UN & CoE

January

February

8 February – In *Ben Faiza v. France* (No. 31446/12), ECtHR holds that real-time geolocation surveillance measures taken against an individual involved in drug trafficking fail to satisfy the "in accordance with the law" requirements, when the law does not indicate with sufficient clarity to what extent and how the authorities are entitled to use their discretionary power. On the other hand, the law enforcement authority's access to the applicant's telephone records is held to be compatible with Article 8 of the ECHR

13 February – In *Ivashschenko v. Russia* (No. 61064/10), ECtHR holds that the relevant customs legislation and practice on inspecting goods did not afford adequate and effective safeguards against abuse in applying the sampling procedure in respect of electronic data contained in an electronic device and was not, therefore, "in accordance with the law" under Article 8 of the ECHR

15 February – Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) (CoE) adopts 'Practical guide on the use of personal data in the police sector'

28 February – UN Special Rapporteur on the right to privacy presents his Annual Report

March

7 March – CoE Committee of Ministers adopts Recommendation CM/Rec(2018)2 to member States on the roles and responsibilities of internet intermediaries

April

24 April – In *Benedik v. Slovenia* (No. 62357/14), ECtHR holds that the Slovenian police's failure to obtain a court order to access subscriber information associated with a dynamic Internet Protocol (IP) address did not meet the convention standard of being "in accordance with the law", and therefore finds a violation of Article 8 of the ECHR

May

18 May – CoE Committee of Ministers adopts the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Amending Protocol CETS N. 223 – "Convention 108+")

June

19 June – In *Centrum för rättvisa v. Sweden* (No. 35252/08 (not final)), ECtHR holds that bulk interception of communications in Sweden meets convention standards and that therefore there was no violation of right to respect for private life (Article 8 of the ECHR)

28 June – In *M.L. and W.W. v. Germany* (No. 60798/10 and No. 65599/10), ECtHR holds that the public's right to access archived material online takes precedence over the right of convicted persons to be forgotten

July

August

September

October

10 October – Convention 108+ is open for signature and immediately signed by 21 countries

November

December

4 December – European Commission for the Efficiency of Justice (CEPEJ) of the CoE adopts the European Ethical Charter on use of artificial intelligence in judicial systems and their environment

EU

January

25 January – CJEU holds in *F v. Bevándorlási és Állampolgársági Hivatal* (C-473/16) that subjecting asylum seekers to psychological tests to determine their sexual orientation amounts to a particularly serious and disproportionate interference with their private life

February

March

19 March – European Data Protection Supervisor (EDPS) adopts Opinion 3/2018 on online manipulation and personal data

April

16 April – EDPS adopts Opinion 4/2018 on the Interoperability Regulation proposal

25 April – European Commission adopts a Communication on Artificial Intelligence for Europe

May

6 May – Deadline for the transposition of the Data Protection Law Enforcement Directive (2016/680/EU)

25 May – Entry into application of the General Data Protection Regulation (EU) (2016/679)

June

5 June – CJEU holds in *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH* (C-210/16) that the concept of 'controller' within the meaning of Article 2 (d) of Directive 95/46 (data controller definition) encompasses the administrator of a fan page hosted on a social network

July

10 July – CJEU holds in *Tietosuojavaltuutettu v. Jehovan todistajat – uskonnollinen yhdyskunta* (C-25/17) that the concept of a 'filing system' covers a set of personal data collected in the course of door-to-door preaching. Thus, a religious community, such as Jehovah's Witnesses, is a controller, jointly with its members who engage in preaching, for the processing of personal data carried out by the latter in the context of door-to-door preaching

August

September

October

2 October – CJEU holds in *Ministerio Fiscal* (C-207/16) that the list of objectives for the purpose of Article 15 of the ePrivacy Directive is exhaustive and that the authorities' need for access must genuinely correspond to one of those objectives

23 October – 40th International Conference of Data Protection and Privacy Commissioners adopts the Declaration on Ethics and Data Protection in Artificial Intelligence

November

December

7 December – European Commission and the Member States publish a Coordinated action plan on the development of AI in the EU to promote the development of AI in Europe

11 December – Entry into application of the Data Protection Regulation for Union institutions, bodies, offices and agencies (EU) 2018/1725

19 December – In *Fashion-ID & Co. KG.* (C-40/17), the Advocate General's opinion concludes that the operator of a website embedding a third party plugin such as the Facebook Like button, which causes the collection and transmission of the users' personal data, is jointly responsible for that stage of the data processing

7 Information society, privacy and data protection

In 2018, news of large-scale abuses of personal data sparked concern and raised awareness of the need for strong privacy and data protection safeguards. This underlined the importance of legislators' efforts in this area – such as the General Data Protection Regulation (GDPR), which became applicable in May – as well as the key role of whistleblowers and civil society. Meanwhile, the Council of Europe opened for signature the Amending Protocol for modernised Convention 108, and the global expansion of Convention 108 continued, reaching a total of 53 States Parties by the end of 2018. Both texts provide individuals with a reinforced legal framework to protect their rights to privacy and protection of personal data. Such legal frameworks are especially vital when fast-evolving technologies bring both economic opportunities and legal challenges. Across the EU, Member States entered an artificial intelligence race to ensure that industry and labour markets are well placed for tomorrow's competitiveness – sometimes leaving fundamental rights on the margin of the debates. Finally, and as in previous years, data protection in the context of law enforcement also remained high on the agenda, with the European Commission proposing new rules for the cross-border acquisition of e-evidence. There were, however, no EU-level developments on data retention: no EU initiatives to comply with the relevant 2014 and 2016 CJEU judgments were proposed.

7.1. 2018: the year of data protection awareness

7.1.1. EU pushes ahead with data protection efforts amid growing awareness of risks

The Council of Europe finalised the modernisation of its legal framework on data protection by adopting the modernised Convention for the protection of individuals with regard to the processing of personal data (Convention 108+)[1] on 18 May 2018; Convention 108+ was opened for signature on 10 October; at the end of the year, it counted 22 signatories. The work was carried out in parallel with other reforms to international data protection instruments, and alongside the reform of EU data protection rules. Regulators at the Council of Europe and EU levels have ensured consistency and compatibility between the two legal frameworks.

In May 2018, the General Data Protection Regulation (GDPR)[2] became applicable. In addition, the transition period for transposing the Data Protection Law Enforcement Directive[3] (2016/680/EU) ended. The GDPR lays down rules on the protection of personal data and rules relating to the free movement of personal data that are directly applicable in all Member States.[4]

Amongst others, the new regulation develops and strengthens the rights of data subjects. One of the key aspects of this enhanced protection of individuals is the reinforcement of consent requirements: from 25 May 2018 onwards, companies and public authorities are obliged, when processing personal data on the basis of consent, to demonstrate that consent has been given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication by which the data subject signifies agreement to the processing of his/her personal data. The GDPR also introduces the concept of transparency, including the obligation that the data subject needs to be provided with relevant information in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Informational self-determination of the data subject has been reinforced through the introduction of the right to data portability and the strengthening of the right to be forgotten. Data portability enables individuals to obtain and reuse their own personal data across different services and service providers. The right to be forgotten, even though it is not absolute, provides that every data subject can demand the erasure of their personal data if certain conditions are met. The GDPR codified this right following the CJEU landmark decision in *Google v. Spain*, which interpreted the right to erasure in relation to the responsibilities of a search engine as data controller.[5]

FRA ACTIVITY

FRA's updated Handbook on European law relating to data protection

FRA, the Council of Europe and the European Data Protection Supervisor (EDPS) jointly published the 2018 Handbook on European law relating to data protection. This publication is part of the wider series of joint handbooks on European law and fundamental rights from FRA and the Council of Europe, providing an overview of the EU's and the Council of Europe's applicable legal frameworks. The handbook also contains explanations of key data protection case law, summarising major rulings of both the Court of Justice of the European Union and the European Court of Human Rights. In addition, it presents hypothetical scenarios that serve as practical illustrations of the diverse issues encountered in this ever-evolving field.

See FRA-Council of Europe (2018), Handbook on European data protection law – 2018 edition, Luxembourg, Publications Office.

Regarding the implementation of the GDPR at national level, a number of Member States, such as Germany and Austria, adopted implementing legislation before 25 May 2018. Other Member States continued their activities related to the alignment of their national laws to the GDPR throughout 2018.[6]

The new data protection rules also include the Data Protection Law Enforcement Directive (2016/680/EU)[7]. This legislation establishes a comprehensive system of protection of personal data in the context of law enforcement, while also acknowledging the particularities of criminal justice authorities. It closely follows the principles and structure of the GDPR, while ensuring the high level of protection of personal data and enhancing data exchanges and better cooperation between Member States' competent authorities.

Just two days before the GDPR became applicable, the Council of the European Union and the European Parliament agreed on a new set of rules for the processing of personal data by EU institutions and bodies. Regulation (EU) 2018/1725,[8] also referred to as the EUI-GDPR,[9] brings the data protection rules that bind EU institutions and bodies in line with standards laid down in the GDPR and the Law Enforcement Directive. Furthermore, it establishes formal duties of the EDPS. Under the new regulation, the EDPS remains responsible for ensuring the effective protection of individuals' fundamental rights and freedoms whenever their personal data are processed by or on behalf of EU institutions and bodies.

