UN & CoE

January

19 February – The European Court of Human Rights (ECtHR) declares inadmissible an application brought by two co-founders of The Pirate Bay, one of the biggest file-sharing websites. The *Neij and Sunde Kolmisoppi v. Sweden* case focuses on the violation of their rights to freedom of expression, because the two were convicted of committing crimes under the Copyright Act. Sharing files online falls under the right to "receive and impart information" enshrined in Article 10 of the European Convention on Human Rights (ECHR), but the domestic courts had correctly balanced the applicants' right against the need to protect copyright

25–27 February – In the recommendations of the first 10-year review event of the World Summit on the Information Society, the United Nations Educational, Scientific and Cultural Organization (UNESCO) reaffirms that the same human rights that apply in the offline world should also be protected online

February

March

17 April – The United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression publishes his annual report, indicating that state communications surveillance undermines the human rights to privacy and freedom of expression

18 April – The ECtHR rules in *M.K. v. France* that there were insufficient safeguards for the authorities' collection, retention and deletion of the fingerprints of a person suspected, but not convicted. of theft, violating that person's right to respect for private life

April

May

4 June – The ECtHR concludes that the *Peruzzo and Martens v. Germany* case is inadmissible. The court's order to collect cellphone material from people convicted of serious crimes and store it in databases in the form of DNA profiles was necessary and proportionate

11 June – The Council of Europe Committee of Ministers adopts a Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies

20–21 June – European stakeholders meet in the regional forum European Dialogue on Internet Governance (EuroDIG) to discuss how to use an open and safe internet to serve the public interest

24 June – The Parliamentary Assembly of the Council of Europe (PACE) Committee on Legal Affairs and Human Rights adopts the report *National security and access to information* and urges governments to align their laws in relation to whistleblowers with a set of global principles

25 June 2013 – The ECtHR finds in *Youth Initiative for Human Rights v. Serbia* that the refusal of the Serbian intelligence agency to provide information on the number of people it had subjected to electronic surveillance violated the right of the applicant non-governmental organisation (NGO) to receive information

June

16 July – The ECtHR finds in *Nagla v. Latvia* that the seizure of data storage devices kept in a journalist's home violated the right to freedom of expression, including journalists' right not to disclose their sources

July

August

September

10 October – The ECtHR rules in *Delfi AS v. Estonia* that finding an internet news portal liable for offensive online comments of its readers is a justified and proportionate restriction on the portal's right to freedom of expression

22–25 October – The first focus session on human rights on the internet in the Internet Governance Forum ends with a call to enhance its role in the field of human rights protection on the internet, as well as for the states to consult stakeholders during the legislative procedure

October

8 November – The ministers responsible for media and information society in the Council of Europe member states adopt a political declaration and three resolutions on internet freedom, the role of media in the digital age and the safety of journalists at the Council of Europe Ministerial Conference in Belgrade

November

18 December – The United Nations General Assembly adopts a resolution on the right to privacy in the digital age

December

EU

11 January – The European Cybercrime Centre (EC3) officially opens at the European Union (EU) law enforcement agency (Europol)

January

7 February – The European Commission publishes a *Joint Communication on Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace*

7 February – The European Commission adopts a proposal for a directive on measures ensuring a high common security level across EU network and information systems

February

19 March – The Court of Justice of the European Union (CJEU) adopts its judgment in the *Sophie in 't Veld MEP v. European Commission* case about the transparency of Anti-Counterfeiting Trade Agreement (ACTA) documents, by annulling the Commission Decision of 4 May 2010, which refused to grant access to documents

27 March – The European Commission proposes a new regulation on Europol, which suggests amending data protection safeguards

March

24 April – The European Commission adopts the green paper *Preparing for a fully converged audiovisual world: Growth, creation and value*

24 April – The European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) rejects the EU Passenger Name Record (PNR) proposal

April

13 May – The European Commission presents plans for the Global Internet Policy Observatory to monitor internet-related policy and regulatory and technological developments across the world

30 May – In *Commission v. Sweden*, the CJEU orders Sweden to pay a €3,000,000 lump sum for its delay in transposing the Data Retention Directive into national law

May

10 June – Vice-President Viviane Reding sends a letter to the United States (US) Attorney General to enquire about PRISM and other surveillance programmes

13 June – In *Michael Schwarz v. Stadt Bochum*, the CJEU concludes that the interference of security features and biometrics in EU Member State passports and travel documents with personal data protection is proportionate

25 June – The Council of the European Union approves the comprehensive text delivered by the Friends of the Presidency Group on Cyber Issues regarding the implementation of the European Strategy for Cybersecurity

June

4 July – The European Parliament passes a resolution instructing LIBE to conduct an in-depth inquiry into the US surveillance programmes

July

12 August – The Directive on Attacks against Information Systems is adopted; it will strengthen the protection of personal data by reducing the ability of cybercriminals to abuse victims' rights with impunity

August

11 September – The European Commission presents a proposal for a regulation laying down measures concerning the European single market for electronic communications and to achieve a connected continent

September

21 October – LIBE adopts its report on the General Data Protection Regulation and the separate directive for the law enforcement sector

October

November

10 December – The CJEU Advocate General issues his opinion on the *Commission v. Hungary* case, suggesting a breach of the independence of the Hungarian data protection authority (DPA)

12 December – In his opinion, the CJEU Advocate General concludes that the Data Retention Directive is incompatible with the EU Charter of Fundamental Rights

18 December – The rapporteur of the LIBE inquiry committee on mass surveillance suggests, in his preliminary conclusions, suspending the Safe Harbour and the Terrorist Finance Tracking Programme (TFTP) agreements, creating a European data cloud and guaranteeing judicial redress for EU citizens whose data are transferred to the United States of America (USA)

December

3 Information society, respect for private life and data protection

Unprecedented revelations about the United States' and United Kingdom's mass surveillance of global telecommunication and data flows captured international newspaper headlines for weeks in 2013. This put the issue of privacy in the public spotlight and highlighted the gap between rapidly evolving technologies and current laws safeguarding the right to privacy. The revelations occurred while the EU was in the midst of its most important data protection legislation reform in 20 years and, by forcefully underlining the need for a strong data protection framework, marked a turning point in the debate. Disturbed by these revelations, EU and Member State policy makers took immediate steps to shore up data protection rules, while civil society pushed for greater transparency and more effective remedies before data protection authorities and courts. In reaction to the revelations, the EU legislature successfully incorporated significant reforms into the data protection reform package. Despite some progress, the reform had not been finalised by the end of 2013.

