Joint Factsheet

Mass surveillance[1] ECtHR and CJEU Case-Law

(Last updated: 31/08/2026)

This factsheet has been prepared by the Registry of the European Court of Human Rights ("ECtHR")[2] and the European Union Agency for Fundamental Rights as part of a collaborative effort to highlight jurisprudence in selected areas where European Union ("EU") law and that of the European Convention on Human Rights ("ECHR" or "the Convention") interact.

I. Mass surveillance

In view of recent technological and social developments in the sphere of electronic communications, the ECtHR and the Court of Justice of the EU ("CJEU") have been called upon to address the risks to human rights stemming from mass surveillance regimes, namely systems allowing large-scale technical collection of information[3] in and related to electronic communications.

In the current, increasingly digital, age the vast majority of communications take digital form and are transported across global telecommunications networks using a combination of the quickest and cheapest paths without any meaningful reference to national borders. Surveillance not targeted directly at individuals has therefore the capacity to have a very wide reach, both inside and outside the territory of the State carrying out the surveillance[4].

Mass surveillance regimes may operate by tapping into and storing large volumes of data drawn from the bearers carrying Internet communications (so-called bulk interception)[5]. They may also require electronic communications service providers ("CSPs") to carry out general retention and storage of users' communications and related communications data[6] and to allow national authorities to have access to those data, either in a direct and unlimited fashion[7], or on the basis of targeted requests[8].

---

[1] For the purposes of this factsheet the general term "mass surveillance" is understood as "general surveillance of communications". The terminology is discussed more extensively in the 2017 report of the EU Fundamental Rights Agency, p. 29 Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update. See also FRA report on Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU - 2023 update | European Union Agency for Fundamental Rights.

[2] The content of this factsheet is not binding on the Court.

[3] The term "information" is used to cover untargeted interception of information in the context of criminal proceedings and not only information collected by intelligence services.

[4] ECtHR, *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, § 322, 25 May 2021; and *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, § 236, 25 May 2021.

[5] See for example ECtHR, *Big Brother Watch* [GC], cited above, § 15, and, more generally, the case-law described below in paragraph A.

[6] See for example ECtHR, *Podchasov v. Russia*, no. 33696/19, 13 February 2024 and, more generally, case-law described below in paragraph B.

[7] See for example ECtHR, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, nos. 72038/17 and 25237/18, 28 May 2024.

[8] See for example ECtHR, *Ben Faiza v. France*, no. 31446/12, 8 February 2018, and *Škoberne v. Slovenia*, no. 19920/20, 15 February 2024; CJEU (Grand Chamber), judgment of 2 March 2021, *Prokuratuur*, C-746/18,

Mass surveillance may target the content of electronic communications and/or related communication data, including subscribers' and registered users' personal data as well as traffic and location data. The acquisition of communications data is not necessarily less intrusive than the acquisition of content, as traffic and location data, taken as a whole, may allow very precise conclusions to be drawn concerning people's private lives, including their habits, permanent or temporary places of residence, daily movements, activities carried out, their personal relationships and social environments[9]. As to the content of electronic communications, a particular set of issues may arise when the bulk interception, retention and access thereof include the national authorities' attempts to decrypt encrypted electronic messages[10].

II. Mass surveillance in the case-law of the CJEU

The CJEU has examined mass surveillance regimes mainly from the standpoint of the protection offered to personal data and to the right to privacy by the e-Privacy Directive[11] and the General Data Protection Regulation ("GDPR")[12], read in the light of the fundamental rights guaranteed by Articles 7 (respect for private and family life), 8 (protection of personal data) and 11 (freedom of expression) of the Charter of Fundamental Rights of the EU ("the Charter")[13].

In specific instances relating to the operation of mass surveillance regimes, the CJEU has also provided guidance on the interpretation of other EU legal instruments, read in the light of the fundamental rights listed above, such as in the contexts of judicial cooperation in criminal matters and the European Investigation Order[14] or the fight against market abuse[15].

III. Mass surveillance in the case-law of the ECtHR

The ECtHR has examined mass surveillance regimes mainly from the standpoints of the right to respect for private life[16] and correspondence (Article 8 of the ECHR) and of the right to freedom of expression (Article 10 of the ECHR), in relation to the protection of journalists' communications.

EU:C:2021:152, (Grand Chamber) judgment of 5 April 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258, judgment of 17 November 2022, *Spetsializirana prokuratura*, C-350/21, EU:C:2022:896.

[9] CJEU (Grand Chamber), judgment of 8 April 2014, *Digital Rights Ireland e.a.*, C-293/12 and C 594/12, EU:C:2014:238, § 27; ECtHR, *Big Brother Watch* [GC], cited above, § 342.

[10] CJEU (Grand Chamber), judgment of 30 April 2024, *M.N. (EncroChat)*, C-670/22, EU:C:2024:372; ECtHR, *Podchasov v. Russia*, cited above.

[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ 2002 L 201, pp. 37-47 ("e-Privacy Directive").

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L 119, pp. 1-88 ("GDPR").

[13] Please refer to the CJEU case-law described below in sections C.1 and C.2.

[14] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ 2014 L 130, pp. 1-36("the European Investigation Order Directive"); see CJEU (Grand Chamber), *M.N. (EncroChat)*, cited above.

[15] Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation, OJ 2003 L 96, pp. 16-25 ("Market Abuse Directive") and Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse, OJ 2014 L 173, pp. 1-61 ("Market Abuse Regulation"); see CJEU (Grand Chamber), judgment of 20 September 2022, *VD and SR*, C-339/20 and C-397/20, EU:C:2022:703.

[16] In assessing interferences with the right to the respect for privacy stemming from mass surveillance regimes, the Court also relied on other Council of Europe legal instruments, such as the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional Protocol to

With respect to Article 8 of the ECHR, building on its case-law on secret surveillance regimes permitting targeted surveillance measures[17], the ECtHR has reiterated that in the special context of secret measures of surveillance, "foreseeability" means that the domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances and conditions on which public authorities are empowered to resort to any such measures and must indicate the scope of discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrariness[18].

It also reiterated that, where the legislation permitting secret surveillance is contested before the ECtHR, it is appropriate to address jointly the "in accordance with the law" and "necessity" requirements. Domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse[19].

As to the safeguards which should feature in a Convention-compliant mass surveillance regime, the ECtHR has considered it necessary to develop and adapt the safeguards set out in previous case-law on targeted interception regimes to the specificities of bulk interception of communications[20] and to the general retention and access to communications data[21].

With regard to Article 10 of the ECHR, the ECtHR has built on its existing case-law on searches of a journalist's home or workplace, adapting the substantive and procedural safeguards provided therein to the context of bulk interception[22] and general data retention[23]. It distinguished, in particular, the safeguards which should feature in a Convention-compliant mass surveillance regime in cases where interference with journalists' freedom of expression is intentional, from cases where a journalistic communication or related communications data have not been deliberately selected for examination, provided that it becomes apparent at the examination stage that the communication or related communications data contain confidential journalistic material[24].

---

the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows of 8 November 2001; the Recommendation of the Committee of Ministers No. R (95) 4 on the protection of personal data in the area of telecommunication services (adopted on 7 February 1995) and the 2015 Report of the European Commission for Democracy through Law on the Democratic Oversight of Signals Intelligence Agencies.

[17] See for example ECtHR, *Roman Zakharov v. Russia* [GC], no. 47143/06, §§ 227-234, ECHR 2015, and the case-law cited therein.