The GDPR protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data as laid down in Article 8 of the Charter. In addition, aspects of Article 7 on the right to private life are regulated by the ePrivacy Directive.[10] However, current rules on electronic privacy refer only to traditional communication providers (e.g. providers of fixed and mobile telephony). During the last decade, a whole new ecosystem of communications service providers, such as messaging platforms, social networks and Voice-over-Internet-Protocol services, has grown rapidly, collecting vast amounts of private and personal data. Consequently, the European Commission proposed an updated ePrivacy Regulation[11] to complete the modernisation of EU data protection legislation and align electronic communications' privacy with the standards established by the GDPR. Once adopted, the updated ePrivacy Regulation should better protect individuals' privacy by ensuring the confidentiality of communications. However, after two years, the negotiations on this legislation are still ongoing. Both the European Data Protection Board (EDPB)[12] and the EDPS[13] invited the EU legislators to conclude an agreement on the proposal rapidly.

Despite the fact that the GDPR is based on the proven principles of the repealed Data Protection Directive (95/46/EC), the new rights and legal requirements established by the GDPR sparked a number of questions regarding the extent to which businesses that process personal data comply with the regulation. The national data protection authorities (DPAs) observed a significant increase in the numbers of complaints submitted and in the notifications of personal data breaches. For example, in **France**, between May and October 2018, the national supervisory authority, CNIL, received 742 notifications of personal data breaches, an increase of almost 50 % since before the GDPR came into application.[14] In the **United Kingdom**, the number of cases received by the Information Commissioner's Office has doubled, to 14,996 complaints and 5,992 breach notifications, which is the highest increase in the EU so far.[15] This demonstrates that the GDPR, in the first months since its entry into application, has proven to be a practical tool for reinforcing the protection of people's privacy.

Civil society plays a key role in the defence of fundamental rights, as FRA's report *Challenges facing civil society organisations working on human rights in the EU* explains.[16] In the GDPR, Article 80 (1) enables qualified entities, such as not-for-profit bodies, organisations or associations that have been properly constituted in accordance with the law of a Member State, have statutory objectives which are in the public interest, and are active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data, to lodge complaints on behalf of individuals. For example, the **Austrian** not-for-profit organisation NOYB filed four complaints over "forced consent" against Google (in France), Instagram (in Belgium), WhatsApp (in Germany) and Facebook (in Austria) with these Member States' data protection authorities.[17]

Promising practice

Helping people exercise their GDPR-based rights

In the **Netherlands**, the privacy-focused civil society organisation Bits of Freedom set up a website that helps individuals exercise their GDPR rights as data subjects. Through this tool, individuals can generate, send and keep track of their requests made to data controllers to access, remove, correct or move personal data.

For more information, see the 'My data done right' website set up by Bits of Freedom.

But the GDPR goes further, as Article 80 (2) allows Member States to provide in their national legislation that not-for-profit organisations may also lodge complaints independently of a data subject's mandate. This is one of the "specification clauses" of the GDPR, meaning that Member States may choose to implement this article or not. A few countries, including **Belgium**,[18] **Germany**,[19] **Hungary**[20] and **Slovakia**,[21] include that possibility in their national legal frameworks incorporating the GDPR, according to FRA's data collection. However, how the actions of consumers' representatives interact with the defence of privacy and data protection by qualified entities is currently under discussion in the EU. The proposal for a directive on representative actions for the protection of the collective interests of consumers now includes references to data protection.[22] A preliminary ruling on the interplay between consumers' collective redress and data protection is currently pending before the CJEU. Advocate General Bobek concluded that the Data Protection Directive (95/46/EC) does not preclude national legislation that grants public-service associations standing to commence legal proceedings against the alleged infringer of data protection legislation in order to safeguard the interests of consumers.[23] The expansion of consumers' collective redress could give another legal basis for civil society organisations to lodge data protection complaints independently of any mandate from individuals.

Large-scale attacks on privacy and data protection often result from the lack of appropriate legal, technical and organisational safeguards within international corporations and governments. As in the context of the Snowden revelations in 2013,[24] whistleblowing has proven to be a necessary tool to fight serious breaches of the rights to privacy and data protection that would otherwise remain undisclosed within an organisation. FRA's report on surveillance by intelligence services[25] highlighted the need to protect whistleblowers. On 23 April 2018, the European Commission presented a proposal for a Directive on the protection of persons reporting on breaches of Union law.[26] At that stage, only 10 EU countries (**France**, **Hungary**, **Ireland**, **Italy**, **Lithuania**, **Malta**, the **Netherlands**, **Slovakia**, **Sweden** and the **United Kingdom**) had comprehensive laws protecting whistleblowers.[27]

7.1.2. Data protection and democracy

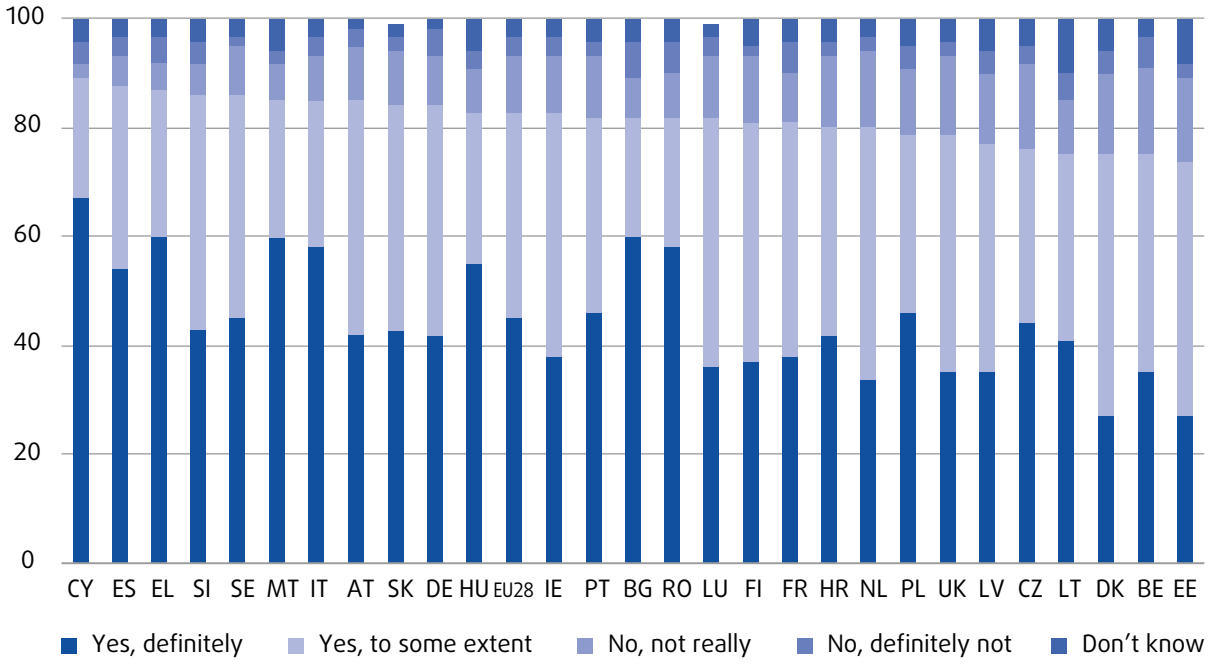
Data protection became a worldwide trending topic in 2018. In March, the Facebook/Cambridge Analytica scandal emerged after revelations by the company's former director of research, Christopher Wylie,[28] revealing an unprecedented abuse of consent of up to 87 million users. Micro-targeting had used their personal information for political campaigning. This abuse resulted in a £ 500,000 fine for Facebook for failing to protect users' personal information.[29] These revelations, which followed the on-going investigation into the cyberattacks during the 2016 US presidential election, fuelled worldwide concerns about the manipulation of democratic processes.[30]

As Figure 7.1 shows, there is a general perception among EU citizens that online disinformation is a problem for democracy.

Data protection has direct implications for other fundamental rights, such as freedom of expression and information, and for the conditions required to implement democratic processes through the right to participate and be elected in a free and secret ballot. Online manipulation of elections is a major threat to the democratic principle, and can also fuel radicalisation and political positions hostile to fundamental rights.

> *"We must protect our free and fair elections. This is why the Commission is today proposing new rules to better protect our democratic processes from manipulation by third countries or private interests."*
>
> *Jean-Claude Juncker, President of the European Commission (2018), 'State of the Union address 2018', 12 September*

Figure 7.1: Perception of the impact of fake news on democracy in the EU-28 (%)[a,b]



Notes: [a] *Question 4.2: 'In your opinion, is the existence of news or information that misrepresent reality or is even false a problem...For democracy in general (%)'.*

[b] *N=26,576.*

Source: *European Commission, 2018 [Flash Eurobarometer 464 on Fake News and Disinformation Online, p. 21]*

Both the EU[31] and the Council of Europe[32] worked in 2018 to provide rules and guidelines to protect personal data, freedom of expression, and the fairness and freedom of European democratic processes with a view to the 2019 European Parliament elections. However, national legal developments on this issue are discrete: On 22 December 2018, the **French** parliament passed a law on the fight against the manipulation of information. It took a comprehensive approach, including provisions on the electoral code, but also on freedom of information, the responsibilities of services providers and measures to reinforce education on fact checking.[33] On the other hand, the **Spanish** parliament passed on 21 November 2018 a data protection law adapting Spanish legislation to the GDPR. It contains a provision allowing political parties to use citizens' personal data that have been obtained from web pages and other publicly accessible sources when conducting political activities during election campaigns.[34] This provision, introduced via amendments to the bill, was the subject of an ad hoc report by the Spanish data protection authority. It highlighted the need to introduce additional safeguards to avoid the use of big data and micro-targeting for campaigning purposes.[35]

Micro-targeting for political campaigning and the distribution of fake news through bots are examples of how disruptive technologies such as big data and artificial intelligence can interfere with fundamental rights.