3.1. Mass surveillance revelations spark global concern

Beginning in June 2013, United States National Security Agency (NSA) contractor Edward Snowden leaked documents to several media outlets, revealing operational details of global surveillance programmes carried out by the NSA and by the United Kingdom's Government Communications Headquarters (GCHQ). Of particular interest in the EU, the global programmes targets included EU institutions and Member States' embassies.[1]

Just weeks before these revelations sent shockwaves across the EU and the globe, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, noting this gap between rapidly evolving technologies and current laws safeguarding the right to privacy, pointed out specific shortcomings, such as a lack of judicial oversight of surveillance measures (see also Chapter 10 on EU Member States and international obligations).[2] The UN General Assembly, echoing the calls of the UN Special Rapporteur, asked member states to review their legislation on such surveillance to ensure that it was aligned with their international human rights obligations. It adopted a resolution on the right to privacy in the digital age in December 2013.[3]

Key developments in the area of information society, respect for private life and data protection

- Revelations of mass surveillance reverberate across the areas of information society, privacy and data protection. These revelations cause civil society organisations to protest and call for better protection; they also incite EU and EU Member State policy makers and legislators to adopt more robust measures, tighten legislative protection and propose greater data protection safeguards.
- As a result of the revelations, the UN General Assembly adopts an unprecedented text on the protection of privacy.
- The revelations – which are made while the EU is in the midst of its biggest data protection legislation reform in 20 years – make clear that the fundamental rights protection in the digital world needs greater attention.
- The European Parliament adopts its report on the data protection reform package, but the reform is delayed in the Council of the European Union.

As media published the first revelations, the Council of Europe Committee of Ministers adopted a Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies. The declaration said: "legislation allowing broad surveillance of citizens can be found contrary to the right to respect of private life. These capabilities and practices can have a chilling effect on citizen participation in social, cultural and political life and, in the longer term, could have damaging effects on democracy."[4] On 24 October 2013, the Council of Europe Commissioner for Human Rights published a human rights comment[5] highlighting the threats to human rights and the right to privacy when secret surveillance spreads. In addition, ministers responsible for media and information society adopted a political declaration in November 2013, underlining that "any [...] surveillance for the purpose of the protection of national security must be done in compliance with existing human rights and rule of law requirements".[6]

Table 3.1 details the most publicised surveillance programmes, but subsequent revelations made clear that these represent just the 'tip of the iceberg'.[7]

3.1.1. European Union takes action in response to mass surveillance news

> *"The surveillance scandals have been a wake-up call, and Europe is responding."*
>
> *Vice-President Viviane Reding, 'A data protection compact for Europe', 28 January 2014, Speech/14/62, available at: http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm*

The European Parliament, European Commission and Council of the European Union reacted promptly to the Snowden revelations, taking a number of steps that expressed concern about the mass surveillance programme, sought clarification and worked to rebuild trust, for example, in data flows. Table 3.2 summarises these measures. The European Parliament instructed LIBE to conduct an inquiry.[8] Its draft report, finalised in January 2014, launches 'a European digital habeas corpus for protecting privacy', based on eight concrete actions. These include the adoption of the EU data protection reform package by 2014 (for more on the data protection reform package, see Section 3.2), the enhanced protection of whistleblowers, the development of

Table 3.1: Main surveillance programmes

Name of the programme	Description of alleged programme
PRISM	Provides the NSA with direct access to the central servers of nine leading United States internet companies, allowing them to collect customer material including search histories, the contents of emails, file transfers and live chats.
XKeyscore	Allows NSA analysts to search, without prior authorisation, through vast databases containing emails, online chats and the browsing histories of millions of internet users, as well as their metadata.
Upstream	Collection programmes operated by the NSA, consisting of warrantless wiretapping of cable-bound internet traffic.
Bullrun	Decryption programme run by the NSA in an effort to break through widely used encryption technologies, allowing the NSA to circumvent encryption used by millions of people in their online transactions and emails.
MUSCULAR	Joint programme operated by the NSA and GCHQ to intercept, from private links, data traffic flowing between major platforms such as Yahoo, Google, Microsoft Hotmail and Windows Live Messenger.
Tempora	Upstream surveillance activity allowing GCHQ to access large fibre optic cables that carry huge amounts of internet users' private communications and then share them with the NSA.
Edgehill	Decryption programme, operated by GCHQ, intended to decode encrypted traffic used by companies to provide remote access to their systems.

Sources: Moraes, C. (2013), Working Document 1 on the US and EU surveillance programmes and their impact on EU citizens' fundamental rights, PE524.799v01-00, Brussels, 11 December 2013; Bowden, C. (2013), The US surveillance programmes and their impact on EU citizens' fundamental rights, study for the European Parliament, PE 474.405, Brussels, September 2013

a European strategy for greater IT independence and the suspension of specific US–EU agreements.

The 2013 draft report, adopted in spring 2014,[9] focuses on Decision 2000/520/EC, the so-called Safe Harbour Decision,[10] which provides the legal basis for the transfer of personal data from the EU to US companies. These transfers rest on the Safe Harbour Privacy Principles, and on the Terrorist Finance Tracking Programme (TFTP), the first of which guarantees that the US companies registered offer the 'adequate' level of privacy protection that EU law requires.

The Council of the European Union set up an ad hoc EU–US working group to establish the facts about the US surveillance programmes and their impact on fundamental rights in the EU and on the personal data of EU citizens. On 27 November 2013, the working group published its findings.[11] As well as describing the data protection guarantees in place, the report highlights the discrepancies between the US and the EU data protection legal regimes.

On 27 November 2013, based on the working group's report, the European Commission published two communications on the consequences of the revelations.[12]

The first, the *Communication on the Functioning of the Safe Harbour*, assesses the implementation of the Safe Harbour Decision and recommends a number of improvements.[13] The communication suggests, for example, that companies inform their customers when US public authorities are allowed to collect and process data for reasons of national security, public interest or law enforcement.

The second, the *Communication on Rebuilding Trust in EU–US Data Flows*,[14] assesses the large-scale surveillance's impact on various EU–US agreements. It questions the necessity and proportionality of the US surveillance programmes in the context of national security. The communication highlights the relevance of the data protection reform package in this context. Once adopted, the reform will enhance EU citizens' data

Table 3.2: Key EU documents adopted in the aftermath of the mass-surveillance revelations

Body	Title	Reference
European Commission	10 June 2013 – Vice-President Viviane Reding requests explanations of and clarifications on the PRISM programme	
European Commission	19 June 2013 – Vice-President Reding and Commissioner Cecilia Malmström send a letter to US authorities expressing their concerns about the consequences of US surveillance programmes for the fundamental rights protection of Europeans	
European Parliament	Resolution of 4 July 2013 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy	P7_TA(2013)0322
European Parliament	Resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US NSA surveillance	P7_TA(2013)0449
Council of the European Union	*Report of 27 November 2013 on the findings by the EU Co-chairs of the ad hoc EU–US Working Group on Data Protection*	16987/13
European Commission	*Communication from the Commission to the European Parliament and the Council: Rebuilding trust in EU–US data flows*	COM(2013) 846 final of 27 November 2013
European Commission	*Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU*	COM(2013) 847 final of 27 November 2013
European Commission	*Communication from the Commission to the European Parliament and the Council on the joint report from the Commission and the US Treasury Department regarding the value of TFTP provided data*	COM(2013) 843 final of 27 November 2013
European Parliament	*Draft report of 8 January 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*	PE526.085v02-00

Source: FRA, 2013

protection guarantees (for more on data protection reform, see Section 3.2). It also suggests improving the Safe Harbour Decision and enhancing the safeguards it provides in the context of law enforcement cooperation. It calls for the strengthening of privacy on the internet, which should not undermine the freedom, openness and security of cyberspace (for more on the information society, see Section 3.3).

