International Journal of Intelligence and CounterIntelligence

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ujic20

European Union Law Restraints on Intelligence Activities

Iain Cameron

To cite this article: Iain Cameron (2020) European Union Law Restraints on Intelligence Activities, International Journal of Intelligence and CounterIntelligence, 33:3, 452-463, DOI: 10.1080/08850607.2020.1754665

To link to this article: https://doi.org/10.1080/08850607.2020.1754665

International Journal of Intelligence and CounterIntelligence, 33: 452–463, 2020
ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2020.1754665

IAIN CAMERON

European Union Law Restraints on Intelligence Activities

Lawyers focus on the regulation and control of activities. Intelligence was previously regarded as something that was on, or even beyond, the boundaries of what should be regulated and controlled by means of the law. If statutory law (i.e., acts passed by parliament) governed intelligence agencies at all, then the provisions tended to be in very general terms, leaving considerable interpretative scope to the agencies themselves (or, at least their taskmasters, the relevant government departments). To the extent that statutory rules applied, this tended to be for the activities of internal security agencies, on the basis that it was these agencies that could impact the rights of citizens. Outside of the state, what governed was the much weaker rules of international law, or, nothing at all, the law of the jungle. This is no longer the case today, even if the rules that apply to extraterritorial intelligence

Iain Cameron is Professor in Public International Law at the University of Uppsala in Sweden, where he teaches international law and constitutional law. He is a member of the Royal Swedish Academy of Sciences. His research interests lie in human rights/civil liberties and police/security issues. Since 2005 he has been one of the two Swedish members of the Commission on Democracy through Law (Venice Commission), the advisory body of the Council of Europe on constitutional law and international law. The author can be contacted at Iain.Cameron@jur.uu.se

activities are still, generally speaking, less rigorous than those that apply to internal intelligence activities.

There has been a general trend in democratic states, beginning in most cases with the end of the Cold War, for external and internal intelligence agencies to "come out from the shadows" and for their activities to be increasingly regulated by statutory law rather than purely government decrees or (secret) internal instructions. External oversight has also become more common. This is a welcome development. The threats facing our states mean that we obviously need to have intelligence agencies, and, for them to work effectively, we need to give them considerable powers. There is thus a corresponding need to subject these agencies to strong regulation and provide for strong safeguards against abuse of power. Accountability for power and safeguards against its abuse are not optional extras in the Rechtsstaat, but essential to the legitimacy of the power exercised.

Intelligence agencies in European states have thus gradually adapted to there being more "actors" to which they have to answer. It is no longer simply the government ministries that are their overseers and task-givers, but also the legislature, which provides for a framework for their activities and places limits on their powers, the courts that set limits on their coercive powers, when these encroach on individuals' rights, and, as noted above, various types of oversight body, expert, parliamentary, or hybrid. And the public are much more active: people no longer trust the experts—although, with social media, everyone seems to regard themselves as an expert. However, despite the process of European integration, national security has still been a *national* responsibility. How this is organized, run, and overseen is thus a matter primarily for each European state. For intelligence agencies, the emergence of European actors that are capable of seriously influencing matters that are central for them, in particular their powers of surveillance, is something relatively new.

European Union (EU) law is complicated, but basically consists of the treaty rules (primary EU law), secondary law—regulations and directives adopted by the EU legislator (which is usually the Council of the EU, acting together with the European Parliament [EP]), and agreements that the EU concludes with third states. Among the important provisions of primary law is the EU Charter of Fundamental Rights (EUCFR), which, after the Treaty of Lisbon entered into force, became binding for EU institutions, and also for EU member states when they act within the scope of EU law.

EU law has supremacy over national law, and can have direct effect in member states. The process of negotiating EU secondary law often results in compromises, which in turn means vague or ambiguous provisions. The judicial body established to oversee EU law, the Court of Justice of the EU (CJEU), can thus exercise considerable power because it has the final word

on what obligations states have under EU law. Most of the cases decided by the CJEU are in the form of "preliminary rulings." These are answers to queries regarding the interpretation, application, or validity of EU law that have been posed by national courts. The CJEU decides the issue of EU law, laying down (usually quite abstract) findings that are meant to serve as interpretative guidelines for national courts in all EU states. The case then "returns" to the national court that determines the factual issue. The CJEU can choose to leave much, or little, discretion to the national court in how it applies the principles it has clarified. Any court in an EU state may ask for a preliminary ruling, and a lower court does not have to seek permission from a higher court before making a referral. Under Article 267 Treaty on the Functioning of the European Union (TFEU), a court from which there is no appeal and that has a case where EU law is central to its outcome, is obliged to ask for a preliminary ruling.