7.2. Artificial intelligence and big data: debates focus on ethics, sidelining fundamental rights

The European Commission defines artificial intelligence (AI) as "systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals".[36] The terms 'artificial intelligence' and 'big data' are currently often used very broadly, and are not clearly defined. However, these terms commonly relate to the relatively recent increased opportunities to process and analyse large quantities of data to automate tasks, deliver analysis or support

decisions. Some pieces of EU legislation address these developments. The GDPR, for example, regulates automated individual decision-making, including decision-making based on profiling, in its Article 22, which inevitably extends to artificial intelligence and big data analytics.[37]

Artificial intelligence, big data and, more generally, new technologies are in constant evolution. Foreseeing the tangible effects that these technologies will have on the economy, societies or people is a difficult exercise; in-depth assessments require time. In this context, 2018 was the year when many initiatives were taken to tackle the potential impact of artificial intelligence, in terms of both opportunities and challenges. As a result, many relevant bodies at international, European and national levels published reports, including societal analysis, legal proposals, policy initiatives and forecasting strategies.

Three main tendencies can be identified:

1. National initiatives on AI aim to make the most of artificial intelligence and big data to boost economic and industrial competitiveness.

2. Most Member States consider it crucial to increase financial support for education and research.

3. Several Member States believe that specific AI challenges will need to be tackled through the adoption of dedicated legislation.

These emerging technologies have varying potential impacts depending on the fields where they are applied, such as insurance, health, transport or education, to name only a few. Consequently, some fields will require the adoption of specific, tailored legislation. The European Commission made several proposals to address different issues, notably in relation to public sector information,[38] the sharing of private sector data in the European economy,[39] access to and preservation of scientific information,[40] and the digital transformation of health and care in the Digital Single Market.[41] Similarly, the Council of Europe has launched research and initiatives to assess artificial intelligence's impact on specific topics.[42] With respect to justice, the Council of Europe has been actively examining the challenges and opportunities related to the use of artificial intelligence and algorithms in judicial systems, including the so-called "predictive" justice tools. The Council of Europe's work culminated in the adoption of the 'European Ethical Charter on the use of artificial intelligence in judicial systems and their environment', on 3 December 2018.[43]

Some Member States also decided to focus studies or initiatives on specific topics. In 2018, the specific national legal initiatives concentrated on four areas: health (in **Finland**,[44] **Latvia**[45] and **Portugal**[46]), the regulation of relationships between financial and other institutions (in the **Netherlands**[47]), the modernisation of the public sector (in **Latvia**,[48] **Portugal**,[49] **Poland**,[50] **Slovakia**[51] and **Sweden**[52]), and transport (**Austria**,[53] **Estonia**[54] and **Spain**[55]).

7.2.1. A debate dominated by ethics, with fundamental rights in the shadows

By the end of 2018, Member States had understood the significant impact that artificial intelligence can have on industry and the labour market. The solutions to ease this technological transition – focusing on increased research and resources – are well under way within most Member States. Foreseeing the economic and labour impacts that AI may have on individuals is necessary to ensure the cohesion of society. However, Member States should also pay close attention to the impact that AI will have on fundamental rights, and should prepare adequate strategies to ensure that such rights, and not only ethical considerations, will be duly respected.

FRA ACTIVITY

Assessing the impact of artificial intelligence and big data on fundamental rights

In 2018, FRA launched a research project on artificial intelligence, big data and fundamental rights. This project aims to assess the positive and negative fundamental rights implications of new technologies, including AI and big data. It analyses concrete uses of AI by carrying out interviews with public administrations and businesses in selected Member States, which feed into case studies in selected areas of application. The project also collects information on awareness of fundamental rights issues among public administrations and businesses that apply AI-related technologies. Finally, the project will explore the feasibility of using either online experiments or simulations to study concrete examples of fundamental rights challenges that people face when they use algorithms for decision making.

For more information on the project, see FRA's webpage on 'Artificial Intelligence, big data and fundamental rights'.

Two EU expert advisory groups have the objective of defining the ethical boundaries of the use of artificial intelligence. In 2018, they published recommendations. The EDPS Ethics Advisory Group published its final report in January 2018,[56] and the European Commission's High Level Expert Group on Artificial Intelligence published a first draft of its

AI ethics guidelines on 18 December 2018.[57] FRA is a member of the High Level Expert Group on AI.

The Council of Europe established a committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence. It published key documents assessing the impacts of AI on fundamental rights, including a draft recommendation on human rights impacts of algorithmic systems, and a draft declaration on the manipulative capabilities of algorithmic processes.[58] The Committee of Convention 108 worked on a report on AI and data protection and the preparation of guidelines providing baseline orientations with regard to data protection.[59] Finally, the OECD announced the creation of an AI policy observatory to be launched in 2019, with the aim of providing insights on public policies and ensuring beneficial uses of AI.[60]

At national level, most research and analysis launched in 2018 focused on the economic opportunities for each country: seven Member States (**Austria**,[61] **Belgium**,[62] **Bulgaria**,[63] **Lithuania**,[64] **Estonia**,[65] **Finland**[66] and **Sweden**[67]) dedicated their initiatives to the evaluation of the impacts on the industry or the labour market; six Member States (**Austria**,[68] **Denmark**,[69] **Finland**,[70] **France**,[71] **Sweden**[72] and the **United Kingdom**[73]) on the need to reinforce research and education; and 13 Member States focused on the impact of AI on dedicated sectors (health in **Finland**,[74] **Latvia**[75] and **Portugal**,[76] banks in the **Netherlands**,[77] the modernisation and digitalisation of public services in **Latvia**,[78] **Portugal**,[79] **Poland**,[80] **Slovakia**,[81] and **Sweden**,[82] or transportation in **Austria**,[83] **Estonia**,[84] **Poland**,[85] and **Spain**).[86]

In several Member States, the ethical and fundamental rights implications were not subject to detailed assessments, but only cursorily mentioned, FRA findings show. In **Sweden**, for instance, the Innovation Agency concluded in its report on artificial intelligence in Swedish business and society that the discussion on ethics and security is far too limited.[87] In **Finland**, the Parliamentary Committee for Future report 'Hundred new opportunities of Finland 2018–2037: Radical technologies reform societal models', identifies the 100 most promising new technologies and 100 new legislative aims. It includes only sporadic references to fundamental rights-related concerns.[88]

Some Member States, however, were notable exceptions, and conducted in-depth analyses of the potential ethical impacts of artificial intelligence. These included **Denmark**,[89] **Finland**,[90] **France**,[91] **Germany**,[92] **Poland**[93] and the **United Kingdom**.[94] In the **United Kingdom**, a report[95] prepared by the Lords Select Committee on Artificial Intelligence considered the economic, ethical and social implications of advances in artificial intelligence. In relation to ethics, the committee recommended that the Law Commission "consider the adequacy of existing legislation to address the legal liability issues of AI and, where appropriate, recommend to Government appropriate remedies to ensure that the law is clear in this area". While recognising the major boost AI could provide to the UK economy in the coming years, the report stresses the need to "put ethics at the centre of AI's development and use".

In **Denmark**,[96] the Danish Expert Group on Data Ethics (SIRI Commission) delivered nine recommendations to the Danish government on how to empower consumers and tech-workers as well as on how to make data ethics a competitive advantage for businesses. The Danish government is translating the recommendations into a range of concrete policy initiatives, e.g. 1) the establishment of a data ethics council with the task of advising the government on data ethical questions, 2) the cooperation with industry bodies to explore the possibility of creating a national seal for digital security and responsible data use that will increase transparency and make it easier for consumers to choose companies that live up to certain security and ethics standards, and 3) a new requirement that the largest Danish companies disclose their data ethics policies as part of their annual management reports. Furthermore, the SIRI Commission's fourth thematic report on AI, media and democracy dealt with the ethical implications and dilemmas of AI. The report recommended, among others, that privacy by design should be applied in AI innovation, that companies, organisations and authorities should develop ethical principles for dealing with data with more safeguards than the legislative requirements, that targeted work should be initiated to reduce problematic bias in data, and that equality issues should be considered in the development and design of AI services and systems.

In **Finland**,[97] the Ministry of Finance has set up a project group to prepare a report on ethical information policy in an age of artificial intelligence. The report addressed the legal and ethical questions linked to the collection, aggregation, opening and preservation of information, including the security and protection of personal data. The report describes the ethical and regulatory issues at stake. To ensure public participation, the report was publicly accessible and open to comments until October 2018.

Promising practice

Taking a strategic approach to AI

In **Germany**, the Federal Government adopted an Artificial Intelligence Strategy on 16 November. It includes the objective of organising a broad dialogue to ensure artificial intelligence is embedded in society in ethical, legal, cultural and institutional terms. Notably, the strategy highlights the principle of "ethics by, in and for design" for the development and application of AI, which is to become a core element of the brand 'AI made in Europe'. Another keyword is "trusted AI", which means that ways to increase transparency of algorithmic decision making and accountable AI shall be promoted by relevant actors when implementing the strategy.