3.1.2. EU Member States respond to mass surveillance

In EU Member States, reactions to the revelations varied from a complete lack of response to popular protest. In **Finland**, for example, citizens submitted an initiative to reform data protection legislation. Entitled 'Yes we can: The law for safeguarding of freedom of expression and privacy internationally', the proposal was submitted to the Ministry of Justice online service on 8 July 2013, but it has not yet brought about concrete legislative changes.[15] The initiative proposes criminalising disproportionate citizen surveillance and making it a universal crime, whose perpetrators could be prosecuted in Finland even if the act has been committed elsewhere. It also proposes to extend the authorities' and telecommunication operators' liability to report mass personal data collection, storage and use. At the moment, the Finnish Ministry of the Interior alone reports to the European Commission on data retention practices; companies are not obliged to report on their data protection practices at all. The initiative also includes provisions aiming to protecting the legal status of whistleblowers, forbidding their extradition or the rejection of their applications for entry or residence permits.

In **Germany**, the Conference of Data Protection Commissioners sharply criticised the lack of clarification by the US authorities on the scope of the mass surveillance programmes and called on the governments of the Federation and the states (*Länder*) to protect fundamental rights, strengthen the oversight of intelligence services, and stop and prevent any unconstitutional cooperation of intelligence services.[16] Civil society reacted strongly. On 7 September 2013, several thousand people protested in Berlin against surveillance. The rally, organised and supported by a broad coalition of 85 civil liberties organisations, privacy advocacy groups, journalists' federations, political parties and their youth organisations,[17] attracted around 15,000 protestors.[18] Under the banner of 'Freedom Not Fear – Stop Surveillance Mania!' (*Freiheit statt Angst. Stoppt den Überwachungswahn!*), the protestors objected to telecommunications surveillance by secret services, data retention, body scanners, biometrics, passenger name record registration and video surveillance. They called for a strong European data protection regime, an independent evaluation of existing surveillance powers and a moratorium on planned surveillance measures.[19] In addition, new types of group protests boomed: 'walk-ins' near the offices of domestic and US intelligence agencies attracted media attention;[20] and at 'cryptoparties' information technology experts trained people in how to protect and encrypt their data and electronic communications.[21]

Some EU Member States assessed reform of intelligence service legislation in the light of the Snowden revelations. In **France**[22] and **Hungary**,[23] for example, amendments regulating intelligence services' access to personal data prompted criticisms from civil society organisations, politicians[24] and specialist bodies such as the French National Digital Council[25] and the Hungarian DPA,[26] respectively. In November 2013, the Hungarian Constitutional Court validated the related law's constitutionality. The court ruled that a counter-terrorism organisation was not violating the right to privacy by collecting covert intelligence on citizens based on ministerial permission rather than on a court warrant.[27]

On 19 July 2013, the **German** Federal Government presented an eight-point programme to help clarify the facts on mass surveillance and ensure more robust protection of privacy and data. Entitled 'Germany is a country of freedom', the programme suggests the following steps:

1) suspend the administrative agreements on communication surveillance with France, the United Kingdom and the US as quickly as possible;

2) hold expert talks with the US to examine the topic;

3) push for an international data protection agreement (in the form of an additional protocol to Article 17 of the International Covenant for Civil and Political Rights);

4) promote the implementation of the EU Data Protection Regulation, including the obligation for private companies to report data transfers to third countries (see Section 3.2);

5) develop standards under which EU Member States' intelligence agencies may cooperate;

6) develop and implement a European information technology strategy in collaboration with the European Commission;

7) establish a roundtable discussion on the subject of 'security technology for information technology', in public–private partnership with research institutes and private companies;

8) strengthen citizens' information technology security education through an internet safety awareness initiative ('*Deutschland sicher im Netz*').[28]

The German government suspended the administrative agreements with the US in August. It also held talks with France and the United Kingdom. Many questions remain unanswered, however, and it is impossible to know which direction the talks on a so-called 'No Spy Agreement' will take.

In the **Netherlands**, the revelations triggered parliamentary questions. On 2 December 2013, the government established a commission to assess the Act on the Information and Security Agencies 2002 (*Wet op de inlichtingen- en veiligheidsdiensten 2002*). It found that the agencies' powers should be extended, given the new threats to national security from cyberattacks and digital espionage.[29]

In **Slovenia**, the revelations also prompted a parliamentary question. The government responded on 28 November 2013, saying that overarching large-scale surveillance is not permissible, due to human rights protection standards, including data privacy rights, and the rule of law.[30]

3.1.3. Requests for information and remedies

The Snowden revelations also prompted calls for more transparency and prompted some to seek remedies for alleged rights violations before data protection authorities and the ECtHR.

In October 2013, Polish NGOs requested information from various state agencies and institutions on the surveillance programmes.[31] Some, such as the DPA, provided comprehensive answers about their PRISM-related activity. Others responded only in part and in general terms. The Polish Parliament's secret services committee confirmed, for example, that there was neither a meeting on PRISM nor did any individual committee member motion to discuss that mass surveillance programme. Finally, some entities, such as the intelligence services, replied that they could not answer any of the questions because of national security concerns or other confidentiality reasons.[32] All the answers are published online.[33]

The Polish Human Rights Defender called for an investigation into PRISM.[34] The Prosecutor General informed the Human Rights Defender on 19 November 2013 that he had not found any grounds to launch such an investigation.[35]

The Irish data protection authority assessed Facebook's compliance with data protection law in the light of the Snowden revelations. The Irish authority dismissed Europe-v-Facebook.org's complaint as frivolous and vexatious, given that Facebook had acted within the terms of the EU–US Safe Harbour data-sharing agreement.[36] On 21 October 2013, the High Court granted permission to seek judicial review of the Data Protection Commissioner's decision. A hearing on the case is likely to take place in 2014.