[18] See for example ECtHR, *Big Brother Watch* [GC], cited above, § 333.

[19] ECtHR, *Big Brother Watch* [GC], cited above, § 334.

[20] ECtHR, *Big Brother Watch* [GC], cited above, §§ 340-347; *Centrum för rättvisa* [GC], cited above, §§ 254-261.

[21] ECtHR, *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, §§ 394-395, 11 January 2022.

[22] ECtHR, *Big Brother Watch* [GC], cited above, §§ 447-450.

[23] ECtHR, *Big Brother Watch* [GC], cited above, §§ 524-525 and 528.

[24] ECtHR, *Big Brother Watch* [GC], cited above, § 447.

IV. Case-law of the Court of Justice of the European Union (CJEU) and of the ECtHR concerning mass surveillance

A. Bulk interception regimes

CJEU (Grand Chamber), judgment of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790

Facts – At the beginning of 2015 the existence of practices for the acquisition and use of bulk communications data by various UK security and intelligence agencies was made public. Under the contested regime, the Secretary of State could require CSPs, if he considered it necessary in the interests of national security or relations with a foreign government, to forward bulk communications data (including traffic and location data, as well as information relating to the services used) to the security and intelligence agencies. Such a disclosure of data concerned all users of means of electronic communication. Once transmitted, that data was retained by the security and intelligence agencies and remained available to those agencies for the purposes of their activities, as with the other databases maintained by those agencies. In particular, the data thus acquired was subject to bulk automated processing and analysis, could be cross-checked with other databases containing different categories of bulk personal data or be disclosed outside those agencies and to third countries. Those operations did not require prior authorisation from a court or independent administrative authority and did not involve notifying the persons concerned in any way.

Privacy International, a non-governmental organisation, brought an action before the Investigatory Powers Tribunal ("IPT") challenging the lawfulness of those practices. The IPT found that, following their avowal, the regimes were compliant with Article 8 of the ECHR. However, it identified the following four requirements which appeared to flow from the CJEU judgment *Tele2 Sverige and Watson and Others* (see below) and which seemed to go beyond the requirements of Article 8 of the ECHR: a restriction on non-targeted access to bulk data; a need for prior authorisation (save in cases of validly established emergency) before data could be accessed; provision for subsequent notification of those affected; and the retention of all data within the EU.

On 30 October 2017, the IPT made a request to the CJEU for a preliminary ruling with a view to clarifying the extent to which the Watson requirements could apply where the bulk acquisition and automated processing techniques were necessary to protect national security.

Law – The CJEU found that national legislation enabling a State authority to require CSPs to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security fell within the scope of the e-Privacy Directive. The interpretation of that Directive had to take account of the rights guaranteed by Articles 7, 8 and 11 of the Charter. Limitations on the exercise of those rights had to be provided for by law, respect the essence of the rights, and be proportionate, necessary, and genuinely meet the objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others. Furthermore, limitations on the protection of personal data had to apply only in so far as was strictly necessary; and in order to satisfy the requirement of proportionality, the legislation had to lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data were affected had sufficient guarantees that data would be protected effectively against the risk of abuse.

In the opinion of the CJEU, national legislation requiring CSPs to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission – which affected all persons using electronic communications services – exceeded the

limits of what was strictly necessary and could not be considered to be justified as required by the e-Privacy Directive read in light of the Charter.

ECtHR, *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, 25 May 2021

Facts – The case concerned the compatibility with Articles 8 and 10 of the ECHR of the UK secret surveillance regime, as it stood on 7 November 2017, governing:

I) the bulk interception of content and related communications data;

II) the receipt of intelligence from foreign intelligence services;

III) the acquisition of communications data from CSPs.

Law – **As to I), Article 8 ECHR:** the applicants complained that the bulk interception of cross-border communications by the intelligence services was in breach of Article 8.

As to the existence of an interference, the ECtHR considered bulk interception as a gradual process in which the degree of interference with individuals' Article 8 rights increased as the process progressed according to four stages:

(a) the interception and initial retention of communications and related communications data;

(b) the application of specific selectors to the retained communications/related communications data;

(c) the examination of selected communications/related communications data by analysts; and

(d) the subsequent retention of data and use of the "final product", including the sharing of data with third parties.

While the initial interception followed by the immediate discarding of parts of the communications did not constitute a particularly significant interference, the degree of interference with individuals' Article 8 rights increased as the bulk interception process progressed.

As to the relevant principles applicable to bulk interception cases, the ECtHR referred to its previous case-law on targeted interception regimes to state that while States enjoy a wide margin of appreciation in deciding what type of interception regime was necessary to protect national security and other essential national interests against serious external threats, in operating such a system the margin of appreciation had to be narrower and a number of safeguards had to be present. It considered that the safeguards identified in the context of targeted interception regimes should have been adapted to reflect the specific features of a bulk interception regime and, in particular, the increasing degrees of intrusion into the Article 8 rights of individuals as the operation moved through the stages identified above.

In assessing whether States had acted within their margin of appreciation the ECtHR addressed the "in accordance with the law" and "necessity" requirements jointly and carried out a global assessment as to whether the domestic legal framework clearly defined:

1. the grounds on which bulk interception could be authorised;
2. the circumstances in which an individual's communications could be intercepted;
3. the procedure to be followed for granting authorisation;
4. the procedures to be followed for selecting, examining and using intercept material;
5. the precautions to be taken when communicating the material to other parties;

6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material could be erased and destroyed;

7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;

8. the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

With particular regard to the precautions to be taken when communicating intercept material to other parties, the ECtHR specified that the transmission to foreign States or international organisations should be limited to material collected and stored in a Convention compliant manner and should be subjected to additional safeguards pertaining to the transfer itself. First of all, the circumstances in which such a transfer could take place had to be set out clearly in domestic law. Secondly, the transferring State had to ensure that the receiving State, in handling the data, had in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State had to guarantee the secure storage of the material and restricted its onward disclosure. This did not necessarily mean that the receiving State had to have comparable protection to that of the transferring State; nor did it necessarily require that an assurance was given prior to every transfer. Thirdly, heightened safeguards would be necessary for the transmission of material requiring special confidentiality, such as confidential journalistic material. Moreover, the transfer of material to foreign intelligence partners should also be subjected to independent control.

With respect to the precautions to be taken for the acquisition of related communications data through bulk interception, the ECtHR noted that these data are capable of being analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with. It considered that the interception, retention and searching of those data should have been analysed by reference to the same safeguards as those applicable to content, even though the legal provisions governing their treatment did not necessarily have to be identical in every respect to those governing the treatment of content.

By applying these principles to the case at hand, the ECtHR considered that the UK secret surveillance regime, despite its safeguards, did not contain sufficient "end-to-end" safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse. It identified the following deficiencies in the regime: absence of independent authorisation, failure to include the categories of selectors in the application for a warrant and failure to subject selectors linked to an individual to prior internal authorisation. These weaknesses concerned not only the interception of content of communications but also the interception of related communications data. While the Interception of Communications ("IC") Commissioner provided independent and effective oversight of the regime, and IPT offered a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services, these important safeguards were not sufficient to counterbalance the shortcomings highlighted above.

As to I), Article 10: the applicants complained that the bulk interception regime was in breach of Article 10 because it had a chilling effect on freedom of communication for journalists.

