

Takeaways about the CJEU rulings “Privacy International” and “La Quadrature du Net, French Data Network et al.”

EU’s top court paves the way for major reforms of European surveillance laws. What do the rulings of 6 Oct. 2020 mean?

On October 6, 2020, the grand chamber of the Court of justice (CJEU) – the European Union’s highest court – ruled that the following measures are contrary to EU law:

- General one year data retention laws of Belgium and France;
- Real-time and automated analysis and collection of the whole traffic and location data in the way provided by France’s “Intelligence Act 2015”;
- General transmission of traffic and location data to the security and intelligence agencies of the UK’s “Investigatory Powers Act 2016”.

Also read: Our Press Release on the judgments, on: <https://datarights.ngo>

1 What is at stake?

When you communicate by phone or via the Internet and when you browse online, considerable amounts of data are generated automatically. This information is often referred to as “metadata”. It indicates ‘where’, ‘when’ and ‘who’ communicates with whom, and may also include information about the type of online content consulted (e.g. URLs). Metadata is ready to be analysed by computers on a massive scale and enables the profiling of individuals. It may reveal sensitive information, sometimes more than the actual content of communications. In particular, metadata “*facilitate[s] the almost instantaneous cataloguing of entire populations, something which the content of communications does not.*”¹

Under Belgium, France and UK laws, communications service providers would be required to retain this metadata for one year, or to forward this data ‘in bulk’ for intelligence and investigation purposes of the State.

Despite their different national implementations, these data retention and transmission schemes cover *all users* of electronic communications (individuals, businesses, judges, attorneys, whistleblowers, etc.) and apply *at all times*. There is no need for any suspicion, or any objective criteria linked to any investigation. There is no need for any court approval. They are systematic and preventive, i.e. ‘just in case’ investigators or intelligence agencies might ever need them.

2 What was the purpose of the legal challenges?

The legal challenges that led to the rulings of 6 October 2020 aim to strike down the general data retention laws and the surveillance rationale behind them, because these laws are fundamentally intrusive and prone to abuse by States.

¹Opinion of Advocate General Saugmandsgaard Øe of 19 July 2016 in *Tele2/Sverige*, para. 259

Why do these laws even exist in the first place? The rationale since 2006 in Europe², and in particular in France since 2001³, could be stated as follows: ‘Because it is impossible to know in advance who is likely to be a threat or a criminal, we ought to keep data to track the behaviours and communications of everyone.’

However, this way of thinking is far from harmless, and the categories of data at stake are far from innocuous. In the words of the CJEU:

“[T]raffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health [...]. Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.” (par. 117 of joint Cases C-511/18, C-512/18 and C-520/18)

From a political standpoint, our legal actions challenge the state of ‘general suspicion’ or ‘State paranoia’ that has led to the development of ‘mass surveillance’ techniques. Opposite to this, our stance is simple: intrusive surveillance measures should not be the norm, they should be the exception. Surveillance measures should be carried out only where strictly necessary, subject to safeguards and in a manner holding authorities accountable.

From a legal standpoint, the rulings are essentially about (1) whether national security purposes are exempted from EU law and (2) to what extent EU law prohibits or allows the retention, real-time automated analysis and/or collection, and/or transmission of electronic communications data for public authorities.

3 Is it a victory for privacy or for security?

This is a victory for both.

Both the right to privacy and confidentiality of communications, and the right to security, contribute to a democratic society. That is why, under European human rights laws, States have both an obligation to protect individuals against interference in their home and communications, as well as to maintain public security.

²In 2006, the European Parliament and the European Council adopted the Data Retention Directive

³In 2001, France’s Parliament adopted the Everyday Security Act now codified in Sec. L34-1 of the French Code of Electronic Communications and Posts

However, one objective should not completely overcome the other. Surveillance measures are allowed, but only as far as they are “necessary in a democratic society” and remain proportionate. That is why the Court strikes a balance between, on the one hand, the right to privacy and confidentiality of communications, the right to an effective remedy, and freedom of expression online, and on the other hand, the public interests to preserve national security, public security and the fight against criminality.

The rulings of 6 October 2020 are a victory for the rights to privacy and confidentiality of communications, because they:

- Confirm that national security services are not above the law - in particular, it means that national security measures impacting communications service providers are subject to EU law. In other words, surveillance and investigative measures shall not escape the scope of EU law for the sole reason that they pursue national security interests;
- Prohibit the general, indiscriminate retention of traffic and location data as preventive measures. Thus, the rationale that data ought to be kept for the State ‘just in case’ is ruled incompatible with a democratic society.