The National Commission for Data Protection of Luxembourg said in the summer of2013 that it was looking into data transfers to the NSA by Skype, a voice-over-internet protocol and instant messaging service belonging to US-based information technology company Microsoft. In November 2013, it announced that the transfer of certain types of data to affiliated companies in the United States, as established in the privacy policies of both companies, is operating legally, in accordance with the rules of the adequacy Decision 2000/520/EC of the European Commission to implement the Safe Harbour agreement. Therefore, the DPA found no violation of the legislation's provisions on personal data protection by either Skype or Microsoft. The DPA emphasised that its decision could not be seen as confirming the existence or otherwise of surveillance programmes such as PRISM, since its competence was limited to the two companies' Luxembourg activities.[37]

In September 2013, three civil society organisations and one individual complained before the ECtHR that the United Kingdom's GCHQ surveillance programmes violated their right to privacy under Article 8 of the ECHR. The ECtHR communicated the complaint to the government of the United Kingdom.[38]

3.2. EU recognises need for robust data protection regime

The Snowden revelations in the spring of 2013 marked a turning point in discussions on the EU data protection reform, forcefully underlining the need for a strong data protection framework.

European Commission Vice-President Viviane Reding, who categorised the revelations of mass surveillance as a wake-up call for the EU legislature, emphasised the need for a robust, clear and enforceable data protection legal framework to ensure the protection of the fundamental rights of those living in the EU.

> *"A strong legislative framework with clear rules that are enforceable also in situations when data is transferred and processed abroad is, more than ever, a necessity. It would provide legal certainty and protection for European data subjects and companies."*
>
> *Vice-President Viviane Reding, 'Mass surveillance is unacceptable – US action to restore trust is needed now', 9 December 2013, Speech/13/1048, available at: http://europa.eu/rapid/press-release_SPEECH-13-1048_en.htm*

3.2.1. Reform of the EU data protection regime

Globalisation and the rapid growth of information technology have fundamentally reshaped the way personal data are collected and processed since the 1995 adoption of Directive 95/46/EC.[39] Even before the Snowden revelations, there was a need to strengthen individuals' fundamental rights to data protection and to boost the digital economy in the EU, which led the European Commission, in January 2012, to propose a comprehensive reform of this directive (see Table 3.3).

The new General Data Protection Regulation[40] aims to create a single set of binding EU data protection rules. Once adopted, it will replace Directive 95/46/EC. The Data Protection Directive,[41] which would replace the Data Protection Framework Decision,[42] covers law enforcement authorities' processing of personal data.

In 2013, the European Data Protection Supervisor (EDPS) published additional comments[43] on the reform to ensure that the new data protection regime is effective in practice. Its comments responded to amendments proposed by various European Parliament committees. The Article 29 Working Party also discussed the reform and issued an opinion[44] on the draft directive and a working document[45] on the implementing acts of the draft regulation.

Unprecedented lobbying from partisan US companies and civil society organisations dogged the European legislature as the Parliament worked out the details of the new data reform package. The Chair of the Article 29 Working Party spoke plainly when summarising the intense pressure, stating that European lawmakers were "fed up" with US lobbying.[46] While the lobby groups generally supported the single set of data protection rules that the regulation would set up in the EU, they opposed the supposed administrative burden, increased accountability and heavier fines – to name just a few of the contentious elements.

> *"The scandal has an impact. But MEPs [Members of the European Parliament] are aware that we're also discussing the broader issue: fundamental rights and privacy in general, especially when it concerns the issue of governmental intelligence. […] Another important impact on the debate is that all MEPs, politicians but also individuals now see the importance of having a common European legal framework. This protects our personal rights, also in the internet environment."*
>
> *Jan Philipp Albrecht, Member of the European Parliament, LIBE rapporteur on the draft regulation, Brussels, 26 September 2013*

The LIBE rapporteurs adopted their draft reports on the draft regulation[47] and directive[48] in January, and four other European Parliament committees also released opinions proposing amendments. After months of negotiations on the proposed amendments, LIBE voted on 21 October 2013 by an overwhelming majority in favour of several compromise amendments that would, in broad terms, strengthen the reform package's data protection safeguards. The plenary is to adopt the package in spring 2014.

The LIBE amendments incorporated into the draft strengthen various protections. These include, for example, reinforcing the role to be given to the future European Data Protection Board. They also tighten the rules on consent needed before an individual's data

Table 3.3: Data protection reform package proposals

EU instrument	Title	Reference	European Parliament report
Draft regulation	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)	COM(2012) 11 final, Brussels, 25 January 2012	Draft European Parliament Report voted in LIBE on 21 October 2013: C70025/2012 – 2012/0011(COD)
Draft directive	Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data	COM(2012) 10 final, Brussels, 25 January 2012	Draft European Parliament Report voted in LIBE on 21 October 2013: C70024/2012 – 2012/0010(COD)

Source: FRA, 2013

are processed. They merge the right to data portability with the right of access, allowing individuals to request that their data be moved from one service provider to another. They also subsume the 'right to be forgotten and to erasure' under the 'right to erasure'. Together, these changes make it possible for individuals to request that their personal data be erased from a website. The LIBE amendments also make mandatory the appointment of a data protection officer for any company which processes the data of 5,000 data subjects in any given consecutive 12-month period. They also restrict the grounds for transfer of personal data to countries outside the European Economic Area.

The LIBE amendments focused particularly on strengthening national DPAs, which are required by EU law and function as the first line of defence against data protection violations.

LIBE secured, for example, enhanced DPA independence, the lack of which has been a focus of pointed criticism in recent years. The committee's input ensured that DPAs will be given adequate financial resources and staff to carry out their obligations. These encouraging developments are in line with previous FRA opinions,[49] which expressed concern at the lack of independence of DPAs. LIBE also improved access to remedies by strengthening the DPAs' sanctioning power: sanctions can now include the obligation to perform periodic audits, and fines could be as high as €100 million or 5 % of annual global turnover. These powers are to be exercised "in an effective, proportionate and dissuasive manner". These amendments were supported by FRA findings published in *Access to data protection remedies in EU Member States*.

The Snowden revelations did not lead the Council of the EU to finalise the data protection reform by the end of 2013. EU Ministers of Justice, meeting both informally in January 2013 in Dublin and in July 2013 in Vilnius and at formal Justice and Home Affairs meetings of the Council of the EU, discussed data reform intensively. The main topics of discussion were controllers' obligations, risk-based approaches, specific rules for small- and medium-sized enterprises, 'one-stop-shop' mechanisms enabling complainants to access remedies before a single DPA, the consistency mechanism and questions relating to judicial review and judicial redress.

3.2.2. Key reforms affect data protection authorities

The role data protection authorities play in enforcing data protection guarantees is pivotal. Like other non-judicial bodies protecting fundamental rights, their independence is crucial (see Chapters 8 on access to justice and judicial cooperation, and 10 on EU Member States and international obligations).