The ECtHR distinguished between intelligence services' intentional access to confidential journalistic material, through the deliberate use of selectors or search terms connected to a journalist or news organisation, and unintentional access, as a "bycatch" of the bulk interception operation. In the first scenario the ECtHR considered that the interference should be commensurate with that occasioned by the search of a journalist's home or workplace and stated that the selectors or search terms should have been authorised by a judge or other independent and impartial

decision-making body invested with the power to determine whether they were "justified by an overriding requirement in the public interest" and, in particular, whether a less intrusive measure could have sufficed to serve the overriding public interest. In the second scenario, the ECtHR considered that the degree of interference with journalistic communications and/or sources could not be predicted at the outset. Consequently, it would not be possible at the authorisation stage for a judge or other independent body to assess the justification of the interference. However, the ECtHR also considered that, due to technological developments, no-targeted surveillance had the capacity to have a very wide reach. Therefore, as the examination of a journalist's communications or related communications data by an analyst could be capable of leading to the identification of a source, the ECtHR considered it imperative that domestic law contained robust safeguards regarding the storage, examination, use, onward transmission and destruction of such confidential material. Moreover, if and when it became apparent that the communication or related communications data contained confidential journalistic material, their continued storage and examination by an analyst should only be possible if authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether continued storage and examination was "justified by an overriding requirement in the public interest".

By applying these principles to the case at hand, the ECtHR considered that the UK legal framework concerning the storage, onward transmission and destruction of confidential journalistic material provided adequate safeguards. However, it did not address the weaknesses identified by the ECtHR in its analysis of the regime under Article 8, nor did it satisfy the requirement that the use of selectors or search terms known to be connected to a journalist be authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether it was "justified by an overriding requirement in the public interest" and whether a less intrusive measure could have sufficed to serve the overriding public interest. Moreover, there were insufficient safeguards in place to ensure that once it became apparent that a communication which had not been selected for examination through the deliberate use of a selector or search term known to be connected to a journalist nevertheless contained confidential journalistic material, it could only continue to be stored and examined by an analyst if authorised by a judge or other independent and impartial decision making body invested with the power to determine whether its continued storage and examination was "justified by an overriding requirement in the public interest".

As to II), Article 8: The applicants mainly complained about the receipt by the domestic authorities of solicited intercept material from foreign intelligence services.

The ECtHR considered that where a request was made to a non-contracting State for intercept material the request had to have a basis in domestic law, and that law had to be accessible to the person concerned and foreseeable as to its effects. It would also be necessary to have clear detailed rules which give citizens an adequate indication of the circumstances in which and the conditions on which the authorities are empowered to make such a request and which provide effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the ECHR.

Upon receipt of the intercept material, the ECtHR considered that the receiving State must have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction. Moreover, any regime permitting the intelligence services to request either interception or intercept material from non-Contracting States, or to directly access such material, should be subject to independent supervision, and there should also be the possibility for independent *ex post facto* review.

By applying these principles to the case at hand, the ECtHR considered that in the UK legal framework there existed clear detailed rules which gave citizens an adequate indication of the

circumstances and conditions under which the authorities were empowered to make a request to a foreign intelligence service; domestic law contained effective guarantees against the use of such requests to circumvent domestic law and/or the ECHR; the UK had in place adequate safeguards for the examination, use, storage, onward transmission, erasure and destruction of the material; and the regime was subject to independent oversight by the IC Commissioner and there was a possibility for *ex post facto* review by the IPT.

As to II), Article 10: The applicants complained that the intelligence sharing regime had breached their rights under Article 10. The ECtHR considered that this argument gave rise to no separate issue over and above that arising out of Article 8.

As to III): please refer to paragraph C below.

Conclusion – Violation of Articles 8 and 10 of the ECHR with regard to the bulk interception. No violation of Articles 8 and 10 of the ECHR as to the receipt of intelligence from foreign services.

ECtHR, *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, 25 May 2021

Facts – The case concerned the compatibility with Article 8 of the Swedish signals intelligence regime as it stood in May 2018, in particular the bulk interception of cross-border communications, including content and related communications data.

The applicant complained primarily that domestic legislation and practice on bulk interception of communications were in violation of Article 8 of the ECHR.

Law – By applying the principles articulated in *Big Brother Watch* [GC], cited above, the ECtHR was satisfied that the main features of the Swedish bulk interception regime met the ECHR requirements on accessibility and foreseeability of the law and considered that the operation of this regime was in most aspects kept within the limits of what is "necessary in a democratic society". It found, however, three shortcomings: the absence of a clear rule on destroying intercepted material which did not contain personal data; the absence of a requirement in the relevant legislation that, when making a decision to transmit intelligence material to foreign partners, consideration was given to the privacy interests of individuals; and the absence of an effective *ex post facto* review.

Conclusion – Violation of Article 8 of the ECHR.

ECtHR, *Wieder and Guarnieri v. the United Kingdom*, nos. 64371/16 and 64407/16, 12 September 2023

Facts – The applicants, individuals residing outside the respondent State, complained primarily about the compatibility with Article 8 of the ECHR of the UK bulk interception regime.

Law – The main legal issue in the present case was whether, for the purposes of a complaint under that provision, persons outside a Contracting State fell within its territorial jurisdiction if their electronic communications were (or were at risk of being) intercepted, searched and examined by that State's intelligence agencies operating within its borders.

Considering that the interference with the privacy of communications clearly takes place where those communications are intercepted, searched, examined and used, and that the resulting injury to the privacy rights also takes place there, the ECtHR held that the interference with the applicants' rights under Article 8 fell within the territorial jurisdiction of the respondent State.

As to the merits of the complaint, the ECtHR relied on the conclusions set out in *Big Brother Watch* [GC], cited above.

Conclusion – Violation of Article 8 of the ECHR.

CJEU (Grand Chamber), judgment of 30 April 2024, *M.N. (EncroChat)*, C-670/22, EU:C:2024:372

Facts – In the context of an investigation carried out by the French authorities, it appeared that accused persons were using encrypted mobile phones that operated under an 'EncroChat' licence in order to commit offences primarily related to drug trafficking. Those mobile phones had special software and modified hardware that enabled end-to-end encrypted communication that could not be intercepted by conventional investigative means ('the EncroChat service'). With the authorisation of a judge, a Trojan software was uploaded to the server in the spring of 2020 and, from there, was installed on those mobile phones via a simulated update. Of a total of 66 134 subscribed users, 32 477 users in 122 countries are said to have been affected by that software, including approximately 4 600 users in Germany. The representatives of the French and Netherlands authorities informed the representatives of the other Member States' authorities of their investigation. The representatives of the German authorities signalled their interest in the data of the German users. The German criminal police announced that it was opening an investigation in respect of all unknown users of the EncroChat service, on suspicion of engaging in organised trafficking in substantial quantities of narcotic drugs and of forming a criminal association. On 2 June 2020 the Frankfurt Public Prosecutor's Office requested authorisation from the French authorities, by way of an initial European Investigation Order ("EIO"), to use the data from the EncroChat service in criminal proceedings.

In the context of the criminal proceedings brought against M.N., the domestic court requested a preliminary ruling concerning several procedural and substantial aspects of the compatibility of these EIOs with EU law, including whether, and if so under what conditions, Article 6(1) of the European Investigation Order Directive precluded a public prosecutor from issuing an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State where that evidence had been acquired following the interception, by those authorities, on the territory of the issuing State, of telecommunications of all the users of mobile phones which, through special software and modified hardware, enabled end-to-end encrypted communication.