There is another set of rules applying to intelligence activities at the European level, although space constraints mean that it can only be dealt with very briefly, namely the European Convention on Human Rights (ECHR). This treaty has been made part of the national law of all European states and is thus frequently applied by national courts. The relatively vague provisions of the ECHR are concretized by judgments of the European Court of Human Rights (ECtHR) which has the final word on what obligations states have under the treaty. There are a number of important judgments from the ECtHR dealing with different aspects of intelligence activity, particularly surveillance. The ECHR is also a part of EU law, by virtue of Article 6 Treaty on European Union (TEU). As there is a considerable overlap between the rights protected in the EUCFR and in the ECHR, these overlapping rights are supposed to be interpreted by the CJEU in the same way as the ECtHR interprets the ECtHR.[1] However, as will become apparent, the CJEU regards the ECHR as a minimum standard from which it can diverge.

PRIMARY EU LAW

The EU, simply put, is a framework treaty. It sets out purposes and establishes institutions to achieve these purposes by means of the adoption of legislation. The EU only exercises competences that have been expressly or impliedly delegated to the EU by the member states (Article 5 TEU). However, so long and so far as the EU exercises its competence, the member states are excluded from legislative action (Article 2(2), TFEU). Article 4 of the TEU provides that "the Union shall respect the … Member States' essential State functions, including safeguarding national security … national security remains the sole responsibility of each Member State."

However, it is clear that the EU does have competence to adopt measures in the area of *internal* security. Title V TFEU provides for an area of freedom, security, and justice (AFSJ), and there are specific articles providing for competence to adopt legislation on police cooperation (Article 87 TFEU) and, in relation to material criminal law, as regards organized crime and terrorism (Article 88 TFEU). Title V bestows shared, not exclusive, competence, meaning that the member states can continue to legislate in these areas, as long as they do not violate existing EU rules. These competences depend on unanimity in the Council but they are not a priori excluded from EU policy.

Even the AFSJ contains a national security clause, Article 72 TFEU, which provides that the EU's competence in justice and security "shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security."

There are different approaches in doctrine to interpretation of these two clauses, mainly in the context of what sort of measures can be covered by the AFSJ. For example, Peers advocates a narrow interpretation of Articles 4(2) TEU and Article 72 TFEU. He does not consider these provisions to be exclusions, either of legislative competence or of CJEU jurisdiction.[2] Others, such as Müller-Graff, take the opposite approach, considering that these provisions guard the member states' *domaine reservée*.[3]

There are other provisions of the treaties that allow member states to invoke security reasons to derogate from their obligations (e.g., the "public security" clause limiting free movement of goods in Article 36 TFEU).[4]

Another part of primary law is the EUCFR. Article 7 of this provides for the right to private and family life, home and communications. Article 8 provides for the right to data protection. Unlike the equivalent provision in the ECHR (Article 8) there is no specific "national security" limitation to these rights. Instead, there is a general limitation clause in Article 52(1) EUCFR that includes national security considerations.

The EU Commission, the European Parliament, and the CJEU have a strong institutional interest in defining national security narrowly, so as to increase their own role in the area. The member states for their part have an institutional interest in keeping the European institutions out of national security. At the same time, the member states cannot avoid the growing European interdependence in security matters.

This struggle of competence has so far mainly manifested itself in disputes over the Terrorist Finance Tracking Programme[5] as regards the question of Passenger Name Records (PNR)[6] and particularly as regards the obligation on telecommunications providers to retain telephony and Internet metadata.

DATA RETENTION CASES

In most countries, metadata had previously been regarded as less sensitive from the perspective of personal integrity, as compared to the content of a communication. However, the digital footprint we leave means that a great deal of personal information is now obtainable by metadata, and machine analysis of communications patterns. The disquiet shown by the public and nongovernmental organizations (NGOs) about surveillance in many states was compounded in 2013 by the extensive leaking of documents by former National Security Agency contractor Edward Snowden, which revealed the existence of very large surveillance programs, both of metadata and Internet-borne content data (e-mails, etc.). The perspective of intelligence agencies is different: they know they have limited resources, they consider that they are not accessing these data unnecessarily, and they are acutely aware about all the data to which they do not have access.