FRA ACTIVITY

Researching access to data protection remedies in EU Member States

The FRA conducted research on how data protection violations are remedied in practice in order to identify the main challenges faced by different actors and ways to improve access to such remedies. The research shows that the bodies most commonly turned to when seeking remedies in this field are DPAs, while judicial procedures are rarely used. However, the research, based on an analysis of legal frameworks in the 28 EU Member States complemented by fieldwork research with over 700 people in 16 EU Member States, found great variations in the national DPAs' powers to remedy data protection violations. While some non-judicial bodies have sufficient powers to offer effective remedies, there is minimal coordination between DPAs and other non-judicial bodies. The project identifies other areas where work remains to be done, suggesting, for example, the need for measures raising awareness about EU legislation. The findings of the FRA project *Access to data protection remedies in EU Member States* are feeding into the European Commission's work on the data protection reform package.

For more information, see: Access to data protection remedies in EU Member States, *available at:* http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf

As the FRA stated in its previous annual reports and discussed in the joint Council of Europe–FRA *Handbook on European data protection law*,[50] the CJEU has addressed concerns about the independence of the DPAs. The CJEU interpreted Directive 95/46/EC in terms of independence in two landmark decisions regarding Austria and Hungary.[51] In response to the CJEU judgment of 16 October 2012, which considered that the Austrian DPA lacked independence, **Austria** passed legislation in 2013 amending its legal framework. As of 1 January 2014, a new data protection authority will replace the previous data protection commission.[52] In *European Commission v. Hungary*, a case which also relates to requirements for DPAs' independence, the CJEU is expected to deliver a judgment in 2014. The CJEU Advocate General concluded on 10 December 2013 that **Hungary** had violated EU law by terminating the Data Protection Commissioner's mandate ahead of its stipulated term and recommended that the CJEU declare Hungary in violation of DPA independence requirements.[53]

The consequences of the CJEU case law for DPAs' independence triggered national legislation reform in other EU Member States as well. The **Latvian** Parliament worked on amendments to the Personal Data Protection Law[54] at the end of 2013. The amendments specify the duties and competences of the State Data Inspectorate,

in particular in the area of complaints related to data protection violations. In **Lithuania**, on 27 November 2013, the new regulation strengthening the independence of the Data Protection Inspectorate[55] was approved. Under this regulation, the director is now in charge of the DPA's administrative structure, whereas this was previously a governmental responsibility. The director acts in this context in total independence. The **Slovakian Parliament** passed a data protection law on 30 April 2013, enhancing the transposition of the Data Protection Directive.[56] In **Poland,** the key change discussed was the establishment of local branches of the DPA in order to decentralise the institution and make it more accessible to individuals living outside Warsaw, where it currently has its headquarters, but a lack of funds has so far kept this from happening.

The 2010 FRA report *Data Protection in the European Union: The role of national data protection authorities* considered the appointment procedure for the Greek DPA a promising practice.[57] The Greek constitution requires a four-fifths majority of the Conference of the Presidents, a parliamentary instrument, to approve the appointment of all independent authority members, including of the Greek DPA. This practice still exists. Owing to a lack of broad consensus among current parliamentary political forces, however, it is not always possible to reach the consensus necessary for these appointments. This issue has affected other independent authorities, but not the Greek DPA.

3.2.3. Raising awareness of data protection

That there is a lack of awareness about data protection safeguards is the overarching finding of the FRA report *Access to data protection remedies in EU Member States*. To address this, the FRA and the Council of Europe finalised the publication of an easy-to-use handbook, and DPAs in several EU Member States launched projects, for example creating booklets intended to raise young people's awareness of data protection and ensure that they are better informed of their rights.

FRA ACTIVITY

Presenting EU and Council of Europe law on data protection

FRA, the Council of Europe and the ECtHR drafted a *Handbook on European data protection law* to provide an overview of EU and Council of Europe law on data protection. Designed for legal practitioners who are not specialists in the field of data protection, the handbook examines the relevant law in this field stemming from both European systems, including important selected case law.

For more information, see: Handbook on European data protection law, *available at:* http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law_en.pdf

Promising practice

Fighting misuse of children's personal data and raising awareness

In several Member States, DPAs implemented various activities targeted specifically at protecting children (see Chapter 4 on the rights of the child and the protection of children).

The German State Commissioner for Data Protection and Freedom of Information in Rhineland-Palatinate launched the first German DPA website to specifically target young people. It raises awareness of data protection issues and disseminates knowledge on how to protect personal data in general and on the internet in particular. It provides concrete suggestions about how to protect personal data when using social media or games consoles.

For more information, see: www.youngdata.de

The Hungarian National Authority for Data Protection and Freedom of Information issued a booklet on data protection for children.[58] Its purpose is to draw attention to the risks of children's internet use, specifically of those aged 10–16, to identify future challenges and to promote the conscious use of the internet and the exercise of privacy rights.

For more information, see: Hungarian National Authority for Data Protection and Freedom of Information (2013), Key to the World of the Internet!, available at: www.naih.hu/files/2013-projektfuzet-internet.pdf

3.2.4. Reform and implementation of the Data Retention Directive

The EU continues its work on revising the Data Retention Directive,[59] which supports the fight against crime and terrorism by requiring telecommunications service providers to retain traffic and location data for between six months and two years from the date of the communication.

Several EU Member States amended their legislation, while others questioned the legality of the adopted laws transposing the Data Retention Directive into national law. The **Belgian** Government for example, adopted a royal decree transposing the Data Retention Directive into Belgian law.[60] In **Poland**, a legislative amendment to the telecommunications law reduced the data retention period to 12 from 24 months and prohibited the use of data retention in civil proceedings.[61] The **Danish** Parliament decided to postpone its review of data retention rules until the parliamentary year 2014–2015, in order to await the revision of the Data Retention Directive.[62] The **Slovenian** Information Commissioner requested a constitutional review of the new Electronic Communications Act governing data

retention, which entered into force in January 2013.[63] According to the Constitutional Court, this task falls under the exclusive competence of the CJEU, so it delayed a review until the CJEU delivers its decisions on the related joined cases of Ireland and Austria, C-293/12 and C-594/12 respectively.[64]

On 12 December 2013, a CJEU Advocate General issued his opinion on the joined cases of Ireland[65] and Austria[66] in relation to the Data Retention Directive. The preliminary rulings concerned the compatibility of the Data Retention Directive with key fundamental rights. For the Advocate General, "The Data Retention Directive is as a whole incompatible with Article 52 (1) of the Charter of Fundamental Rights of the European Union, since the limitations on the exercise of fundamental rights which that directive contains because of the obligation to retain data which it imposes are not accompanied by the necessary principles for governing the guarantees needed to regulate access to the data and their use."