Law – The CJEU held that the lawfulness of the EIOs at issue was subject to the same conditions as those which could be applicable to the transmission of such data in a purely domestic situation in the issuing State. Consequently, if, under the law of the issuing State, that transmission was subject to there being concrete evidence that the accused person had committed serious offences or to the evidence in the form of the data at issue being admissible, the issuing of an EIO was subject to all of those conditions. By contrast, Article 6(1)(b) of the European Investigation Order Directive did not require – including in a situation such as that at issue in the main proceedings, where the data in question were collected by the competent authorities of the executing State on the territory of the issuing State and in its interest – that the issuing of an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State should be subject to the same substantive conditions as those that applied in the issuing State in relation to the gathering of that evidence.

The CJEU noted in this respect that the EIO was an instrument falling within the scope of judicial cooperation in criminal matters based on the principle of mutual recognition of judgments and judicial decisions and on the rebuttable presumption that other Member States comply with EU law and, in particular, fundamental rights. Therefore, the authority issuing an EIO is not authorised to

review the lawfulness of the separate procedure by which the executing State gathered the evidence sought to be transmitted.

The CJEU also recalled that under Article 14(1) of the European Investigation Order Directive Member States must ensure that legal remedies equivalent to those available in a similar domestic case are applicable to the investigative measure to which an EIO relates and, in that context, the competent court must check that the conditions for issuing an EIO are satisfied, namely that it is necessary and proportionate for the purpose of the criminal proceedings initiated in the issuing State and that the investigative measures indicated in the EIO could have been ordered under the same conditions in a similar domestic case.

The CJEU finally held that in criminal proceedings against a person suspected of having committed criminal offences, national criminal courts are required to disregard information and evidence obtained through the EIO if that person is not in a position to comment effectively on them and they are likely to have a preponderant influence on the findings of fact.

ECtHR, *A.L. and E.J. v. France* (dec.), nos. 44715/20 and 47930/21, 24 September 2024

Facts – The applications concern the collection by French authorities of data concerning users of encrypted mobile phones that operated under an 'EncroChat' licence and its transmission to the UK law enforcement authorities. The applicants were the subject of criminal proceedings in the UK in two separate cases in which they were accused of using EncroChat. They invoked Article 8, alone and in conjunction with Article 13, and Article 6 of the Convention.

Law – Building on the principles articulated in *Wieder and Guarnieri*, cited above, the ECtHR held that the data collection, storage and transmission to UK authorities took place in France and therefore the interference with the applicants' rights under Article 8 fell within the territorial jurisdiction of the respondent State. The ECtHR noted that this conclusion was in line with the case-law of the CJEU (*M.N. (EncroChat)*, cited above) under which the principle of mutual recognition of judgments and judicial decisions prevented the authority issuing an EIO from reviewing the lawfulness of the separate procedure by which the executing State collected the evidence sought to be transmitted.

As to the exhaustion of domestic remedies, the ECtHR considered that neither the fact that the applicants resided outside French territory nor the fact that they did not voluntarily choose to place themselves under the jurisdiction of that State exempted them from their obligation to exhaust the domestic remedies available therein. The ECtHR found that in the domestic legal system there were provisions implementing Article 14 of the European Investigation Order Directive according to which Member States must ensure that legal remedies equivalent to those available in a similar domestic case are applicable to the investigative measure to which an EIO relates and noted that these provisions appeared to be consistent with the case-law of the CJEU, according to which the Member States are required to ensure respect for the right to an effective remedy enshrined in Article 47 of the Charter in the context of the procedure for issuing and executing an EIO. Since under domestic law a person under investigation could challenge the inclusion in the case file of criminal proceedings of evidence obtained in a separate set of proceedings, including by invoking a breach of the rights guaranteed by the Convention, this remedy was also opened to the applicants, who could have sought the annulment of the measure implementing the EIO under the same conditions and in the same manner as a person under investigation in France, including by invoking Article 8 of the Convention.

In reaching the conclusion that the applicants had an effective remedy at their disposal, the ECtHR also noted that under Article 14(7) of the European Investigation Order Directive the issuing State had to take account of the fact that an EIO had been successfully contested. Therefore, since criminal proceedings against the applicants were still pending, UK criminal courts would have been required to take into account a possible favourable outcome of proceedings before French courts.

Conclusion – Inadmissibility of the complaints under Article 8 of the Convention for non-exhaustion of domestic remedies; inadmissibility of the complaints under Articles 6 and 13 of the Convention as manifestly ill-founded.

B. CSPs' duties of data retention and targeted access by national authorities

B.1. Subscriber data

CJEU (Grand Chamber), judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788

Facts – Spanish police, in the course of investigating the theft of a wallet and mobile telephone, asked the investigating magistrate to grant them access to data identifying the users of telephone

numbers activated with the stolen telephone during a period of twelve days after the theft. The investigating magistrate rejected the request on the ground, *inter alia*, that the acts giving rise to the criminal investigation did not constitute a "serious" offence.

The referring court subsequently sought guidance from the CJEU on fixing the threshold of seriousness for which an interference with fundamental rights may be justified.

Law – The CJEU held that Article 15(1) of the e-Privacy Directive, read in the light of Articles 7 and 8 of the Charter, must be interpreted as meaning that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners, entailed an interference with their fundamental rights which was not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime. In particular, it indicated that in accordance with the principle of proportionality, a serious interference could be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime that was itself defined as "serious". By contrast, when the interference that such access entailed was not serious, that access was capable of being justified by the objective of preventing, investigating, detecting and prosecuting criminal offences generally. It did not consider access to the data which were the subject of the request to be a particularly serious interference because it only enabled the SIM cards activated with the stolen mobile telephone to be linked, during a specific period, with the identity of their owners. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data did not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data did not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data was concerned.

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

Facts – The applicants complained primarily under Article 8 of the ECHR (respect for private life) that, as users of prepaid mobile phone SIM cards, certain personal data (telephone number, name and address, date of birth and date of the contract) had been stored by their respective CSPs owing to a legal obligation as in force on 1 January 2008.

Law – The ECtHR recalled its well-established case-law concerning interferences with the right to private life under Article 8 as a result of the storage, processing and use of personal data (including *Ben Faiza v. France*, no. 31446/12, 8 February 2018, see below).

As to the justification of the interference, the ECtHR found that the contested storage had a basis in domestic law which was sufficiently clear and foreseeable. In addition, the duration and the technical side of the storage were clearly laid out. As to whether the interference was necessary in a democratic society, the ECtHR acknowledged that pre-registration of mobile-telephone subscribers strongly simplified and accelerated investigation by law enforcement agencies and could thereby contribute to effective law enforcement and prevention of disorder or crime. It also reiterated that in a national security context, national authorities enjoy a certain margin of appreciation when choosing the means for achieving a legitimate aim and noted that there was no consensus between the Member States as regards the retention of subscriber information of prepaid SIM card customers. Having regard to that margin of appreciation, the obligation to store subscriber information was, in general, a suitable response to changes in communication behaviour and in the means of telecommunications. In assessing the proportionality of the contested legal

obligation, the ECtHR distinguished the case at hand from those where highly personal information was stored (for instance, *Ben Faiza*, cited above) and, relying also on the CJEU judgment in the case *Ministerio fiscal*, cited above, found that the interference was limited in nature.