For more information, see Germany, Federal Government (Die Bundesregierung) (2018), Strategie Künstliche Intelligenz der Bundesregierung, 16 November 2018.

In **Austria**, **Denmark**, **Finland**, **Germany** and the **United Kingdom**, new research centres will expressly include legal issues and/or ethics in their mandate. The **United Kingdom**'s Centre for Data Ethics and Innovation was established to look into the safe and ethical use of data and artificial intelligence.[98] The **Austrian** Government Programme 2017–2022[99] calls for the establishment of an "ethics council on digitisation" for social issues related to digitisation. The Council for Robotics and AI could be extended to fulfil the function of this ethics council. Similarly, in **Germany**, the Artificial Intelligence Strategy also envisages the establishment of an "observatory for artificial intelligence" for technology assessment.[100] At EU level, the AI4EU project is an AI-on-demand platform that will provide access to AI resources in the EU for all users. It also plans to establish an AI4EU Ethics Observatory to ensure respect for human-centred AI values.[101] In **Denmark**, CREDI (Centre for Law and Digitisation)[102] was established in 2018 with the aim of assessing the legal aspects of the digital society and analysing the links between technology, digitalisation and law. In **Finland**, the Finnish Center for Artificial Intelligence (FCAI) was created with the aim of delivering "real AI for real people in the real world". The center established a forum, FCAI Society,[103] composed of humanists, legal experts and social scientists, to assess the ethical impacts of AI on society, promote public debates and advise technical experts. Finally, in **Italy**,[104] the *White Paper on artificial intelligence at the service of citizens* recommended establishing a Trans-disciplinary Centre on AI, to promote and support public debate on emerging ethical issues.

Promising practice

Raising awareness on algorithms and AI

Data for Good is a community of data scientists in **France** acting on a voluntary basis to propose solutions to societal challenges raised by the use of AI. It has developed a project, Algo Transparency, aimed at raising awareness and informing citizens of the algorithms behind access to information. Its first test case focused on YouTube, analysing the functioning of the algorithm that selects the recommended videos, and highlighting the impact on freedom of expression and freedom of information.

For more information, see the websites of the Data for Good community and the Algo Transparency project.

The initiatives listed above show that discussions around the principles to be established for guaranteeing safe and legal use of artificial intelligence focused almost exclusively on *ethics*, and not on fundamental human rights. The only exception was found in a report by the University of Utrecht on 'Algorithms and fundamental rights', which the **Dutch** government requested.[105] By the end of 2018, the government had not commented on the report. Furthermore, the Dutch Council of State published an opinion in which it highlighted the potential negative impacts of the Dutch Digital Agenda on individuals' rights and freedoms.[106]

The extent to which most debates have been concentrating on ethics – rather than "fundamental rights" – should therefore be questioned. Ethical standards may guide Member States and private actors, but they should not be seen as a substitute for rights. Fundamental rights are enshrined by law, so they provide individuals with a strong, harmonised and legally binding framework. In contrast, the meaning and exact limitations of ethics may differ from one national or cultural context to another, and from one field of AI application to another. Although ethical dimensions may complement fundamental rights, such inconsistency could jeopardise a harmonised and coherent approach to the rules governing AI implementation across the EU.

7.2.2. Legal challenges set boundaries of use of AI and big data

Complaints related to misuse of data, algorithms and related technologies have emerged in several Member

States. That makes it all the more important to use commonly agreed, and legally binding, fundamental rights as a basis for assessing AI's potential impacts on individuals.

In **Finland**,[107] the Data Protection Ombudsman received complaints about scoring methods used by credit companies. The ombudsman transferred the complaints to the National Non-Discrimination and Equality Tribunal, which held that the applicant had been subjected to multiple discrimination. In this case, the company denied credit using a scoring system that calculated the applicant's rating on the basis of, among other things, the applicant's language, gender, age and place of residence. The applicant had no payment defaults, but no individual assessment of payment ability was made and the denial was made on statistical data alone.

Promising practice

Scrutinising data for potential bias

In **Germany**, Open Knowledge Foundation and AlgorithmWatch, two civil society organisations, collected anonymised financial and credit-scoring data that individuals voluntarily donated. They analysed the data to show if the credit scoring led to bias and/or mistakes. In some cases, individuals were rated negatively even though their profile did not include negative features, the findings showed. They also showed that the algorithm used to assess the creditworthiness of individuals relies on a database that includes inaccurate or incomplete data for some individuals. Finally, the use of personal data such as age or gender creates a risk of biased or discriminatory scoring, they showed. Such research is very important to raise awareness of the potential impact on fundamental rights of using automated systems to establish scores.

For more information, see the project website.

In **France**,[108] the Public Defender of Rights launched an investigation into the operation of the new admissions system for higher education (*Parcoursup*), following complaints from individuals and elected officials. These complaints cited the "opacity" of the "local algorithms" set up in the institutions to file 812,000 university applications. Following the adoption of a new law on student orientation and academic success, universities for the first time ranked candidates' applications through the use of an algorithm. However, as academic institutions did not make the details of the processes public, the lack of transparency served to feed suspicion of discrimination and led the Public Defender of Rights to open an investigation into the subject.

FRA ACTIVITY

Focus on discrimination in data-supported decision making

In June 2018, FRA published a focus paper dealing specifically with discrimination when using algorithms for decision making. It points out the potential for built-in bias that leads to discrimination in applications and services. To help improve fundamental rights compliance, the paper gives examples of what could be done:

1. being transparent about how algorithms were built so others can detect and rectify discriminatory applications;
2. assessing the impact of potential biases and abuses resulting from algorithms;
3. assessing the quality of all data collected and used for building algorithms;
4. ensuring that how algorithms are built and operate can be meaningfully explained so people can challenge data-supported decisions.

For more information, see FRA (2018), #BigData: Discrimination in data-supported decision making, Luxembourg, Publications Office. See also FRA (2018), Big data, algorithms and discrimination – in brief, Luxembourg, Publications Office.

In **France**, similarly to the complaints brought by NOYB in Austria (see Section 7.1.1), the internet advocacy group La Quadrature du Net filed five collective complaints against Google, Apple, Facebook, Amazon and LinkedIn (Microsoft), accusing them of illegally using the personal data of their users.[109] The complaints bring together the names of nearly 12,000 people and were filed with the French data protection authority (CNIL). The complainants believe that the way Google, Facebook and others obtain the consent of internet users does not comply with the rules of the GDPR. In particular, they criticise pre-ticked boxes, or clauses stipulating that continuing to use a service constitutes acceptance. Although CNIL considers itself the relevant authority to investigate the complaint against Google directly, it intends to handle this case in cooperation with the other data protection authorities.

In the **Netherlands**,[110] a coalition of several civil society organisations, including the Dutch section of the International Commission of Jurists, Privacy First Foundation, KDVP Foundation and the Dutch Platform for the Protection of Civil Rights, filed a lawsuit against the Dutch government on the use of the System Risk Indication (SyRI) to assess potential violations of the law. SyRI links together databases of participating partners, such as the tax authority, a municipality and the social security agency (UWV). The databases relate to the inhabitants of a particular postal code

within the involved municipality. The algorithm checks whether there are discrepancies between the databases, which could indicate that one of the laws covered by the SyRI system is being violated.[111] An example is that a person is registered in the municipal database as a home owner, while the same persons collects rent benefits from the tax authority. Identified individuals are included in a Risk Reports Register. The signals are sent to the participating partners for further investigation. According to the coalition, SyRI could violate several fundamental rights while simultaneously undermining the relationship of trust between citizens and those in power.

In **Poland**,[112] the Polish Commissioner for Human Rights asked the Constitutional Tribunal to assess the legality of an automated decision-making system that the Ministry of Labour and Social Policy used to profile unemployed individuals. The decision by the tribunal clarified that such profiling should be regulated in a legal act, and not only based on a minister's ordinance.

Finally, in **France**,[113] more than 60 senators asked the Constitutional Court to give its opinion on, among other matters, the use of algorithms by public authorities for decision-making purposes. The Constitutional Court clarified that, to be lawful, such a decision must meet three conditions under French law: first, the decision should clearly state that it was adopted on the basis of an algorithm, and the main criteria fed into the algorithm should be communicated to the individual; second, individuals should be able to challenge the decision and have access to effective remedies; third, the use of algorithms is prohibited if sensitive personal data are involved. Finally, the court clarified that public authorities should have sufficient control of the algorithms to clearly explain to individuals how any decision was made.