3.2.5. Google

Google privacy policy

The **French** DPA ordered Google on 20 June 2013 to comply with French data protection law within three months. When Google did not comply, the French DPA initiated a formal procedure for imposing sanctions, fining Google €150,000 on 3 January 2014.[67]

The **United Kingdom**'s DPA said in July 2013 that Google's privacy policy raised serious concerns about its compliance with the Data Protection Act and that it was investigating.[68] The Information Commissioner's Office (ICO) instructed Google to revise its privacy policy by 20 September to make it more informative.[69] In the absence of any changes, the ICO could initiate formal enforcement actions, but by the end of the reporting period the DPA had not taken any action.

The **Spanish** DPA fined Google €300,000 on 19 December 2013 for violating Spanish data protection law, saying that Google had carried out illegal processing linked to its new privacy policy.[70]

Google search engines

In **Germany**, the Federal Court of Justice decided in favour of complainants who demanded that Google stop a search engine function that resulted in the automated display of compromising terms when the complainants' names were typed into the Google search field. The court did not expect Google to take precautionary measures to prevent this function's unintended effects from ever occurring. The judges ruled, however, that the company must examine affected people's claims and stop the automated display of terms, called 'predictions', shown when searching a person's name if this is necessary to protect complainants' privacy.[71]

In another case, an individual who wanted material erased from a newspaper internet page lodged a complaint with the Spanish Data Protection Authority (AEPD). In this case, the Spanish DPA held that the material was lawfully published and declined to order removal. The case went to the Spanish National High Court (*Audiencia Nacional*), which proceeded to refer a series of preliminary questions to the CJEU. In *Google v. AEPD*, the CJEU Advocate General issued his opinion on 25 June 2013.[72] The Advocate General concluded that Google was not responsible for the information or the dissemination of search result data. The Advocate General declined to classify Google as a 'controller' of personal data within the meaning of the Data Protection Directive and, finally, considered that the directive does not provide for a general 'right to be forgotten'. The CJEU will deliver its judgment in 2014.

Google Street View

In July 2013, Google started photographing **Slovenian** streets for its Google Street View application. The Information Commissioner reported that Google had committed to adopting measures aimed at reducing the interference with privacy, which inevitably occurs in such cases. These measures include: informing the public regularly on the locations of Google cars; providing more information on the street view application; blurring faces and number plates in photographs before publication; installing a 'report error' button on each image; introducing security procedures and measures for the protection of collected data; training drivers; and adapting shooting schedules and locations.[73]

3.3. Information society: EU moves to protect and codify fundamental rights online

Modern technologies have a considerable impact on the protection of fundamental rights, since they present fresh ways to fully realise these rights while also posing new challenges to their protection. The Snowden revelations on mass surveillance provided a prominent example. For the first time in 2013, the Internet Governance Forum[74] organised a plenary session on human rights on the internet. Access to and use of the internet from a human rights perspective were at the forefront of discussions. It was unanimously accepted that human rights and freedom of expression online should remain a priority of the Governance Forum's agenda.[75]

3.3.1. The protection of fundamental rights online

The protection of fundamental rights in the digital environment is a much discussed issue. It is now universally accepted that human rights online are protected to the same extent as they are in the physical world.[76] At regional level, the Council of Europe adheres to this view, affirming in its Internet Governance Strategy that human rights law applies equally online and offline.[77] The EU has also accepted in its Cybersecurity Strategy that core EU values apply both in the physical and in the digital world and that fundamental rights, as enshrined in the EU Charter of Fundamental Rights, should be promoted in cyberspace.[78]

> *"For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline should also apply online."*
>
> *Cecilia Malmström, EU Commissioner for Home Affairs, 'Delivering a cybersecurity strategy to protect an interconnected Europe', 16 May 2013, Speech/13/423, available at: http://europa.eu/rapid/press-release_SPEECH-13-423_en.htm?locale=en*

The European Commission Cybersecurity Strategy emphasises the respective tasks of key government and private sector players: governments need to safeguard access and openness, respect and protect fundamental rights online and maintain the reliability and interoperability of the internet. The private sector owns and operates significant parts of cyberspace, and so any initiative in this area must recognise its leading role if it is to succeed.[79]

3.3.2. Codifying fundamental rights online

The private sector's contribution is essential when it comes to the implementation of fundamental rights online. In fact, representatives of the private sector, individuals, NGOs and government actors are working together on all matters related to the internet's development. In 2013, the multi-stakeholder approach achieved concrete results in the codification of online fundamental rights. Both the draft Council of Europe guide to human rights for internet users and the Charter of Human Rights and Principles for the Internet were made available. In addition, the EU published the Code of EU Online Rights. Table 3.4 shows the similarities and differences between these texts.

The European Commission's proposal for a regulation laying down measures concerning the European single market for electronic communications and to achieve a connected continent[80] establishes the freedom of end-users to access and distribute information and content, run applications and use services of their choice via their internet access service. It aims to guarantee a truly free and open internet; operators are prohibited from blocking, slowing down, degrading or discriminating against specific content, applications and services, or specific classes thereof, except in a very limited number of cases when reasonable traffic management can be applied. These measures must be transparent, non-discriminatory and proportionate.

The Code of EU Online Rights,[81] published on 21 December 2012, does not establish new rights, nor is it directly enforceable. It summarises and consolidates the minimum existing rights deriving from EU legislation on electronic communications, electronic commerce, data protection and consumer protection. According to the code, the fundamental rights enshrined in the EU Charter of Fundamental Rights should be respected and the open and neutral character of the internet should be preserved.

The Charter of Human Rights and Principles for the Internet is the flagship document of the Internet Rights and Principles Dynamic Coalition.[82] This coalition is part of the Internet Governance Forum, which provides a neutral space for all stakeholders to discuss issues related to internet governance.[83] The coalition consists of researchers, lawyers, activists, NGOs, intergovernmental organisations, government representatives and internet service providers. The Charter is based on existing human rights standards, notably the Universal Declaration of Human Rights. It should serve as a policy document for all stakeholders. It is underpinned by the idea that everyone has the right to access and make use of the internet. Based on the consultations for the Charter, the Coalition also compiled 'Ten Internet Rights and Principles' which must form the basis of internet governance.[84] Some of these principles draw directly on fundamental rights such as free expression, privacy, life, liberty and security.

In line with the its Internet Governance Strategy for the years 2012–2015,[85] the Council of Europe finalised a draft guide to human rights for internet users.[86] The guide raises awareness and helps internet users understand, exercise and enjoy the rights they have online. It does not create new rights but builds on the rights enshrined in the ECHR and other Council of Europe documents, as interpreted by the ECtHR. The guide provides information about their application to online environments. It should be adopted by the Council of Europe Committee of Ministers in 2014.