The ECtHR further observed that, even though the applicants had only complained about the storage of their personal information, it could not consider the proportionality of the interference without closely assessing the future possible access to and use of that information. It considered that access to the data was restricted to a certain number of authorities (either explicitly enumerated, access being allowed in this case through a centralised and automated procedure; or identified with reference to the tasks they performed, in which case access could be requested by means of a written request). Moreover, access was subject to a number of safeguards, including the fact that only the Federal Network Agency or the respective CSP could release the data; access was limited to necessary data; this necessity requirement was safeguarded by a general obligation for the respective authorities retrieving the information to erase, without undue delay, any data they did not need; in the context of the prosecution of offences, there had to be at least an initial suspicion. As to the available possibilities of review and supervision of information requests, the ECtHR distinguished the case from previous judgments concerning different interferences with Article 8, considering that such safeguards had to be considered an important, but not decisive, element in the proportionality assessment having regard to the limited data set involved. With this respect, it considered that the relevant legal framework offered sufficient guarantees since each retrieval and the relevant information regarding the retrieval were recorded for the purpose of data protection supervision, conducted by independent data protection authorities and an appeal was available to anyone who believed that his or her rights had been infringed.

Conclusion – No violation of Article 8 of the ECHR.

B.2. Traffic and location data

CJEU (Grand Chamber), judgment of 8 April 2014, *Digital Rights Ireland e.a.*, C-293/12 and C 594/12, EU:C:2014:238

Facts – The case originated in two requests for a preliminary ruling concerning the validity of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105, pp. 54-63 ("the Data Retention Directive"), raised in the context of domestic proceedings where the legality of national legislative and administrative measures concerning the retention of electronic communications data was challenged against constitutional and EU rights to data protection.

Law – The CJEU held that the obligation for CSPs to retain data relating to private life and communications and the national authorities' subsequent access to them interfered with the rights guaranteed by Articles 7 and 8 of the Charter. The interference was considered particularly serious and likely to generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance.

The CJEU held that the assessment of proportionality included an analysis of: (i) the appropriateness and (ii) necessity of the contested measures in the light of their objectives. Relying also on the principles set out in the ECtHR's case-law on the margin of appreciation, the CJEU held that the extent of the EU legislature's discretion could be limited by a number of factors, including the area concerned, the nature of the right at issue, the nature and extent of the interference and the object pursued by the interference, and that in the case at hand that discretion was reduced due to the importance of protection of personal data and the seriousness of the interference.

While the contested measures could be considered appropriate, having regard to the growing importance of means of electronic communication and their usefulness as valuable tool for criminal investigations, the CJEU considered that the Data Retention Directive was not limited to what was strictly necessary to achieve its goals, for the following reasons.

First, it covered, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. It was not restricted to data pertaining to a particular time period and/or a particular geographical zone and it applied even to persons for whom there was no evidence capable of suggesting that their conduct might have a link with serious crime.

Second, it did not contain substantive and procedural conditions governing the competent national authorities' access to the data and to their subsequent use. By simply referring, in a general manner, to serious crime, as defined by each Member State in its national law, the Directive failed to establish any objective criterion by which to determine which offences might be considered to be sufficiently serious to justify such an extensive interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Moreover, access by the competent national authorities to the data retained was not dependent on a prior review carried out by a court or independent administrative body whose decision sought to limit access to the data and their use to what was strictly necessary.

Thirdly, it required that all data be retained for a period of at least six months, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned. The CJEU concluded that the Directive entailed a wide-ranging and particularly serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, without such an interference being precisely circumscribed to ensure that it was actually limited to what was strictly necessary. The CJEU also noted that the Directive did not provide for sufficient safeguards, by means of technical and organisational measures, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use. It neither ensured the irreversible destruction of the data at the end of the data retention period, nor required that the data in question be retained within the EU.

CJEU (Grand Chamber), judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970

Facts – The case originated from two requests for preliminary rulings concerning the compatibility with EU law of domestic legislation providing for a general retention of all traffic and location data for the purposes of combating crime.

Law – The CJEU held that Article 15(1) of the e-Privacy Directive, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, had to be interpreted as precluding national legislation:

1) which, for the purpose of fighting crime, provided for the general and indiscriminate retention of all users' traffic and location data relating to all means of electronic communication.

In particular, the CJEU relied on *Digital Rights Ireland e.a.*, cited above, and specified that the retention of data had to be limited to what was strictly necessary with respect to the categories of data, the means of communication affected, the persons concerned and the retention period adopted. In order to satisfy these requirements, national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing

minimum safeguards. Second, it must provide for substantive conditions for data retention to maintain a connection between the data to be retained and the objective pursued;

2) governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where (i) the objective pursued by that access, in the context of fighting crime, was not restricted solely to fighting serious crime, (ii) access was not subject to prior review by a court or an independent administrative authority, and (iii) there was no requirement that the data concerned should be retained within the EU.

ECtHR, *Ben Faiza v. France*, no. 31446/12, 8 February 2018

Facts – The case mainly concerned compatibility with Article 8 of the ECHR of the access by judicial police, upon authorisation by the public prosecutor, to traffic and location data retained by CSPs.

Law – The ECtHR considered that access by national authorities to traffic and location data constituted an interference with the applicant's right under Article 8.

As to the justification of the interference, the ECtHR considered that the access had a basis in domestic law and was foreseeable. As to the safeguards against arbitrariness, the ECtHR observed that judicial police could have access to communications data upon authorisation of the public prosecutor. Moreover, access was subjected to *ex post facto* judicial review in the context of criminal proceedings against the interested person, where judges could assess its legality and, if they were to find it to be unlawful, could exclude the relative evidence from the proceedings. The ECtHR also noted that the guarantees provided for access to communications data were less stringent than those set out for real-time geolocation but considered that this differentiation was justified by the less severe nature of the interference.

As to whether the interference was necessary in a democratic society, the ECtHR considered that it was necessary to dismantle a large-scale drug trafficking operation. Moreover, the information obtained had been used in the context of criminal proceedings where the applicant benefited from an effective control as required by the rule of law and capable of limiting the interference at issue to what was necessary in a democratic society.

Conclusion – No violation of Article 8 of the ECHR.

CJEU (Grand Chamber), judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559

Facts – Following the CJEU judgment of 6 October 2015 in *Schrems*, C-362/14, EU:C:2015:650, which had ruled on the invalidity of the Safe Harbour Decision, under which the European Commission had considered that the United States ensured an adequate level of protection of the personal data transferred, Mr Schrems again challenged the transfer of his data by Facebook Ireland to the United States and the retention of his data on servers located in that country. He complained that the United States' law required Facebook Inc. to make the personal data transferred to it available to certain United States' authorities, such as the National Security Agency and the Federal Bureau of Investigation. Mr Schrems argued that since those data were used in the context of various monitoring programmes in a manner incompatible with Articles 7, 8 and 47 of the Charter, Decision 2010/87/EU could not justify the transfer of those data to the United States.

The domestic court referred a number of questions to the CJEU for a preliminary ruling, asking, *inter alia*, whether EU law applied to the transfer of data from a private company in the EU to a private company in a third country; if so, how the level of protection in the third country should be

assessed; and whether the level of protection afforded by the United States respected the essence of the rights guaranteed by Article 47 of the Charter.