This, is no less of a major victory.

4 Are these rulings a surprise?

No. The rulings of 6 October 2020 are not a change of case law. They are the direct continuity of previous cases where the grand chamber of the CJEU – the highest jurisdiction for European law – already ruled that European States’ security logic was at odds with the protection of European fundamental rights and freedoms.

- 2014: in *Digital Rights* (cases coming from Ireland and Austria), the CJEU annulled Directive 2006/24 which provided communications data retention rules at the European level.
- 2015: in *Schrems I*, the CJEU ruled the *Safe Harbour* agreement invalid because US laws on access to communications data, as highlighted by the Snowden leaks, were incompatible with the level of protection of rights under EU law (as confirmed in *Schrems II* in July 2020 with regard to the *Privacy Shield* arrangement).
- 2016: in *Tele2/Watson*, the CJEU ruled that Sweden and UK laws on data retention and data access were incompatible with the ePrivacy Directive 2002/58 read in light of the Charter of fundamental rights. In that ruling, the Court already held that national security purposes were not exempted from complying with EU law.
- 2017: in the *Canada PNR Opinion*, the CJEU declared incompatible with EU law the envisaged agreement negotiated between Canada and the European Commission for transfers of data in relation to the fight against terrorism and serious transnational crime

Since 2014 and even more so since 2016, it is undeniably clear that the data retention laws of Belgium, France and many other EU Member States are not compatible with EU law. Same goes for France's "Intelligence Act 2015" and the UK's "Investigatory Powers Act 2016".

So these rulings hardly come as a surprise. The need to change European States' surveillance laws has been the 'elephant in the room' since 2014.

Yet, as mentioned, while the CJEU has been constant in its interpretation of the EU legal framework — many European States have been constant in their inability to engage substantial reforms; whether at EU or national level. Many representatives justified the lack of reform with false legal arguments — the main one being that national security was out of reach of EU law. The rulings of 6 October 2020 finally and unequivocally put an end to this invalid argument, hopefully once and for all.

5 Are the judges on a political crusade for privacy?

Judges apply the law.

They do not write it. Even more importantly, Member States of the European Union have chosen to hold themselves to strict fundamental rights they set themselves, via the Charter of fundamental rights. The CJEU based its rulings on specific provisions of EU laws, read in light of this Charter.

The divide between the level of protection of some EU laws voted in Parliament, and the wishes of national authorities to give precedence to national security over the respect of human rights, is not consistent with the law and treaties that have been negotiated and agreed at the European level.

What is more of concern is that, since 2014, many intelligence services or investigatory bodies have constantly criticised the Court judgments — claiming they were deprived of tools necessary for the fight against crime.

After six years of clear rulings from EU's top highest court, it is time that national authorities finally listen and act accordingly. To do otherwise would be a serious and concerning breach of the rule of law in Europe.

Disrespect for the rule of law — voted in Parliament and applied by judges — is a serious political concern.

6 What did the Court decide exactly?

In a nutshell, the CJEU concluded that current laws in Belgium, France and the UK, are incompatible with EU law. Reforms are necessary.

The Court clarified that:

- The law regulating confidentiality in the communications sector (ePrivacy Directive) prohibits general and indiscriminate traffic and location

data retention by electronic communications providers as preventive measures;

- This same Directive also prohibits general and indiscriminate transmission of traffic and location data to the security and intelligence agencies for the purpose of safeguarding national security;
- The General Data Protection Regulation (GDPR) prohibits general and indiscriminate retention of personal data by hosting providers, related to our activities online.

In addition to the general prohibitions above, the Court sets the conditions, limitations, and safeguards that must be put in place for surveillance laws and investigatory or intelligence measures to be compatible with EU law. Laying out these requirements is a major victory, as the Court paves the way to reforms of surveillance laws in Europe.