3.3.3. Corporate social responsibility

As a result of the multi-stakeholder model underpinning internet governance, private sector actors play an important role in safeguarding fundamental rights in the digital environment. The UN Guiding Principles on Business and Human Rights have gained broad acceptance and are the global reference point for business and human rights. They are based on the three pillars of the UN 'Protect, Respect and Remedy' Framework, which are:

Table 3.4: Codification of fundamental rights online

Name	Created by	Legal basis	Legal standing	Purpose	Rights covered
Code of EU Online Rights	European Commission (Digital Agenda, Action 16)	EU legislation on electronic communication, electronic commerce, data protection and consumer protection	It does not establish new rights nor is it directly enforceable. It consolidates minimum existing rights	To increase consumer awareness and confidence, in order to promote the use of online services	Rights and principles applicable when accessing and using online services Rights and principles applicable when buying goods or services online Rights and principles protecting consumers in case of conflict
Charter of Human Rights and Principles for the Internet	Internet Rights and Principles Dynamic Coalition	The Universal Declaration of Human Rights and other covenants that make up the International Bill of Human Rights at the United Nations	Not binding	To provide: a reference point for dialogue and cooperation between different stakeholders, a document that can frame policy decisions for the local, national and global dimensions of internet governance and an advocacy tool for governments, businesses and civil society	Right to access the internet, right to non-discrimination in internet access, use and governance, liberty and security, development through the internet, freedom of expression and information, freedom of religion and belief, freedom of online assembly, privacy, digital data protection, access to knowledge, rights of the child, rights of people with disabilities, right to work, online participation in public affairs, consumer protection, health and social services, legal remedy and fair trial for actions involving the internet, appropriate social and international order for the internet, duties and responsibilities on the internet, general clauses
Guide on human rights for internet users	Council of Europe Committee of Ministers	The European Convention on Human Rights and other Council of Europe conventions and instruments as interpreted by the European Court of Human Rights	Not binding. It does not create new rights. It is neither an exhaustive nor a prescriptive explanation of human rights standards	To raise awareness and serve as a tool to help every internet user without specialised knowledge to understand and take advantage of their online rights	Access and non-discrimination, freedom of expression and information, assembly, association and participation, privacy and data protection, education and literacy, children and young people, effective remedies

Source: FRA, 2013

- the state duty to protect against human rights abuses by third parties, including businesses;
- the corporate responsibility to respect human rights, meaning both to avoid human rights violations and to address the negative consequences if companies are involved in such violations;
- the need for greater access to effective remedies for victims of business-related human rights violations, through both judicial and non-judicial means (see Chapter 10 on Member States and international obligations).[87]

As part of its policy on corporate social responsibility,[88] the European Commission issued in June 2013 three guides applying the UN Guiding Principles in the following business sectors: employment and recruitment agencies, ICT, and oil and gas. The *ICT sector guide*[89] is not a legally binding instrument, but it is designed to help all ICT companies effectively implement the principles into their policies. In particular, the guide sets out the key elements of corporate social responsibility to respect human rights, which are: developing a human rights policy commitment; carrying out a human rights impacts assessment, whose findings should then be integrated; tracking and communicating how effectively the impacts are addressed; and putting in place remedy mechanisms. For each of these elements, the guide summarises the standards set out in the UN Guiding Principles, explains why they is important and offers guidance, indicating possible approaches the company could use to tackle the issues. It also offers a list of resources for further information and provides examples from everyday business life, such as how an ICT company uses icons to inform users on privacy issues or how a telecommunications company has developed a global framework agreement.

3.3.4. Intermediary liability

The extent to which an internet portal can be held accountable for content uploaded by users of blogs or news portals is a topic of debate. It raises the question of the scope of intermediary liability, particularly in cases where defamatory comments are posted by such readers. The ECtHR judgment in the *Delfi AS v. Estonia* case[90] raised considerable concern among internet actors. The ECtHR held that finding a portal liable for offensive comments posted by readers below one of the online articles was a justified and proportionate restriction to the portal's right to freedom of expression.

In **Poland**, the Supreme Administrative Court[91] held that an individual has the right to ask an internet service provider to disclose email and internet protocol addresses associated with offensive online communications, because such data are necessary for the victims of an online privacy breach to claim their rights effectively before the court. Most internet service providers had claimed that, according to e-commerce law,[92] these data could be accessed only by enforcement agencies, and courts had usually accepted this argument. The Supreme Administrative Court, however, ruled that internet service providers should allow individuals to access the data if this serves a legitimate aim and is proportionate to the circumstances of a particular case.

In the **United Kingdom**, the Court of Appeal issued its decision in the *Tamiz v. Google* case,[93] which concerned Google's liability for defamatory comments posted on a blog hosted by Google's blog service. The High Court had held that Google cannot be considered a publisher due to its passive role in relation to individual blog posts and comments. The Court of Appeal generally supported these findings. It considered separately, however, the period after the notification of the complaint, concluding that Google might as well have become a publisher, since it allowed the defamatory comments to remain on the blog after the notification. The appeal was dismissed, nonetheless, since the court found that the damage to the applicant's reputation was trivial.

Many consider the Google–Vividown case the most significant **Italian** case on internet rights. In February 2013, the Court of Appeal overturned the first instance ruling, which had sentenced three Google managers to six months in prison because Google's search engine broadcast a video showing a boy with disabilities being bullied. The Court of Appeal held that the uploader of the video was responsible, not the hosting site.

3.3.5. Right to an effective remedy

FRA ACTIVITY

Securing remedies for online data protection violations

The FRA report *Access to data protection remedies in EU Member States,* drafted in 2013 and published in 2014, examines the availability of EU remedy mechanisms to address data protection violations. It identifies challenges faced by individuals and suggests improvements. The data protection violations most frequently mentioned during the fieldwork research in 16 EU Member States relate to internet-based activities. This includes social media, online shopping, leakage of personal data from e-shops, email account and database hacking, identity theft, security breaches and misuse of personal data by global internet companies. It is for this reason that effective remedies on the internet need to be put in place. (see also Section 3.2.3)

For more information, see: FRA (European Union Agency for Fundamental Rights) (2014), Access to data protection remedies in EU Member States*, Luxembourg, Publications Office of the European Union (Publications Office)*

The internet's uniqueness does not alter the principle that victims of fundamental rights violations need access to remedies. The right to an effective remedy is enshrined in all the main documents mentioned that set out internet users' fundamental rights. The frequent violation of rights online makes the existence of proper remedy mechanisms in the information society field indispensable. At the same time, the crucial role the private sector plays in internet governance creates challenges for the proper implementation of remedial avenues.