Law – The CJEU held that the GDPR applied to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, those data were liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security. Moreover, the appropriate safeguards, enforceable rights and effective legal remedies required by the GDPR had to ensure that data subjects whose personal data were transferred to a third country pursuant to standard data protection clauses were afforded a level of protection essentially equivalent to that guaranteed within the EU. To that end, the assessment of the level of protection afforded in the context of such a transfer must take into consideration both the contractual clauses agreed between the controller or processor established in the EU and the recipient of the transfer established in the third country concerned, and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country.

Furthermore, unless there was a valid Commission adequacy decision, the competent supervisory authority was required to suspend or prohibit a transfer of data to a third country if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, the standard data protection clauses adopted by the Commission were not or could not be complied with in that third country and the protection of the data transferred (as required by EU law) could not be ensured by other means.

In order for the Commission to adopt an adequacy decision, it must have found that the third country concerned ensured, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order. In the CJEU's view, the Safe Harbour Decision was invalid. The relevant provision did not indicate any limitations on the power it conferred to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances, it could not ensure a level of protection essentially equivalent to that guaranteed by the Charter. Furthermore, with respect to the monitoring programmes, it was clear that that order did not confer rights enforceable against the United States' authorities in the US courts.

CJEU (Grand Chamber), judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791

Facts – The case originated from three requests for a preliminary ruling on the application of the e-Privacy Directive to national legislation imposing on CSPs an obligation requiring:

(i) the general and indiscriminate retention of traffic and location data for the purpose of safeguarding national security and combating terrorism;

(ii) to implement, on their networks, measures allowing the automated analysis and real-time collection of traffic and location data and real-time collection of technical data concerning the location of the terminal equipment used.

Law – The CJEU stressed that the objective of safeguarding national security had not yet been specifically examined by the CJEU in its judgments interpreting the e-Privacy Directive. It confirmed that while that Directive, read in light of the Charter, precluded legislative measures which provided for the general and indiscriminate retention of traffic and location data, where a Member State was facing a serious threat to national security that proved to be genuine and present or foreseeable,

there was no bar on legislative measures requiring CSPs to retain, generally and indiscriminately, traffic and location data for a period limited to what was strictly necessary, but which could be extended if the threat persisted. In such a case, the decision imposing such an instruction would be required to be subject to effective review, either by a court or by an independent administrative body whose decision was binding, the aim of that review being to verify that one of those situations existed and that the conditions and safeguards which had to be laid down were observed. For the purposes of combating serious crime and preventing serious threats to public security, a Member State could also provide – if it was limited in time to what was strictly necessary – for the targeted retention of traffic and location data, on the basis of objective and non-discriminatory factors according to the categories of persons concerned or using a geographical criterion, or of IP addresses assigned to the source of an Internet connection. It was also open to a Member State to carry out a general and indiscriminate retention of data relating to the civil identity of users of means of electronic communication, without the retention being subject to a specific time limit.

Furthermore, the e-Privacy Directive, read in light of the Charter, did not preclude national rules which required CSPs to have recourse, first, to the automated analysis and real-time collection of traffic and location data, and second, to the real-time collection of technical data concerning the location of the terminal equipment used, where it was limited to situations in which a Member State was facing a serious threat to national security that was genuine and present or foreseeable, and where recourse to such analysis could be the subject of an effective review by a court or independent administrative body whose decision was binding; and where recourse to the real-time collection of traffic and location data was limited to persons in respect of whom there was a valid reason to suspect that they were involved in terrorist activities and was subject to a prior review carried out either by a court or by an independent administrative body whose decision was binding.

CJEU (Grand Chamber), judgment of 2 March 2021, *Prokuratuur*, C-746/18, EU:C:2021:152

Facts – The case originated from a request for a preliminary ruling on the application of the e-Privacy Directive to national legislation allowing access to data retained by CSPs in the context of criminal proceedings.

Law – The CJEU reiterated that Article 15(1) of the e-Privacy Directive permitted access to retained traffic or location data for the purpose of fighting crime only when it came to serious crimes or serious threats to public security, regardless of the length of the period in respect of which access was sought and the quantity or nature of the data available in respect of that period.

The CJEU went on to hold that the power to examine access requests could not be given to a prosecutor's office, given that the latter's tasks of directing pretrial proceedings and prosecuting could affect its independence *vis-à-vis* the parties to the criminal proceedings.

ECtHR, *Big Brother Watch and Others v. the United Kingdom* [GC], cited above

Facts – Please refer to the dedicated box in paragraph B above.

Law – The applicants complained that the regime for the acquisition of communications data from CSPs was incompatible with their rights under Articles 8 and 10 of the ECHR. With respect to both complaints, the Grand Chamber upheld the Chamber's conclusions:

As to Article 8, at the date of the Chamber's examination of the case, domestic proceedings were pending concerning new legislation governing the retention of communications data by CSPs. In the course of those proceedings, the UK Government conceded that the relevant legal framework was

inconsistent with EU law and, consequently, the domestic judges found it to be incompatible with fundamental rights as guaranteed by EU law.

In view of both the primacy of EU law over UK law at the time and the Government's concession in the domestic proceedings, the ECtHR considered it clear that domestic law required that any regime permitting the authorities to access data retained by CSPs should limit access to the purpose of combating "serious crime", and that access should be subject to prior review by a court or independent administrative body. As the predecessor regime suffered from the same flaws as its successor, the ECtHR found that it could not be found to be in accordance with the law within the meaning of Article 8 of the ECHR.

As to Article 10, the ECtHR acknowledged that the contested regime afforded enhanced protection where data were sought for the purpose of identifying a journalist's source. Nevertheless, these provisions did not apply in every case where there was a request for the communications data of a journalist, or where such collateral intrusion was likely. Furthermore, in cases concerning access to a journalist's communications data there were no special provisions restricting access to the purpose of combating "serious crime". Consequently, the ECtHR considered that the regime was not in accordance with the law within the meaning of Article 10 of the ECHR.

Conclusion – Violation of Articles 8 and 10 of the ECHR as to the regime for the acquisition of communications data from CSPs.

ECtHR, *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, 11 January 2022

Facts – The case concerned the compatibility with Article 8 of Bulgarian laws and practices relating to the retention of and access to communications data. The applicants, two lawyers and two non-governmental organisations, asserted that the nature of their activities put them at risk of having their communications data accessed by the authorities.

Law – The applicants complained that the system of retention and subsequent accessing of communications data (subscriber, traffic and location data) did not meet the requirements of Article 8 of the ECHR.

Relying on its previous case-law (*Breyer*, *Centrum för rättvisa* [GC] and *Big Brother Watch* [GC], all cited above), the ECtHR considered that:

(a) the mere storing of those data amounted to interference with the individual applicants' right to respect for private life and correspondence and with the right to respect for correspondence of the applicant organisations;

(b) access by the authorities to the retained communications data constituted a further interference with Article 8.

As to the justification of the interference, relying on *Centrum för rättvisa* [GC] and *Big Brother Watch* [GC], both cited above, the ECtHR considered that acquisition of that data through bulk interception could be as intrusive as the bulk acquisition of the content of communications. Therefore, the same safeguards as those applicable to content should apply. The ECtHR added that by the same token, the general retention of communications data by CSPs and its access by the authorities in individual cases had to be accompanied, *mutatis mutandis*, by the same safeguards as secret surveillance (it relied in particular on *Roman Zakharov* [GC], cited above).