Security and intelligence agencies can obtain these data in bulk themselves; for example, by means of an obligation placed on telecommunications providers to channel communications through certain communications nodes, where it (or rather, parts of it) can be copied. This is a method used by signals intelligence agencies for exterritorial communications. Alternatively, an obligation can be placed on telecommunications providers in a particular state (and, now, other Internet platforms such as messaging services)[7] to retain these data for certain periods. These data can then be accessed for the purposes of law enforcement and national security. As regards the second method, it made sense to use the EU internal market to agree on common legal rules and technical standards for data retention. However, it later became clear that a price would be exacted for this.

In the Digital Rights case,[8] the CJEU annulled the EU directive,[9] which provided that states were required to provide for a duty on telecommunications providers to retain metadata for a period of six months (minimum) and two years (maximum) and make these data available for the investigation of serious crime. The directive had left it to states to put safeguards in place to regulate access to metadata and prevent abuse of power. The implications of this case were not entirely clear: some states interpreted it as requiring them to provide for increased safeguards, such as judicial or quasi-judicial authorization. Others considered that their existing system of regulation was sufficient. Digital Rights was followed by the Schrems case,[10] where the CJEU found that states were not free to transfer data to third states unless these third states provided for data protection standards equivalent to those applying within the EU.

The third case, Tele2/Watson,[11] concerned the e-privacy directive, 2002/58.[12] This lays down rules applicable to the processing of traffic and location data generated by using electronic communications services, and the

anonymization or deletion of these data, while making certain exceptions for the purposes of law enforcement and national security. The CJEU clarified its earlier ruling in Digital Rights. It found, on a textual interpretation of the directive, that the safeguards on retention and access that must exist were a matter of EU law (even though these had deliberately been left to each state to decide on). It required states to make access to metadata contingent on prior approval by a court or quasi-judicial expert body. Such a ruling is understandable, bearing in mind the public disquiet about the surveillance potential of metadata. However, accessing metadata is a measure often taken at the beginning of an investigation, when there is, naturally enough, not much to go on. Thus, how such a prior authorization will actually work in practice will be dependent on how offenses are formulated in national law (including inchoate offenses), as well as the national police/intelligence and judicial culture (e.g., how the evidential threshold is placed).

The CJEU also stated that persons affected must be notified "as soon as this is no longer liable to jeopardize the investigations being undertaken by those authorities," as this is necessary for these persons to be able to exercise their EU right to a legal remedy. There is also a lot of doubt as to how this can work.

However, much more controversial is the CJEU's ruling in the same case that "general" and "indiscriminate" data retention is not compatible with the EUCFR. The argument for general retention is that the police and intelligence agencies very often do not know who is involved in terrorism, espionage, or other serious crime. A general duty of retention permits the police or intelligence agency to go "back in time." Metadata analysis can reveal the structures, hierarchies, and communication patterns involved—which is all the more useful bearing in mind the difficulties now involved in obtaining content data, because of difficult, or impossible, to break encryption. Removing a general duty of retention means that these historical data are simply not there any more.

The CJEU considers that the *targeted* retention of traffic and location data, for the purpose of fighting serious crime, can be acceptable as a preventive measure under the following conditions. There must be "clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse."[13] An indirect link to serious crime can suffice, as long as this can "contribute in one way or another to fighting serious crime or to preventing a serious risk to public security" but "such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected."[14] Nonetheless, it stated that "such limits may be set by using a geographical

criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences."[15]

The CJEU clearly meant this last point to be a concession to the needs of the police and intelligence agencies, but it is doubtful how useful this will be in practice. Bearing in mind the number of companies providing telecommunications and Internet services in most states, it would be impossible to keep such geographic retention orders confidential.