In particular, the Court held that:

- General and indiscriminate retention of traffic and location data by electronic communications providers, and the real-time automated analysis of traffic and location data, are allowed provided that all of the following conditions are met:
 - only for purposes of safeguarding national security;
 - upon injunction to providers (as opposed to available by default due to the law);
 - only if the Member State is confronted with a serious threat to national security, shown to be genuine and present or foreseeable (as opposed to a preventive or systematic measure ‘just in case’);
 - limited in time, which can be renewed, as strictly necessary;
 - subject to effective review of the injunction by a court or by an independent administrative authority whose decision is binding, the aim of that being that accountability for following the previous conditions in the process.
- Targeted or expedited retentions (sometimes referred to as “quick freeze”) of traffic and location data, or general retention of limited categories of personal data (e.g. IP addresses and civil identity of subscribers) are also allowed under specific conditions, limitations and safeguards, as far as strictly necessary in a democratic society. Here, the court expands on the conditions and rationale laid out in December 2016, in the *Tele2/Watson* case.
- Real-time collection of traffic and location data is allowed provided that it is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding in order to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the review must take place within a short time.

In any event, the rulings impose minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. The need for such safeguards is even bigger where personal data is subjected to automated processing.

7 What are the impacts of the judgments for France and UK surveillance laws?

7.1 Specifically for France:

Data retention laws and decrees (L34-1 and R10-13 of the French Code of Electronic Communications and Posts and Decree 2011-219) will have to be modified because data retention may not be general, indiscriminate and systematic as a preventive measure.

The Intelligence Acts of 2015 (and related decrees codified in Book 8 of the Internal Security Code) will have to be structurally changed — in particular:

- the so-called ‘black boxes’ (L851-3 and R851-5) are considered to also spy on the kind of online communications (URLs) and create substantial risks – they must be subject to the most stringent requirements of national security. Additionally, because of the inherent risks of these algorithmic surveillance measures, the Court requires more transparency;
- the list of purposes allowing intelligence measures will have to be modified to account for the distinctions made by the Court depending on the level of seriousness of intrusions into communications.

The scrutiny of intelligence measures should also undergo deep reforms. As of today, the French intelligence oversight body, the *Commission Nationale de Contrôle des Techniques de Renseignement* (CNCTR) provides non-binding opinions to the Prime Minister, it does not take binding decisions. We hope that the necessary reforms will also be an opportunity to discuss the means allocated. Historically, the CNCTR (former CNCIS) has known times where it was underresourced, by its own admission, which could in turn increase the quality of its investigations and management of data subjects rights.

Reforms in the Code of criminal procedure for related techniques may also be expected.

More generally, to comply with the ruling, French law will have to include a notification to inform data subjects of surveillance or investigative measures, when such notification does not undermine the purposes of the measure.

This must become a requirement regarding access to traffic and location data (whether real-time or delayed access) but also with regard to automated analysis of that data that singles out individuals. To provide information when doing so no longer poses a threat to the investigation is fundamental, as the right to access a judge and obtain justice if one has been unfairly treated (right to an effective remedy) is a cornerstone of EU fundamental rights law.

A part of the case also impacts obligations to retain personal data imposed upon hosting providers, in relation to users who contribute to content online

(LCEN Art 6 II). While the legality of Decree 2011-219 is now seriously at stake, the specific impact of the ruling here is not entirely clear, and it remains to be seen how the Conseil d'État will interpret it.

7.2 Specifically for the UK:

Read Privacy International's analysis⁴ to learn more about the implications for the UK.

8 What is the impact elsewhere in Europe?

Many Member States in Europe have laws requiring general data retention: see this study from 2017 by Privacy International⁵. The rulings of 6 October 2020 have an impact within all the European Union.

9 What was the involvement of Data Rights and what are the next steps?

Data Rights was founded by people including activists who brought the challenge in France that led to the ruling of 6 October 2020, as part of their contributions with the Exegetes Amateurs⁶.

The cases will go back to national jurisdictions who sent the matters to the CJEU. In France, the case goes back to the highest administrative court (Conseil d'État). In the UK, the case goes back to the Investigatory Powers Tribunal. Privacy International will as usual keep the UK in check too.


Beside these cases, the rulings may spark reforms and discussions among lawmakers in Brussels and in every EU country. Data Rights will work to ensure the essence of the rulings is taken into account, and effective reforms are made.

⁴<https://privacyinternational.org/long-read/4206/qa-eus-top-court-rules-uk-french-and-belgian-mass-surveillance-regimes-must-respect>

⁵https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf

⁶<https://exegetes.eu.org/en/>

<https://datarights.ngo>

 @dataRights_

Data Rights is a new non-governmental organization with a mission to empower users, organisations and communities, to control their data.