By applying these principles to the case at hand, and by assessing a number of elements (the accessibility of the law; the level of protection of retained data guaranteed by CSPs; analysing the grounds on which retained data can be accessed by the authorities; the procedures for obtaining access; the duration for storage and use of accessed data not subsequently used in criminal

proceedings; and considering the procedures for storing, accessing, examining, using, communicating and destroying data accessed by the authorities; oversight arrangements; notification to the interested individuals; remedies), the ECtHR concluded that the legal framework at issue fell short of the minimum safeguards against arbitrariness and abuse required under Article 8 of the ECHR in the following respects:

(a) the authorisation procedure did not appear capable of ensuring that retained communications data was accessed by the authorities solely when that was "necessary in a democratic society";

(b) no clear time-limits had been laid down for destroying data accessed by the authorities in the course of criminal proceedings;

(c) no publicly available rules existed on the storing, accessing, examining, using, communicating and destroying communications data accessed by the authorities;

(d) the oversight system did not appear capable of effectively checking for abuse;

(e) the notification arrangements were too narrow; and

(f) there was no effective remedy.

Conclusion – Violation of Article 8 of the ECHR as to the system of retention and accessing of communications data.

CJEU (Grand Chamber), judgment of 5 April 2022, *Commissioner of An Garda Síochána e.a.*, C-140/20, EU:C:2022:258

Facts – The case originated from a request for a preliminary ruling on the application of the e-Privacy Directive to national legislation allowing access to data retained by CSPs in the context of criminal proceedings.

Law – The CJEU confirmed its established case-law to the effect that EU law precluded national legislation providing for the general and undifferentiated retention of traffic data and location data relating to electronic communications as a preventive measure for the purposes of combating serious crime and preventing serious threats to public security. It considered however that EU law did not preclude:

– the targeted retention of traffic and location data for a limited time and circumscribed by means of objective and non-discriminatory factors;

– the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a limited period in time;

– the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and

– recourse to an instruction requiring CSPs, by means of a decision of the competent authority subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,

provided that those measures ensured, by means of clear and precise rules, that the retention of data at issue was subject to compliance with the applicable substantive and procedural conditions and that the persons concerned had effective safeguards against the risks of abuse.

Moreover, the CJEU considered that EU law precluded national legislation pursuant to which the centralised processing of requests for access to data retained by CSPs, issued by the police in the context of the investigation or prosecution of serious criminal offences, was the responsibility of a police officer, assisted by a unit established within the police service which has a degree of

autonomy in the exercise of its duties, and whose decisions could subsequently be subject to judicial review.

CJEU (Grand Chamber), judgment of 20 September 2022, *SpaceNet et Telekom Deutschland*, C-793/19 and C-794/19, EU:C:2022:702

Facts – The case originated from two requests for preliminary rulings on the application of the e-Privacy Directive to national legislation imposing on CSPs to retain, in a general and indiscriminate way, most of the traffic and location data of the end users of those services (including data relating to websites visited and data from electronic mail services), laying down a retention period of several weeks and rules intended to ensure the effective protection of the retained data against the risks of abuse and against any unlawful access to those data.

Law – The CJEU confirmed its established case-law against the generalised and indiscriminate retention of traffic data and location data for the purposes of combating serious crime or preventing serious threats to public security (see *La Quadrature du Net and Others* and *Commissioner of An Garda Síochána e.a.*, both cited above). It found that the national legislation in question did not comply with EU law, despite the existence of safeguards and a shorter retention period than in previous cases. The CJEU also ruled that the retention of these data and access to them constituted separate interferences with the fundamental rights of the data subjects, requiring separate justification, and that, consequently, national legislation ensuring full compliance with the conditions resulting from the case-law on access to retained data could not, by its very nature, be capable of limiting or even remedying the serious interference with the rights of the data subjects that would result from the general retention of these data.

CJEU (Grand Chamber), judgment of 20 September 2022, *VD and SR*, C-339/20 and C-397/20, EU:C:2022:703

Facts – The case originated from two requests for a preliminary ruling concerning the interpretation of EU provisions on market abuse read in conjunction with Article 15(1) of the e-Privacy Directive. The requests have been made in the context of criminal proceedings brought against VD and SR in respect of insider dealing, concealment of insider dealing, aiding and abetting, corruption and money laundering.

Law – The CJEU ruled that the Market Abuse Directive and the Market Abuse Regulation, read in conjunction with the e-Privacy Directive and in the light of Articles 7, 8 and 11 of the Charter, did not authorise the general and indiscriminate retention of traffic data by CSPs for a period of one year from the day on which they were recorded, for the purposes of combating market abuse offences.

The CJEU also held that EU law precluded national legislation from restricting the temporal effects of a declaration of invalidity which it was required to make, under national law, with respect to provisions of national law which, first, required CSPs to retain generally and indiscriminately traffic data and, second, allowed such data to be submitted to the competent financial authority, without prior authorisation from a court or independent administrative authority, owing to the incompatibility of those provisions with Article 15(1) of the e-Privacy Directive, read in the light of the Charter. The admissibility of evidence obtained pursuant to provisions of national law that were incompatible with EU law was, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, *inter alia*, with the principles of equivalence and effectiveness.

CJEU, judgment of 17 November 2022, *Spetsializirana prokuratura*, C-350/21, EU:C:2022:896

Facts – The case originated from a request for a preliminary ruling on the application of the e-Privacy Directive in the light of Articles 7, 8, 11 and 52 of the Charter to national legislation:

(i) imposing on CSPs to retain, in a general and indiscriminate way, all traffic and location data of the end users of those services to fight serious crime, laying down a retention period of six months, and rules intended to ensure certain safeguards;

(ii) which did not restrict access to those data to what was strictly necessary, nor provided individuals with the right to be informed where that information did not hamper criminal proceedings and with the right to a remedy against unlawful access.

Law – The CJEU confirmed its established case-law against the generalised and indiscriminate retention of traffic data and location data for the purposes of combating serious crime (see *La Quadrature du Net and Others* and *Commissioner of An Garda Síochána e.a.*, both cited above). It found that the national legislation in question did not comply with EU law, despite the existence of safeguards and a retention period of six months. As to procedural guarantees against unlawful access, the CJEU held that an authorisation issued by a national court was not in itself sufficient to ensure the effective protection of data subjects against the risks of abuse and unlawful access to data concerning them where, as in the present case, the national legislation at issue provided that such authorisation was granted solely on the basis of a request made by the national authorities responsible for criminal investigations, without the persons concerned having been heard and, consequently, without the court competent to issue such authorisation having been able to take account of any objections on the part of those persons.

ECtHR, *Škoberne v. Slovenia*, no. 19920/20, 15 February 2024

Facts – The applicant's traffic and location data – which were retained by CSPs for a period of fourteen months as part of a systemic measure – were obtained by law-enforcement authorities pursuant to court orders that were based on grounds for suspicion that the applicant had been involved in bribery. The case concerns the compatibility with Article 8 of the ECHR of legislation permitting the retention of his telecommunication data and their use by the authorities in the proceedings against him.

Law – In assessing whether the data retention regime was necessary in a democratic society, the ECtHR considered (i) the level of interference; (ii) the breadth of the margin of appreciation and (iii) whether a "fair balance" had been struck.

As to (i), the ECtHR distinguished the case from *Breyer*, cited above, noting that in the present instance the interference was more severe, as it extended to communications data.