7.3. Data protection and measures to ensure security: striking the right balance

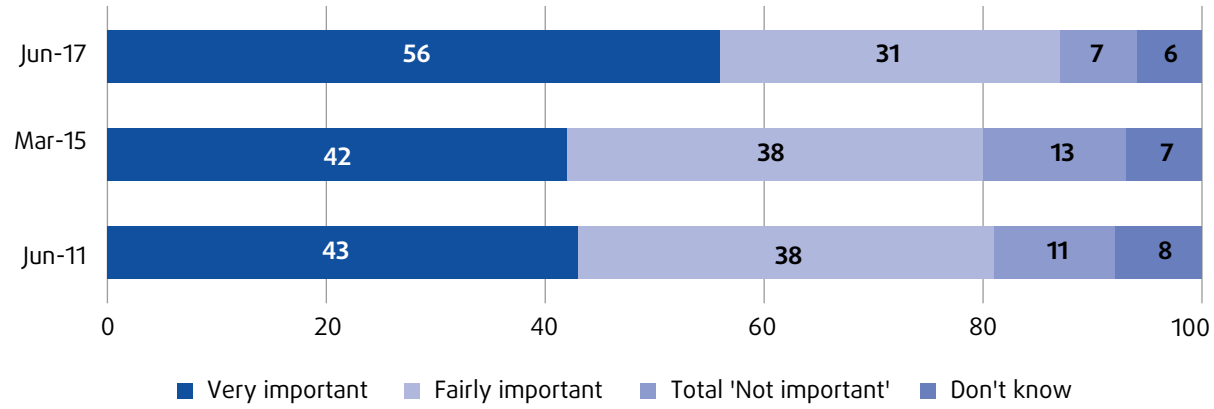
Data protection and democratic processes are threatened not only by illegal commercial practices but also by cybercrime. In September 2018, Facebook reported a significant attack affecting nearly 50 million users,[114] and in December 2018 the personal data of hundreds of politicians in **Germany** were leaked on Twitter.[115]

Surveys on Europeans' perception towards security show that nearly nine in 10 respondents (87 %) see cybercrime as an important problem. This figure has risen since the previous survey, when eight in 10 (80 %) respondents expressed this opinion. Over half (56 %) see cybercrime as a very important problem, while just under a third (31 %) view it as a fairly important problem (Figure 7.2).

In 2018, European users generally perceived the internet as unsafe (see Figure 7.3).

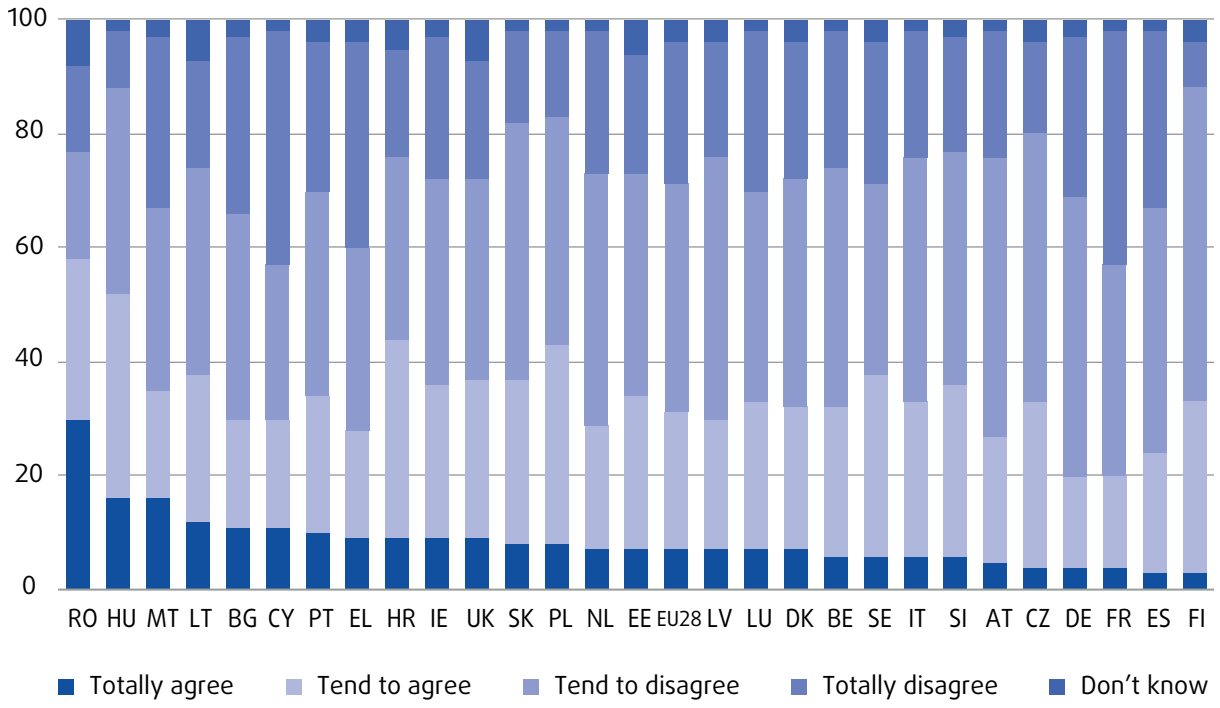
In 2018, both the EU and the Council of Europe worked to introduce new instruments to provide effective tools for investigating cybercrime and to facilitate cross-border access to electronic evidence. However, the Charter and the ECHR also require them to strike a fair balance between the applicable fundamental rights and the need to ensure the security of citizens. The CJEU demonstrated that by invalidating the Data Retention Directive in 2014.

Figure 7.2: Perception of the importance of the challenges to the internal security of the EU (%)



Source: *European Commission, 2017 [Special Eurobarometer 464b, p. 16, QB2]*

Figure 7.3: Perception in the EU of the internet's safety for users (%)[a,b]



Notes: [a] *Question 1.1: 'Do you agree or disagree with each of the following? The Internet is safe for its users.'*
[b] *N=33,244.*

Source: *European Commission, 2018 [Flash Eurobarometer 469, p. 19]*

FRA ACTIVITY

Handbook on European law relating to cybercrime and fundamental rights

In 2018, following a request from the European Parliament, FRA and the Council of Europe started a new joint project to produce a Handbook on European law relating to cybercrime and fundamental rights. This new manual will provide guidelines on supervisory and scrutiny controls for Member States to ensure compliance with fundamental rights safeguards while countering cybercrime. It will compile and explain key aspects of the European legal framework at the Council of Europe and EU levels together with selected extracts from relevant European and national case law, such as key judgments and decisions delivered by the European Court of Human Rights, the Court of Justice of the EU and higher national courts.

For more information, see FRA's webpage on the project.

7.3.1. Data retention: EU and national legal frameworks in the making

As past FRA fundamental rights reports pointed out,[116] following the CJEU's annulment of the Data Retention Directive[117] in 2014,[118] the EU has still not legislated on the matter. Member States remain responsible for regulating data retention on the basis of Article 15 (1) of the ePrivacy Directive,[119] and in line with the fundamental rights standards in *Tele2 Sverige* and *Watson*.[120]

Developments at ECtHR and CJEU

During 2018, both the CJEU and the ECtHR delivered some important judgments on data retention. The CJEU delivered its judgment in *Ministerio Fiscal* in October.[121] It held that national authorities can access subscriber information regarding users of stolen mobile phones.[122] Access to mere subscriber information that is not "cross-referenced" to other communication and location data does not allow precise conclusions to be drawn about the private lives of individuals.[123] Therefore, the court held that such access was a proportionate interference with the rights to privacy and personal data protection.[124] The judgment did not,

however, examine the lawfulness of the preceding data retention scheme.[125]

In September, the ECtHR issued its long-awaited judgment in *Big Brother Watch and Others v. the United Kingdom*.[126] The judgment is not yet final; at the beginning of 2019, the case was referred to the Grand Chamber. It ruled that the interception regime operated by UK authorities violated the right to private life and freedom of expression, in particular with regard to journalistic freedom (Articles 8 and 10 of the ECHR). This regime enabled the general ("bulk") interception of communications, which were then filtered to spot any suspicious communications. It also provided for targeted interception of communications belonging to specified persons or phone numbers, etc. In particular, the court found that there was inadequate independent oversight – both of the selection that allows transmission of information signals between network interfaces (internet bearers) for interception; and of the filtering, searching and selection of intercepted communications for examination.[127] Targeted acquisition of data did not require a prior review by a court or another independent body and was not restricted to "serious crimes".[128]

In *Benedik v. Slovenia*, the ECtHR dealt with the police's failure to obtain a court order to access subscriber information associated with a dynamic Internet Protocol (IP) address.[129] The court held that the law allowing the police to obtain such information lacked clarity and did not provide for the necessary independent supervision.[130] The court emphasised that anonymity online is part of the right to private life (Article 8 of the ECHR) and should attract appropriate protection.[131]

National developments

Both legislation and case law in Member States regarding data retention and access still remain very diverse. Some Member States made efforts during 2018 to align their law with the judgments of the CJEU. For example, **Austria** passed legislation allowing targeted retention of data following 'quick freeze orders' issued on the basis of suspicion, on special occasions and in special conditions.[132] In the **Netherlands**[133] and **Denmark**,[134] legislative initiatives were pending at the end of 2018 to address the issues raised by the CJEU. However, in **Sweden**, courts and the DPA criticised the amendments that the government proposed to comply with the CJEU judgments.[135] **Italy**[136] allowed longer data retention periods than those Directive 2006/24/EC originally provided for, and the Italian DPA has raised its concerns about these developments.[137]

In 2018, courts in the Member States delivered several judgments related to this topic. Overall, national courts tend to follow the case law of the CJEU with regard to legislation incorporating Directive 2006/24/EC or legislation passed on the basis of Article 15 (1) of Directive 2002/58/EC. For example, on 20 April 2018, the Administrative Court in Cologne, **Germany**, held in two decisions that the newest national legislation also violates EU law, as it still allows general and indiscriminate retention, albeit for shorter periods.[138] Similarly, the Court of Appeal and the High Court in the **United Kingdom** held that national legislation was inconsistent with EU fundamental rights standards, lacking the requirement of prior judicial control.[139] In **Ireland**, the High Court also ruled that national legislation on data retention violates EU law and the ECHR, as it established a general and indiscriminate data retention regime.[140] In **Cyprus**, there is conflicting jurisprudence among courts. Some courts that follow the CJEU judgments declare evidence inadmissible if it is acquired on the basis of a general and indiscriminate retention regime, while others admit such evidence.[141]

However, important case law developments are still pending. In the **Czech Republic**, the lawfulness of general and indiscriminate storage of traffic and location data is a matter currently pending before the Constitutional Court.[142] The Constitutional Court of **Belgium**[143] and the **French**[144] *Conseil d'Etat* asked the CJEU to issue a preliminary ruling on whether or not blanket retention is compatible with fundamental rights. In particular, they wanted to know if a general retention scheme is justified in view of positive obligations of states to ensure effective criminal investigation, and the right to security enshrined in Article 6 of the Charter. The Supreme Court of **Estonia** asked the CJEU[145] to clarify whether or not access to traffic and location data pertaining to a short time period is a serious interference with fundamental rights. It also asked whether public prosecutors amount to an independent administrative authority that can lawfully authorise access to data retained.

