June 2016, in which the use in disciplinary proceedings against a lawyer of a transcript of a transcript of a lawfully intercepted telephone conversation between her and a client, while an interference with the right under Article 8, was not found to entail a violation of it where the domestic courts had satisfied themselves that the transcript did not infringe the client's defence rights and she was particularly well-qualified to know that her utterances were in breach of professional confidentiality.

There was no suggestion in *Karabeyoğlu* that the use in disciplinary proceedings of evidence gathered as part of a criminal investigation also amounted to a violation of Article 6.

Furthermore, it was held in *Starkevič v. Lithuania*, no. 7512/18, 29 March 2022 that the use in such proceedings of evidence based on the interception of electronic communications as part of a criminal investigation had not impaired the accused's right to a fair hearing. In so ruling, the European Court confirmed what it described as its practice that the use of material of the criminal case within disciplinary proceedings was not ruled out, provided that the rights of the defendant have been respected (which had been found not to have occurred in *Vanjak v. Croatia*, no. 29889/04, 14 January 2010).

A violation of Article 8 has also been found in *Eminağaoğlu v. Turkey*, no. 76521/12, 9 March 2021 in respect of the use in disciplinary proceedings of recordings obtained through telephone tapping undertaken as part of a criminal investigation, for the same reason as that in the in *Karabeyoğlu* case. However, the complaints in that case relating to Article 6(1) did not concern the reliance placed on recordings.

9.7. USE IN CIVIL PROCEEDINGS

Where reliance is placed in civil and administrative proceedings on electronic evidence obtained contrary to the right to respect for private life, the European Court has followed the same approach as that regarding criminal proceedings when determining whether this has given rise to a violation of the right to a fair trial, namely, by assessing whether this has rendered the proceedings as a whole unfair.

In particular, it will be concerned with whether the party concerned had been given an opportunity to challenge the authenticity of the evidence and to oppose its use, as well as the quality of the evidence, any doubts casts on its reliability or accuracy by the circumstances in which it was obtained and whether the evidence in question was or was not decisive for the outcome of the proceedings.

Thus, having regard to the opportunity to challenge and oppose the use in adversarial proceedings of material obtained through video surveillance, the ample consideration given to the part's request in that regard and the fact that the impugned recording was not the only evidence relied on, the European Court considered in *Vukota-Bujic v. Switzerland*, no. 61838/10, 18 October 2016 that the proceedings whereby a benefits claim was determined were not in conflict with the requirements of fairness under Article 6(1) of the European Convention.

Similarly, in *López Ribalda and Others v. Spain* [GC], no. 1874/13, 17 October 2019, the use of evidence obtained through video surveillance was not, despite being obtained in breach of the right to respect for private life, found to have undermined the fairness of proceedings for unfair dismissal where the applicants had access to the recordings concerned, could contest their authenticity and oppose their use in evidence, their arguments in favour of their exclusion had been examined and they were not the only evidence relied upon. Moreover, as there was no reason to question their authenticity or reliability, they constituted sound evidence which did not necessarily need to be corroborated by other material.

This publication was produced with the financial support of the European Union and the Council of Europe. Its contents are the sole responsibility of the author(s). Views expressed herein can in no way be taken to reflect the official opinion of the European Union or the Council of Europe.

ENG

The Member States of the European Union have decided to link together their know-how, resources and destinies. Together, they have built a zone of stability, democracy and sustainable development whilst maintaining cultural diversity, tolerance and individual freedoms. The European Union is committed to sharing its achievements and its values with countries and peoples beyond its borders.

www.europa.eu

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

www.coe.int

Co-funded by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Co-funded and implemented by the Council of Europe