As to (ii), the ECtHR relied on its previous case-law to reiterate that the fight against crime, upholding public safety and the protection of citizens constitute "pressing social needs" and that national authorities enjoy a certain margin of appreciation when choosing the means to achieve such a legitimate aim. However, the margin would tend to be narrower where – as in the instant case – the right at stake was crucial to the individual's effective enjoyment of intimate or key rights or where the interference was far-reaching.

As to (iii), the ECtHR considered that the safeguards applicable to the general retention of communications data by CSPs and its access by the authorities in individual cases should be the same, *mutatis mutandis*, as those pertaining to secret surveillance.

It found that the contested legal framework contained no provisions circumscribing the scope and application of the measure in relation to that which was necessary to achieve the purposes for

which the telecommunications data was to be retained. Also relying on the CJEU judgment in the case *Digital Rights Ireland e.a.*, cited above, the ECtHR found that national law should define the scope of application of the measure in question and provide appropriate procedures for ordering and/or reviewing it with a view to keeping it within the limits of what is necessary. The mere limitation of the retention to fourteen months could not undermine this conclusion. The ECtHR also considered that the fact that the retention regime was declared invalid by the CJEU and the Constitutional Court after the data in question had been accessed could not be taken to mean that it had complied with Article 8 at the material time.

The ECtHR further noted that despite the applicant having clearly argued that his communications data had been retained in breach of his privacy rights, the domestic courts limited their assessment almost exclusively to the grounds on which the judicial orders had authorised access to the retained data – even though those grounds had not been challenged by the applicant. The ECtHR emphasised that even though the access to his data was accompanied by certain safeguards (such as judicial oversight), these safeguards, while being among the criteria that had to be met, were not in themselves sufficient to render the retention regime compliant with Article 8 of the ECHR. It also relied on the CJEU judgment *SpaceNet and Telekom Deutschland*, cited above.

As to the acquisition and use of the applicant's data in the domestic proceedings, relying on the CJEU judgment *Commissioner of An Garda Síochána e.a.*, cited above, the ECtHR considered that when the retention of communications data is found to violate Article 8 because it does not respect the "quality of law" requirement and/or the principle of proportionality, access to such data – and its subsequent processing and storage by the authorities – could not, for the same reason, comply with Article 8.

Conclusion – Violation of Article 8 of the ECHR.

ECtHR, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, nos. 72038/17 and 25237/18, 28 May 2024

Facts – The case concerned the compatibility with Article 8 of the Polish secret surveillance regime governing storage and processing of communications data[25]. The applicants did not complain that they had in fact been placed under surveillance but of the risk of being subjected to such measures.

The applicants complained that the system of retention and subsequent accessing of communications data (traffic and location data and data related to Internet searches) did not meet the requirements of Article 8 of the ECHR.

Law – Relying on *Ekimdzhiev*, cited above, the ECtHR considered that retention and subsequent accessing of communications data amounted to separate interferences with Article 8 and that the general retention of communications data by CSPs and its access by the authorities in individual cases had to be accompanied, *mutatis mutandis*, by the same safeguards as secret surveillance.

The ECtHR distinguished the case from *Ekimdzhiev*, cited above, noting that the contested regime allowed national authorities to have permanent, direct and unlimited access to communication data, without the CSPs even knowing about it and without any intervention on their part. The interferences at stake were deemed very serious. Moreover, while *Ekimdzhiev*, cited above,

[25] The applicants also complained under the same provision about operational control in the context of police activities and secret surveillance measures carried out in the context of the fight against terrorism, by means of techniques including eavesdropping, recording the content of telephone conversations or correspondence carried out *via* telecommunications and digital communications networks. This part of the judgment will not be analysed since the contested system allowing targeted surveillance measures falls outside the scope of this factsheet.

concerned a regime for the retention of communications data similar to that at issue in the present case, the ECtHR had not ruled on whether the regime in question as such complied with the requirements of Article 8, but had rather focused on the guarantees relating to access and storage of the collected data.

Relying also on the case-law of the CJEU (*Digital Rights Ireland e.a*, *Privacy International*, *Commissioner of An Garda Síochána e.a.* and *La Quadrature du Net and Others,* all cited above), the ECtHR found that the contested regime imposed a generalised and undifferentiated retention of communications data of all users of communications services, affecting persons that were not, even indirectly, in a situation likely to give rise to criminal proceedings. Moreover, that regime gave police and intelligence services access for any purpose relevant to the performance of their respective statutory duties. Under these circumstances, the safeguards against possible abuse, including *ex post facto* judicial review, were insufficient to bring the regime in question into line with the requirements of Article 8.

Conclusion – Violation of Article 8 of the ECHR as to the system of retention and accessing of communications data.

B.3. Content of communications

ECtHR, *Podchasov v. Russia*, no. 33696/19, 13 February 2024

Facts – The applicant, a user of Telegram, complained about the compatibility with Article 8 of the ECHR of the statutory requirement for "Internet communication organisers" (ICO) to store all communications data for a duration of one year and the contents of all communications for a duration of six months, and to submit those data to law-enforcement authorities or security services in circumstances specified by law, together with information necessary to decrypt electronic messages if they were encrypted.

Law – The ECtHR relied on its previous case-law (*Breyer, Ekimdzhiev* and *Roman Zakharov* [GC], all cited above), to find that the continuous storage of the applicant's Internet communications and related communications data by Telegram and the authorities' potential access to these data amounted to interference with the applicant's Article 8 rights. As to the obligation imposed on Telegram to provide the authorities with encryption keys to enable them to decrypt end-to-end encrypted communications, the ECtHR accepted the applicant's argument that it was technically impossible to provide the authorities with encryption keys associated with specific users of Telegram without affecting all users of their services. The ECtHR accordingly accepted that the applicant was affected also by that legal provision.

The ECtHR found that although the case fell to be examined primarily from the standpoint of the storage of the applicant's personal data (similarly as in *Breyer* and *Ekimdzhiev*, cited above), it had also to be considered, where appropriate, in the light of its case-law on secret surveillance (*Roman Zakharov* [GC], *Big Brother Watch* [GC], cited above).

As to the storage of Internet communications and communications data, the ECtHR stressed the extensive breadth of the data retention imposed by the contested legislation, noting that it included the contents of all Internet communications and related communications affecting all users of Internet communications, even in the absence of a reasonable suspicion of involvement in criminal activities or activities endangering national security, or of any other reasons to believe that retention of data may contribute to fighting serious crime or protecting national security and without any circumscription of the scope of the measure in terms of territorial or temporal application or categories of persons liable to have their personal data stored. It found that the interference was exceptionally wide-ranging and serious.

As to the potential access to the stored data for the purposes of targeted secret surveillance, the ECtHR found that law enforcement authorities were not required under domestic law to show the judicial authorisation to the CSPs before obtaining access to a person's communications. Moreover, ICOs were required to install equipment giving the security services direct access to the data stored so that they had the technical means to circumvent the authorisation procedure and access stored Internet communications and communications data without obtaining prior judicial authorisation. The ECtHR also reiterated its findings, concerning lack of adequate and sufficient safeguards against abuse, in *Roman Zakharov* [GC], cited above, where the same legal regime was examined in the context of interceptions of mobile telephone communications.

Finally, as to the statutory requirement to decrypt communications, the ECtHR found it disproportionate to the legitimate aims pursued, since while it accepted that encryption could also be used by criminals, the contested provision risked weakening the encryption mechanism for all users.

Conclusion – Violation of Article 8 of the ECHR.