If the criteria formulated by the CJEU (clear and precise rules, etc.) were applied to the *accessing* of retained data, this would not be a problem for states that already regulate and oversee their security and intelligence agencies adequately. But the criteria apply to retention rendering general retention unlawful, even for a relatively short period. The judgment thus deliberately throws a large spanner into the work of the police and security and intelligence agencies. The CJEU clearly considers this is justified in the interests of protecting human rights. The "Snowden revelations" seem to have strongly influenced the judges. There is, of course, cause for concern in many EU states where intelligence agencies are poorly regulated and subject to only limited (or only formal) oversight.[16] However, the CJEU has no power to order individual member states to take reform measures.[17] Instead, it has used the power it has to interpret the law in one area—telecommunications and data protection—to try to remove an investigative and intelligence-gathering tool that the legislatures in all EU states have deemed essential. The CJEU, in my view, displays a disturbing indifference toward understanding the technology involved (not only its surveillance potential, which is admittedly great, but its limitations in practice). Nor does the CJEU—which is interested in a uniform EU solution—pay attention to how differently police and intelligence agencies in EU states are regulated and how differently they actually use surveillance technology.

PENDING CASES

All three of the above cases illustrate how telecommunications corporations, but also human rights interest groups (nongovernmental organizations), have been provided with a potent weapon to challenge, in a supranational court, national laws that have been agreed on in democratically elected legislatures. This should not be seen as a surprise: it has been part of the point of the EU from the beginning. In fact, the judgments fit into a familiar pattern of CJEU removal of regulatory burdens on companies in the interests of market integration.

There is also a pattern in that a judgment spawns another judgment. There are, at the time of writing (March 2020), four pending requests for preliminary rulings: from the Belgian Constitutional Court,[18] the French

Conseil d'État,[19] and the UK specialist court established to hear cases concerning security matters, the Investigatory Powers Tribunal (IPT).[20] The issue before the pending French and UK cases is, simply put, do the principles laid down by the CJEU in Tele2/Watson for the investigation of serious crime, including terrorism, also apply to surveillance and surveillance systems designed to protect national security?

The cases have not yet been decided. However, Advocate-General Campos Sánchez-Bordona delivered his opinion in these cases on 15 January 2020. He gives very limited effect to Article 4(2) TEU, and instead largely repeats the CJEU's textual interpretations of directive 2002/58. He draws a distinction between the "activities" of security and intelligence agencies to protect national security and legislation enacted for the protection of national security that imposes obligations on individuals that affects their EU rights.[21] The former fall outside of the scope of EU law, the latter do not. His main reason is that otherwise the simple invocation of national security would allow a state to undermine individuals' rights under the directive and the EUCFR.[22] He discusses briefly the question of whether national security surveillance requires a different set of safeguards for individuals compared to surveillance for the purpose of criminal investigation but ends up by stating that the CJEU's standards might be able to be "qualified" but that their "essential content should be endorsed."[23] Arguments about the impracticality of methods other than general retention are dismissed: the issue is regarded not as a matter of practical effectiveness but the rule of law.[24]

The advocate-general's opinion is not binding on the CJEU and it remains to be seen if the court will follow it. If the CJEU takes the same approach then it in practice means paying little attention to the limit on competence set out in Article 4(2) TEU as regards interpreting adopted legislation (although it can still have significance when the member states negotiate new legislation).

The distinction the advocate-general draws between legislation and activities is of doubtful value. The real issue is rather how satisfactory the system of regulation is overall, including the safeguards provided, not how the security and intelligence agencies physically get hold of the data. However, it does provide for an opening for a state wishing to avoid the application of the prohibition of general retention. If a state took ownership over (nationalized) part of its telecommunications infrastructure (e.g., the Internet exchange points), and gave its security and intelligence agencies access to the data flows, when they pass through the exchanges, then this would mean that the state would be "using its own resources." Of course, as far as signals intelligence is concerned, it is still open to the state to argue that it does not, in fact, engage in general and indiscriminate retention, because

the external Internet traffic is subject to filters to remove much of it. But it is hard to see the CJEU accepting this.

A BETTER DIALOG WITH THE CJEU?

For security and intelligence agencies the CJEU is a new, and presumably unwelcome, actor that has appeared on the scene. One question that arises for such agencies is how to engage in a dialog with it. The primary partners for dialog with the CJEU are not national administrative agencies but the national courts. They initially frame the issues for the CJEU's appraisal and they are the ones that receive the case back for implementation. For example, the IPT made it very clear in the questions that it posed that it considered that the Tele2/Watson standards should not be applied to national security surveillance.