7.3.2. European challenges on cross-border access to data for law enforcement purposes

The legal challenges in achieving a balance between data protection and security require effective safeguards governing law enforcement agencies' access to personal data as well as data retention. Electronic data are increasingly used as evidence in criminal investigations. Digital forensics are regularly used not only in the investigation of cybercrimes, but to establish the identity of the suspect, the victim and many other circumstances in ordinary (non-IT) crimes. The use of cloud computing is currently prevalent. Cloud computing is a "paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand", according to the WP29 code of conduct for cloud service providers.[146] This

type of evidence is rarely located on a single server, and it can be moved within seconds to another jurisdiction. Traditional cross-border access mediated through mutual legal assistance is considered too time-consuming to tackle the volatility of electronic evidence, and direct cross-border access to data by law enforcement agencies is considered too risky under the current jurisdictional rules and the different human rights standards. The current policy debate is trying to find a middle way between them. The proposed solution to the problem of the loss of location of electronic data is the "business link": in most cases, e-evidence can be traced and retrieved through providers of electronic communications, information society services, internet domain services and IP numbering services (service providers).[147] However, many of the major service providers are US-based companies, and therefore not under the EU's jurisdiction.

In April 2018, the European Commission published two proposals aimed at facilitating law enforcement agencies' and judicial authorities' cross-border access to electronic evidence.[148] The proposed instruments are a directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings[149] and a regulation on European production and preservation orders for electronic evidence in criminal matters.[150] On 26 September, the EDPB adopted Opinion 23/2018, which expresses concern about a number of provisions of the proposed regulation on e-evidence because of the negative impact on the safeguards to the right of privacy and data protection. Academia[151] and lawyers[152] have highlighted the limitation on the fundamental rights safeguards as a result of the proposed changes in the application of the principle of mutual recognition recognised in Article 82 (1) of the TFEU, which is the legal basis of the proposed regulation on e-evidence. According to this new shift, the authorities of the Member State where the requested service provider is established or represented will be able to play a role only if the service provider does not comply with the order.[153]

Non-personal data can be also used as evidence in a criminal investigation. However, the Regulation on a framework for the free flow of non-personal data in the EU provides a procedure for cooperation between the competent authorities. It gives a more important role to the authorities of the Member State from which data are requested. They must assess a duly justified request with a written explanation of the reasons and the legal bases for seeking access to the data.[154]

The US and the vast majority of the EU Member States – the only exceptions being Ireland and Sweden – are parties to the Budapest Convention on cybercrime,[155] which is the only binding international instrument on this issue. In 2018, the Council of Europe's Cybercrime Convention Committee worked on drafting a second additional Protocol to the Budapest Convention. The aim of this new protocol is to provide for enhanced international cooperation, including provisions on direct cooperation of law enforcement authorities with service providers in other jurisdictions.

FRA opinions

In 2018, the Council of Europe updated its legal framework on data protection with the adoption of modernised Convention 108. Meanwhile, the global expansion of the original Convention 108 continued, with 53 countries bound by that convention by the end of the year. In the EU, the GDPR became applicable, Member States were to transpose the Law Enforcement Directive, and revised data protection rules for EU institutions and bodies were adopted. However, the adoption of the e-Privacy Regulation was still pending. The proposed regulation concerns the right to privacy in electronic communications; it is critical for ensuring that the EU legal framework is updated to align it with the GDPR, especially in view of new technological developments.

Even with several existing and new instruments in place, implementation and enforcement of data protection rules remained a challenge, as did the fight against abuses of these rules by public and private institutions. Qualified civil society bodies are often in a better position than ordinary citizens are to initiate proceedings that trigger data protection authorities' enhanced powers. However, only a few Member States have empowered qualified bodies to lodge complaints without an explicit mandate from a data subject.

FRA opinion 7.1

EU Member States should encourage the effective involvement of qualified civil society organisations in the enforcement of data protection rules, by providing the necessary legal basis for such organisations to lodge complaints regarding data protection violations independently of a data subject's mandate.

Whistleblowers are crucial for helping to ensure that data protection and privacy violations result in effective remedies, both by warning of potential breaches or by bringing important evidence during investigations. They contribute to public awareness and deterrence of serious and large breaches of rights to privacy and data protection that otherwise would remain undisclosed within organisations. FRA recommended enhanced protection for whistleblowers in its report on surveillance by intelligence services. However, few Member States have specific rules in place to provide effective protection against retaliation. In April 2018, the Commission proposed a directive on the protection of persons reporting on breaches of Union law.

FRA opinion 7.2

EU Member States should consider providing for effective protection of whistleblowers, thereby contributing to the effective compliance of business and governments with the fundamental rights to privacy and data protection.

Despite the CJEU's annulment of the Data Retention Directive (Directive 2006/24/EC) back in 2014 and relevant judgments in the field, the EU has still not adopted legislation on data retention. Consequently, the situation in Member States remains diverse, in particular when it comes to legislation. Some Member States have made efforts to align their legislation with the CJEU's judgments. Other Member States have not made any noteworthy changes in their legislation. The CJEU's ruling in the *Tele 2 and Watson* case confirms that national legislation regulating data retention and access for criminal and public security purposes falls within the scope of EU law and, in particular, under Article 15 (1) of the previous e-Privacy Directive (2002/58/EC). Such national legislation must not impose a general and indiscriminate data retention scheme, and must include procedural and substantial safeguards with regard to access to data retained. If Member States retain national legislation adopted to incorporate the former Data Retention Directive (Directive 2006/24/EC), or legislation that does not comply with the requirements laid down in the case law of the CJEU, they risk undermining respect for the fundamental rights of EU citizens and legal certainty across the Union.

FRA opinion 7.3

EU Member States should align their legislation on data retention with the CJEU rulings, and avoid general and indiscriminate retention of data by telecommunication providers. National law should include strict proportionality checks as well as appropriate procedural safeguards so that it effectively guarantees rights to privacy and the protection of personal data.

Recent developments in the areas of artificial intelligence and big data have led to many policy initiatives with a focus on maximising the economic benefits of new technologies. At the same time, many initiatives by various national and international bodies discuss ethical implications, and less often fundamental and human rights implications with a view to putting forward guidelines and soft law. Many Member States and EU institutions have started preparing national strategies on artificial intelligence.

FRA opinion 7.4

Given that only a rights-based approach guarantees a high level of protection against possible misuse of new technologies and wrongdoings using them, Member States should put fundamental rights at the heart of national strategies on AI and big data. Such strategies should incorporate know-how from experts in various disciplines such as lawyers, social scientists, statisticians, computer scientists and subject-level experts. Ethics can complement a rights-based approach but should not replace it.

Index of Member State references

Endnotes

1 Council of Europe, *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, CM/Inf(2018)15-final, 18 May 2018.

2 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 (General Data Protection Regulation), OJ (2016) L 119.

3 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive), OJ (2016) L 119.

4 To clarify the new rules, the European Commission published guidance on the direct application of the General Data Protection Regulation: Communication from the Commission to the European Parliament and the Council, *Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018*, COM/2018/043 final.

5 CJEU [GC], C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 13 May 2014.

6 More information on national legislation implementing the GDPR is available on the website of the International Association of Privacy Professionals.

7 Law Enforcement Directive, OJ (2016) L 119.

8 General Data Protection Regulation, OJ (2016) L 119.

9 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

10 Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

11 Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

12 EDPB, *Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications*, 25 May 2018.

13 EDPS Blog, "The urgent case for a new ePrivacy law", 19 October 2018.

14 See the CNIL website.

15 See the 'GDPR Today' website.

16 FRA (2018), *Challenges facing civil society organisations working on human rights in the EU*, Luxembourg, Publications Office.

17 Information available on NOYB's website.

18 Belgian law on the implementation of the GDPR of 30 July 2018, Art. 220.

19 German Act for the Improvement of the Enforcement of Consumer Protection Provisions in Data Protection Law by Means of Civil Law (*Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts*), 17 February 2016.

20 Hungarian information act (Act CXII of 2011), Art. 52 (1).

21 Slovak act No. 18/2018 on personal data protection (*Zákon o ochrane osobných údajov*) 29 November 2017.

22 COM (2018) 184 final, 11 April 2018, proposal for a Directive on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, recital (6) and Art. 5 and Art. 6.