The dialog between the national courts and the CJEU works relatively well most of the time, but there are occasional frictions. Attempts have been made, particularly by constitutional courts in several EU states, to get the CJEU to accept that the protection of human rights in the EU is a multilevel system of protection with responsibility to be shared between the national courts, the ECtHR, and the CJEU.[25] The implication is that the CJEU in particular should show a degree of restraint before it imposes a one size fits all model. Sometimes this argument seems to sway the CJEU and sometimes not. The CJEU is used to states trying to avoid or minimize their obligations under the internal market. The fact that a case "returns" to the national court for a final determination of the facts usually means leaving the national court a degree of discretion in how it adapts EU principles to its own legal system. However, the central finding of Tele2/Watson is that general retention is forbidden. The discretion left here is minimal.

Another method of dialog is when the respondent state explains how its law and practice works in written and oral proceedings before the court. The written proceedings are crucial. Here security and intelligence agencies have to brief their ministries fully on how the technology works (and does not work), how the system of regulation is constructed and how the safeguards are working in practice. The oral proceedings are of limited use to convey such important information. These are very short. The CJEU has already decided how the issues are to be framed, and what further information it needs (if it considers it needs any at all).[26] As the CJEU's ruling will have a general effect in all EU states, other EU states are also entitled to intervene in the case to explain their laws and practices. Many EU states intervened in all of the above cases. At the risk of some simplification, none of them, and none of the respondent states, considered that general retention should be prohibited by EU law.

Some intelligence agencies might think that, if only there was a method of supplying the CJEU with secret information, then it might be easier to convince. There is a mechanism to review secret evidence submitted by member states in the Council of the EU.[27] This is designed for review of decisions in the EU General Court (the EU court of first instance) on EU sanctions. However, this mechanism has so far not been used. I am skeptical of the value of this mechanism, which is anyway meant for contentious proceedings rather than preliminary rulings.

CONCLUSION

Although I have not had space to analyze the case law of the other European court, the ECtHR, it can be said that it does not follow the rigid approach of the CJEU. The ECtHR in the recent cases of *Centrum för Rättvisa v. Sweden*,[28] and *Big Brother Watch and others v. UK*[29] accepted that the choice of whether or not to engage in bulk collection of communications data is a matter within states' margin of appreciation.[30] Focus on these cases (which have both been appealed to the Grand Chamber of the ECtHR) has correctly been on the regulation and safeguards applying in these two states' systems of signals intelligence. The ECtHR has explicitly accepted the realities of differential (mis)trust in Europe. The ECtHR has stated that it will henceforth apply two levels of scrutiny to allegations of abuse of powers of secret surveillance: where the national system of remedies ostensibly provided to individuals is not working in practice, the ECtHR will regard the menace of surveillance as sufficient to give an applicant standing.[31] Thus, the issue of whether or not a person is a victim is linked to how well the oversight and remedies system appears to be working. Nor does the ECtHR insist on "one size fitting all."

There is clearly a serious schism in the "worldview" of NGOs and security and intelligence agencies in democratic states. One way of looking at the CJEU's case law is that it has adopted the worldview of NGOs. The basic message in the article is that the CJEU has entered the stage as an important regulator of intelligence activities, and that European intelligence agencies have to find ways of coping with this.

REFERENCES

1 EUCFR, Article 52(3).
2 Steve Peers, *EU Justice and Home Affairs Law: vol II, EU Criminal Law, Policing and Civil Law* (Oxford: Oxford University Press, 2016), p. 54ff.
3 Peter-Christian Müller-Graff, "The Legal Bases of the Third Pillar and its Position in the Framework of the Union Treaty," *Common Market Law Review*, Vol. 31 (January 1994), pp. 493–510.

[4] See, for example, Case C-300/11, ZZ v Secretary of State for the Home Department. EU:C:2013:363. If an extensive approach is taken to the concept of "public security" as including combating terrorism, then relatively few activities are left to be covered by the national security exception. This case is admittedly not about defining national security for the purpose of the delineation of competences, but it does give an indication of how the CJEU is likely to approach this issue too.

[5] https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/tftp_en (accessed 20 March 2020).

[6] The EP referred the draft EU-Canada PNR agreement to the CJEU, which laid down certain data processing standards with which the agreement must comply, to be compatible with the EUCFR Opinion 1/17, EU:C:2017:592.