23 Opinion of Advocate General Bobek delivered on 19 December 2018 in CJEU, C-40/17, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*.

24 European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)).

25 FRA (2017), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update*, Luxembourg, Publications Office, p. 13, Opinion 8.

26 European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law, COM(2018) 218 final, 23 April 2018.

27 European Commission, factsheet on whistleblower protection, April 2018.

28 The Facebook/Cambridge Analytica scandal was reported by the Observer and the NY Times on 17 March 2018. See also the Guardian, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", 17 March 2018.

29 United Kingdom, Information Commissioner's Office, *Facebook Ireland Ltd monetary penalty notice*, 24 October 2018.

30 Grand Jury's indictment in Case 18-263 of the U.S. District Court for the Western District of Pennsylvania, filed on 3 October 2018.

31 The European Commission on 12 September 2018 presented a security package focusing on free and fair European elections. More information available on the Commission's website.

32 15th European Conference of Electoral Management Bodies, organized by the Venice Commission in Oslo, Norway, on 19 and 20 April 2018, and the annual Octopus Conference on cooperation against cybercrime, in Strasbourg, France, on 11-13 July 2018.

33 France, *Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*.

34 Organic Law 3/2018 of 5 December on data protection and safeguard of digital rights, third final provision (in Spanish).

35 AEPD´s notice of 19 December 2018 (available in Spanish).

36 European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe*, Brussels, 25 April 2018, p. 2.

37 General Data Protection Regulation, OJ (2016) L 119.

38 European Commission, *Proposal for a revision of the Public Sector Information (PSI) Directive*, 25 April 2018.

39 European Commission, *Staff Working Document - Guidance on sharing private sector data in the European data economy*, 25 April 2018

40 European Commission, *Recommendation on access to and preservation of Scientific Information*, 25 April 2018.

41 European Commission, *Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*, 25 April 2018.

42 For more information on each initiative, see the Council of Europe's webpage on AI-related work in progress.

43 Council of Europe, European Commission for the Efficiency of Justice (CEPEJ), *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment*, Strasbourg, 3 December 2018.

44 Finland, Government Bill (*hallituksen esitys/regeringsproposition*) No. 159/2017 for an Act on Secondary Use of Social and Health Data and Related Acts.

45 Latvia, Cabinet of Ministers, Regulations Regarding Unified Electronic Information System of the Health Sector (*Noteikumi par vienoto veselības nozares elektronisko informācijas sistēmu*), 11 March 2014.

46 Portugal, *Ordinance 126/2018 defining the rules for prescription, register and delivery of results of auxiliary diagnostic and therapeutic means and regulates the invoicing of the respective providers to the National Health System*, 5 August 2018.

47 The Netherlands, Minister of Finance (*Minister van Financiën*), *Draft Bill for Banking Information Reference Portal Act [Concept wetsvoorstel. Wet verwijzingsportaal bankgegevens*), May 2018.

48 Register of Enterprises, *Uzņēmumu reģistrs atklāj pirmo publiskās pārvaldes virtuālo asistentu Latvijā – UNA*, Press release, 13 June 2018.

49 Portugal, *Ordinance 267/2018 that amends the framework on electronic conduct of proceedings in judicial, administrative and fiscal courts (Citius/SITAF) (Portaria 267/2018 que procede à alteração dos regimes de tramitação eletrónica dos processos nos tribunais judiciais e nos tribunais administrativos e fiscais (Citius/SITAF))*, 20 September 2018.

50 Poland, Ministry of Digitization (*Ministerstwo Cyfryzacji*), *Konsultacje Komunikatu Komisji Europejskiej dotyczącego sztucznej inteligencji*, 14 June 2018.

51 Slovakia, *Strategic Priority the Data Management* (*Strategická priorita. Manažement údajov*).

52 Sweden, Ministry of Finances (*Finansdepartementet*), *The law as a support for the digitalisation of public administration*, Governmental Official Report (*Juridik som stöd för förvaltningens digitalisering, SOU 2018:25*), March 2018.

53 Austria, Ministry for Transport, Innovation and Technology, Traffic Telematics Report 2018 (*Verkehrstelematikbericht 2018*).

54 Estonia, Republic of Estonia Government Office (*Riigikantselei*), *Self-driving vehicles: beginning of an era* (*Isejuhtivate sõidukite ajastu algus*), 15 February 2018.

55 Spain, Public Prosecutor, *Public Prosecutor's Annual Report*, Madrid, 2018.

56 EDPS, *Ethics Advisory Group Report 2018*, 25 January 2018.

57 European Commission, High-Level Expert Group on Artificial Intelligence, *Draft ethics guidelines for trustworthy artificial intelligence*, 18 December 2018.

58 Council of Europe, Committee of experts on Human Rights dimensions of automated data processing and different forms of artificial intelligence, *Draft recommendation on human rights impacts of algorithmic systems*, MSI-AUT(2018)06, 12 November 2018; and Council of Europe, Committee of experts on Human Rights dimensions of automated data processing and different forms of artificial intelligence, draft declaration on the manipulative capabilities of algorithmic processes, MSI-AUT(2018)07, 16 November 2018.

59 Council of Europe, Committee of Convention 108, *Guidelines on AI and data protection*. See also Council of Europe, Committee of Convention 108, *Report "Artificial Intelligence and Data Protection: Challenges and Possible Remedies"*, 2018.

60 OECD, AI Policy observatory, Paris, 13 September 2018.

61 Austria, Report on Research and Technologie 2018, *Österreichischer Forschungs- und Technologiebericht 2018: Bericht der Bundesregierung an den Nationalrat gem. § 8 (2) FOG über die Lage und Bedürfnisse von Forschung, Technologie und Innovation in Österreich*.

62 See Belgium, Federal Parliament (2018), Commission Robot and Digital Agenda, March 2018; and Belgium, Royal Flemish Academy of Belgium for Science and the Arts (2018), *Artificial Intelligence, Towards a Fourth Industrial Revolution? (Artificiële intelligentie, Naar een vierde industriële revolutie?),* 16 April 2018.

63 Bulgaria, Ministry of Transport, Information Technology, and Communications, *Roadmap 2018-2025* (*Пътна карта 2018-2025*).

64 Lithuania, *National Reform Programme for 2018*.

65 Estonia, Republic of Estonia Government Office (*Riigikantselei*), *Estonia will have an artificial intelligence strategy*, 27 March 2018.

66 Finland, Ministry of Economic Affairs and Employment, *Work in the age of artificial intelligence: four perspectives on economy, employment, skills and ethics*, Publications of the Ministry of Economic Affairs and Employment 19/2018.

67 Sweden, Sweden's innovation agency (*Vinnova*), "*Artificial intelligence in Swedish business and society", Report* (*Artificiell intelligens i svenskt näringsliv och samhälle*), May 2018.

68 Austria, Austrian Council for Robotics and Artificial Intelligence.

69 Denmark, University of Copenhagen, *New centre for artificial intelligence raises Danish research to a higher level Artificial intelligence*, 8 February 2018.

70 The Aalto University, the University of Helsinki and the VTT Technical Research Center of Finland established the Finnish Center for Artificial Intelligence (FCAI).

71 France, French Government, *Report on Artificial Intelligence*, March 2018, p. 91.

72 Sweden, *AI innovation for Sweden*.

73 United Kingdom, HM Government, *Stellar new board appointed to lead world-first Centre for Data Ethics and Innovation*, 20 November 2018.

74 Finland, Government Bill (*hallituksen esitys/regeringsproposition*) No. 159/2017 for an Act on Secondary Use of Social and Health Data and Related Acts.

75 Latvia, Cabinet of Ministers, Regulations Regarding Unified Electronic Information System of the Health Sector (*Noteikumi par vienoto veselības nozares elektronisko informācijas sistēmu)*, 11 March 2014.

76 Portugal, *Ordinance 126/2018 defining the rules for prescription, register and delivery of results of auxiliary diagnostic and therapeutic means and regulates the invoicing of the respective providers to the National Health System*, 5 August 2018.

77 The Netherlands, Minister of Finance (*Minister van Financiën*), *Draft Bill for Banking Information Reference Portal Act [Concept wetsvoorstel. Wet verwijzingsportaal bankgegevens)*, May 2018.

78 Register of Enterprises, *Uzņēmumu reģistrs atklāj pirmo publiskās pārvaldes virtuālo asistentu Latvijā – UNA,* Press release, 13 June 2018.

79 Portugal, *Ordinance 267/2018 that amends the framework on electronic conduct of proceedings in judicial, administrative and fiscal courts (Citius/SITAF) (Portaria 267/2018 que procede à alteração dos regimes de tramitação eletrónica dos processos nos tribunais judiciais e nos tribunais administrativos e fiscais (Citius/SITAF))*, 20 September 2018.

80 Poland, Ministry of Digitization (*Ministerstwo Cyfryzacji*), *Konsultacje Komunikatu Komisji Europejskiej dotyczącego sztucznej inteligencji*, 14 June 2018.

81 Slovakia, *Strategic Priority the Data Management* (*Strategická priorita. Manažement údajov*).

82 Sweden, Ministry of Finances (*Finansdepartementet*), *The law as a support for the digitalisation of public administration*, Governmental Official Report (*Juridik som stöd för förvaltningens digitalisering, SOU 2018:25*), March 2018.

83 Austria, Ministry for Transport, Innovation and Technology, Traffic Telematics Report 2018 (*Verkehrstelematikbericht 2018*).

84 Estonia, Republic of Estonia Government Office (*Riigikantselei*), *Self-driving vehicles: beginning of an era* (*Isejuhtivate sõidukite ajastu algus*), 15 February 2018.

85 Poland, *Ustawa z dnia 11 stycznia 2018 r.o elektromobilności i paliwach alternatywnych*, January 2018.

86 Spain, Public Prosecutor, *Public Prosecutor's Annual Report*, Madrid, 2018.

87 Sweden, Sweden's innovation agency (*Vinnova*) (*Sveriges innovations-myndighet*),"*Artificial intelligence in Swedish business and society*", May 2018, p. 45.

88 Finland, Parliamentary Committee for Future, *Suomen sata uutta mahdollisuutta 2018-2037. Yhteiskunnan toimintamalit uudistava radikaali teknologia*. TuVJ 1/2018 vp.

89 Denmark, SIRI Commission (*SIRI-Kommissionen*), *Etik og AI - scenarier fra SIRI-kommissionen*, September 2018.

90 Finland, Ministry of Economic Affairs and Employment, *Work in the age of artificial intelligence: four perspectives on economy, employment, skills and ethics*, Publications of the Ministry of Economic Affairs and Employment 19/2018, 2018.

91 France, French Government, *Report on Artificial Intelligence*, March 2018.

92 Germany, Federal Government (Die Bundesregierung) (2018), *Strategie Künstliche Intelligenz der Bundesregierung*, 16 November 2018.

93 Poland, Ministry of Digital Affairs (*Ministerstwo Cyfryzacji*) (2018*), Założenia do strategii AI w Polsce Plan działań Ministerstwa Cyfryzacji*, 9 November 2018.

94 United Kingdom, House of Lords, Select Committee on Artificial Intelligence, *Report of Session 2017–19, AI in the UK: ready, willing and able?*, 16 April 2018.

95 *Ibid.*

96 Denmark, Ministry of Industry, Business and Financial Affairs, factsheet, February 2019; and Denmark, SIRI Commission (*SIRI-Kommissionen*), *Etik og AI - scenarier fra SIRI-kommissionen,* September 2018.

97 Finland, Opinion Service, *Draft Government Report "Ethical Information Policy in the Age of Artificial Intelligence"*, October 2018.

98 The United Kingdom, HM Government, *Stellar new board appointed to lead world-first Centre for Data Ethics and Innovation*, 20 November 2018.

99 Austria, *Together. For our Austria. Government Programm 2017-2011 (Zusammen. Für unser Österreich. Regierungsprogramm 2017 – 2022).*

100 Germany, Federal Government (*Die Bundesregierung*) (2018), *Strategie Künstliche Intelligenz der Bundesregierung*, 16 November 2018.

101 European Commission, *AI4EU*, 12 December 2018.

102 Denmark, CREDI - Center for Ret & Digitization.

103 Finland, FCAI society.

104 Italy, Agency for Digital Italy, *White Paper on Artificial Intelligence at the service of citizens*, March 2018, p. 70.

105 The Netherlands, House of Representatives, *Algoritmes en grondrechten*, 2018.

106 The Netherlands, Raad van State, *Advies W04.18.0230/I*, 31 August 2018.

107 Finland, National Non-Discrimination and Equality Tribunal, decision 216/2017, 21 March 2018.

108 France, Le Monde, *Parcoursup:le Défenseur des droits enquête sur des soupçons de discrimination,* 24 August 2018.

109 France, La Quadrature du Net, *Collective complaints filed against the GAFAM! («Dépôt des plaintes collectives contre les GAFAM!»*), 28 May 2018.

110 The Netherlands, Public Interest Litigation Project (PILP), *'State sued for profiling citizens', ['Staat gedagvaard om risicoprofilering burgers']*, News release, 27 March 2018.

111 Before the data are linked through SyRI, the data are transferred into globally unique identifiers. Only the globally unique identifiers for which the system has found an indication of possible violations of the law will be transferred into personal data.

112 Poland, Constitutional Tribunal, Decision K 53/16, 6 June 2018.

113 France, Constitutional Court, Decision n° 2018-765 DC, 12 June 2018.

114 See Ireland, Data Protection Commission, notice of investigation, 3 October 2018.

115 Germany, Hamburg DPA (*Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*), press release, 4 January 2019.

116 FRA (2018), *Fundamental Rights Reports 2017*, Luxembourg, Publications Office, p. 162.

117 Directive 2006/24/EC 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 (Data Retention Directive).

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

119 Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Art. 15(1).

120 CJEU [GC], Joined Cases C-203/15 and C-698-15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 21 December 2016.

121 CJEU, C-207/16, *Ministerio Fiscal*, 3 October 2018.

122 *Ibid.*, para. 49.

123 CJEU, C-207/16, *Ministerio Fiscal*, 3 October 2018, paras. 59-60.

124 *Ibid.*, paras. 55-56, 62-63.

125 *Ibid.*, paras. 26, 50, 63 and operative part.

126 ECtHR, Nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch and Others v. the United Kingdom*, 13 September 2018 (pending before the Grand Chamber).

127 *Ibid.*, paras. 387-388.

128 *Ibid.*, paras. 466-468, 496-499.

129 ECtHR, *Benedik v. Slovenia*, No. 62357/14, 24 April 2018.

130 *Ibid.*, 129-134.

131 *Ibid.*, paras. 105, 117.

132 Austria, Amendment in § 135 (2b) of the Criminal Procedure Code 2018 *(Strafprozessrechtsänderungsgesetz 2018)*.

133 The Netherlands, Ministry of Justice and Security (*Ministerie van Justitie en Veiligheid*) (2018), Data retention ['*Dataretentie*'], Letters Sent to House of Representatives, 26 March 2018 and 25 September 2018.

134 Government's legislative programme for 2018-19 (*Lovprogram for folketingsåret 2018-19*), October 2018.

135 Sweden, Svea Court of a Appeal (*Svea hovrätt*), "Opinion on mid-term report Data retention – crime prevention and integrity, Government report 2017:75" (*Yttrande över delbetänkandet Datalagring – brottsbekämpning och integritet, SOU 2017:75*), Opinion No. 2017/982, p.1, 24 January 2018; Sweden, Data Protection Authority (*Datainspektionen*), "Data retention – crime prevention and integrity, Government report 2017:75" (*Datalagring – brottsbekämpning och integritet, SOU 2017:75*), Opinion No. 02403-2017, 30 January 2018.

136 *Legge 20 novembre 2017, n. 167, "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017"*, confirmed by Article 11 of Legislative Decree No. 101 of 10 August 2018.

137 The Italian DPA's opinion is available on the DPA's website.

138 Germany, Administrative Court Cologne (*Verwaltungsgericht Köln*), 9 K 3859/16 and 9 K 7417/17, 20 April 2018.

139 UK, Court of Appeal (Civil Division), *Secretary of State for the Home Department v Tom Watson & Others*, 30 January 2018; High Court of Justice, Queen's Bench Division, Divisional Court, *The National Council for Civil Liberties (Liberty) v. Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs*, 27 April 2018.

140 Ireland, The High Court, *Graham Dwyer v. Commissioner of An Garda Síochána, Minister For Communications, Energy And Natural Resources, Ireland and Attorney General,* 6 December 2018.

141 Cyprus, Supreme Court, Primary Jurisdiction, *Re. the application of Ioannis Hadjioannou and George Longkritis* for permit to file an application for a certiorari order, Civil application No. 33/2018, 2 May 2018. Cyprus, Supreme Court, Appeal Jurisdiction, *Re. the Application of Artemis Kkolos* for the issue of a certiorari order, 26 April 2017.

142 Czechia, Constitutional Court of the Czech Republic, pending plenary cases, Case No. 45/17.

143 CJEU, C-520/18, request for a preliminary ruling from the Cour constitutionnelle (Belgium) lodged on 2 August 2018 — *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*.

144 CJEU, C-511/18, request for a preliminary ruling from the Conseil d'État (France) lodged on 3 August 2018 — *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.*

145 CJEU, C-746/18, request for a preliminary ruling from the Supreme Court (Estonia) lodged on 29 November 2018 – *H.K. v. Openbaar Ministerie*.

146 See the WP29 code of conduct for cloud service providers.

147 As defined in Art. 2 (3) of the Proposal for a regulation of the European Parliament and of the council on European production and preservation orders for electronic evidence in criminal matters, COM/2018/ 225 final – 2018/0108 (COD).

148 See European Commission, "Security Union: Commission facilitates access to electronic evidence", Press release, 17 April 2018.

149 See Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final – 2018/0107 (COD).

150 See Proposal for a regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters, COM/2018/ 225 final – 2018/0108 (COD).

151 Böse, M., Rheinische Friedrich-Wilhelms-Universität Bonn, *An assessment of the Commission's proposals on electronic evidence*, (2018); study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee.

152 Council of Bars and Law Societies of Europe (CCBE) position on the Commission proposal for a Regulation on European Production and Preservation CCBE position on the Commission proposal for electronic evidence in criminal matters, 19 October 2018.

153 Proposal for a regulation of the European Parliament and of the council on European production and preservation orders for electronic evidence in criminal matters, COM/2018/ 225 final – 2018/0108 (COD), Art. 14.

154 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, recital (32), and Art. 5 and Art. 7.

155 Convention on cybercrime (CETS No. 185), Budapest, 23 November 2001.