[7] The new definition of an "electronic communication service" in Article 2 (4) of the European Electronic Communication Code includes "interpersonal communications services," such as instant messaging (e.g., Facebook messenger, WhatsApp) and online chat. Such services will fall within the scope of Directive 2002/58 from December 2020.

[8] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland (Grand Chamber), EU:C:2014:238.

[9] OJ L. 2006, 105/54.

[10] Case C-362/14, Maximillian Schrems v Data Protection Commissioner (Grand Chamber), EU:C:2015:65.

[11] Joined Cases C 203/15 and C 698/15, Tele2 Sverige AB (C 203/15) v Post- och telestyrelsen, and Secretary of State for the Home Department (C 698/15) v Tom Watson, Peter Brice and Geoffrey Lewis, (Grand Chamber) EU:C:2016:970. For analysis, see Iain Cameron, "Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson," *Common Market Law Review*, Vol. 54 (October 2017), pp. 1467–1496.

[12] OJ L 2002, 201/37.

[13] Tele2/Watson, para 109.

[14] Tele2/Watson, para 110.

[15] Tele2/Watson, para 111.

[16] See, for example, the following recent judgments from the ECtHR disclosing systemic failures of regulation and oversight: *El-Masri v. Macedonia* (Grand Chamber), No. 39630/09 13 December 2012; *Bucur and Toma v. Romania*, No. 40238/02, 8 January 2013; *Al Nashiri and Husayn (Abu Zubaydah) v. Poland*, Nos. 28761/11 and 7511/13, 24 July 2014; *Nasr and Ghali v. Italy*, No. 44883/09, 26 February 2016; *Szabó and Vissy v. Hungary*, No. 37138/14, 12 January 2016; *Abu Zubaydah v. Lithuania*, No. 46454/11, 31 May 2018; *Al Nashiri v. Romania*, No. 33234/12, 31 May 2018.

[17] It is hardly a consolation to intelligence agencies to hear that the CJEU has legitimacy problems in other areas too. For discussions see, for example, G. Davies, "Democracy and Legitimacy in the Shadow of Purposive Competence," *European Law Journal*, Vol. 21, No. 1 (2015), pp. 2–22.

[18] Case C 520/18, Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de

l'Homme ASBL, VZ, WY, XX v. Conseil des ministers. The Belgian court asks the question whether criteria set out by the CJEU are to be applied cumulatively (a question already answered in Tele2/Watson) and whether evidence obtained under national legislation later ruled not to comply with EU law can nonetheless be used in investigations or criminal proceedings.

[19] Joined cases C 511/18 and C 512/18, La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs,, Igwan.net v. Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées.

[20] Case C 623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service.

[21] Opinion on Joined cases C 511/18 and C 512/18, para. 73.

[22] *Ibid*., para. 74. If this approach is followed, there is potential for future case law in other areas, e.g., the national security exclusions in Directive (EU) 2016/680 on data processing for law enforcement, 4.5.2016, OJ L 119/89, are framed in similar terms.

[23] *Ibid*., para. 134.

[24] *Ibid*., para. 135.

[25] See, for example, Andreas Voßkuhle, "Multilevel Cooperation of the European Constitutional Courts: Der Europäische Verfassungsgerichtsverbund," *European Constitutional Law Review*, Vol. 6 (2010), pp. 175–198.

[26] The CJEU asked the European Data Protection Supervisor (EDPS) to give evidence in the above pending cases; see Pleading notes of the EDPS, https://edps.europa.eu/sites/edp/files/publication/19-09-11_data_retention_pleading_en.pdf (accessed 19 March 2020).

[27] See Article 105 of the Rules of Procedure of the General Court, 4.3.2015 OJ L 105/1, Decision (EU) 2016/2386 of the Court of Justice of 20 September 2016 concerning the security rules applicable to information or material produced before the General Court in accordance with Article 105 of its Rules of Procedure, 24.12.2016, OJ L 355/5.

[28] No. 35252/08 19 June 2018.

[29] No. 58170/13, 13 September 2018.

[30] Big Brother Watch, para. 314, Centrum för Rättvisa, para. 112.

[31] Roman Zakharov v. Russia [GC] No. 47143/06, 4 December 2015, para. 171.