Promising practice

In France, the DPA created an online document, available on its website, entitled "How do I remove personal information from a search engine?" This tip sheet gives instructions about the procedure to be followed, including a template for a letter to be sent to the webmaster of the site and information about the procedure for voluntary deindexation of the website.

For more information, see: www.cnil.fr/documentation/fiches-pratiques/fiche/article/comment-effacer-des-informations-me-concernant-sur-un-moteur-de-recherche/

3.3.6. Fighting cybercrime

The EU adopted a number of policy initiatives in 2013 aimed at strengthening the fight against cybercrime. In a majority of cases, criminal activities conducted online result in infringements of human rights and fundamental freedoms. The EU cybersecurity strategy, adopted on 7 February 2013, sets out as one of its main principles the protection of fundamental rights, freedom of expression, personal data and privacy, and it expresses the view that 'individuals' rights cannot be secured without safe networks and systems'. At the same time, the strategy states that 'cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and the EU core values'.

Some clear examples of violations of human rights and fundamental freedoms by criminal activities carried out online are the production and dissemination of child sexual abuse content, which is a gross violation of the children's rights, and also intrusions into IT systems, which in most cases has a direct impact on users' privacy and/or result in data breaches.

To step up the fight against cybercrime, with the objective of better protecting citizens' fundamental rights, the EU legislature adopted, on 12 August 2013, a directive on attacks against information systems. This directive complements the already adopted Directive 2011/93/EU of 13 December 2011, which introduced common measures against the sexual abuse and sexual exploitation of children and child pornography.

Furthermore, the European Cybercrime Centre (EC3) was created in January 2013 within Europol, becoming the European focal point in the fight against cybercrime, with the main task of assisting in and coordinating cross-border cybercrime investigations in the following three priority areas: intrusion, child sexual abuse online and payment card fraud.

The findings of three wide-scale FRA surveys on lesbian, gay, bisexual and transgender (LGBT) people, violence against women and antisemitism reveal that online manifestations of hate crime are an increasingly serious problem, as the internet can be used as a platform for hate and harassment. The anonymity the internet affords may lead some users to publish offensive material online.

The findings of the FRA EU LGBT survey[94] showed that, in the 12 months prior to the survey, one in five (19 %) of all respondents were victims of harassment, which they thought happened in part or completely because they were perceived to be LGBT.[95] Almost one in 10 (9 %) of the most recent incidents of hate-motivated harassment and 6 % of the most serious experiences of discrimination happened online.[96]

Data from the FRA survey on gender-based violence against women[97] show that one in 10 (11 %) women in the EU has been a victim of cyberharassment at least once since the age of 15, and 5 % were victims of cyberharassment in the 12 months before the survey. The risk of women aged 18–29 becoming the target of threatening or offensive advances on the internet is twice as high as it is for women aged 40–49 and more than three times higher than it is for women aged 50–59. Based on the FRA survey, 5 % of women in the EU have experienced one or more forms of cyberstalking[98] since the age of 15, and 2 % did so in the 12 months preceding the survey. Taking the victim's age into consideration, the 12-month rates vary from 4 % among 18–29 year olds to 0.3 % among women aged 60 and over.

The FRA survey on discrimination and hate crimes against Jews[99] indicates, similarly, that victims see online antisemitism as a serious problem. Three quarters of all respondents (75 %) view it as either 'a very big' or a 'fairly big problem', and almost as many (73 %) believe it has increased over the past five years. Overall, 10 % of respondents have experienced offensive or threatening antisemitic comments made about them on the internet.

In the **United Kingdom**, two people who made abusive and menacing comments to a feminist campaigner on Twitter were sentenced to 12 and eight weeks in

prison.[100] The recipient of the menacing tweets characterised this case, however, as a "small drop in the ocean" compared with the hate speech she and other women had been subjected to online. The case exemplifies the major problems faced and the challenge of finding solutions using traditional legal means.

Action is needed to prevent the misuse of the internet as a zone where hate crime can be committed with impunity. The EU and its Member States should identify effective methods and promising practices to address growing concerns about online hate. This is particularly true because the nature of online hate crime implies an issue that is not confined within the borders of individual Member States but a cross-border problem that must be tackled jointly (see Chapter 6 on racism, xenophobia and related intolerance).

FRA ACTIVITY

Tackling cyberhate

The FRA organised its annual fundamental rights conference for 2013 on the subject of hate crime, including a workshop dedicated to cyberhate. The conference workshop, held in Vilnius on 12–13 November 2013, discussed problems related to the rise of cyberhate, the challenges in combating it, good practices and possible solutions. Key points raised include the need to strengthen education, training and cyberliteracy for all actors, including law enforcement, users, companies and governments, as well as enhancing transparency and reporting in order to raise awareness. This could be achieved by reducing the anonymity of users while ensuring data protection. As online hate speech is a global problem, a common approach is needed. The differences in legislation and the criminal codes' definitions should be harmonised, so that victims are all treated on equal terms. Minimum standards on what is absolutely not allowed should also be set. Other suggestions concerned the development of mechanisms to report unwanted content that go beyond the legal prosecution of hate speech. To raise young people's awareness and respond to the challenge of impunity, participants strongly suggested establishing cyber-actors in law enforcement within private services and content and platform providers, such as an ombudsman for Facebook. Good practices reported include child helplines in the **United Kingdom**, dedicated police officers for cyberhate in **Finland**, awareness-raising campaigns in **Denmark** and a **Belgian** Federal Police unit working in schools and engaging with potential victims.

At national level, EU Member States have also become active in ensuring respect for human rights in the digital environment and promoting awareness-raising campaigns. In **Austria**, the Advisory Board on the Information Society at the Federal Chancellery met four times in 2013[101] to discuss relevant developments at European and global level – such as the European Commission's Digital Agenda for Europe,[102] the telecommunications package,[103] the Internet Governance Forum and the European Dialogue on Internet Governance (EuroDIG)[104] – and at national level, such as strengthening information security in Austria and providing a safer internet. In this context, Safer Internet Day, on 5 February 2013, dealt with online rights and responsibilities. The **French** government announced its roadmap for digital issues at the end of February.[105] As well as increasing the use of information and communications technologies among young people and enhancing the competitiveness of companies through digital technologies, the roadmap also aims to ensure the protection of civil liberties on the internet.

Promising practice

Discouraging children's risky online behaviour

The **Spanish** initiative 'You choose', aimed at 10–15 year olds, uses worksheets and a comic to make students think about the possible consequences of their online actions. There is a focus on social networks and risk situations such as cyberbullying and online sexual harassment.

For more information, see: www.agpd.es/portalwebAGPD/index-ides-idphp.php

FRA ACTIVITY

Putting numbers to gender-based violence against women

The FRA EU-wide survey on gender-based violence against women shows that 5 % of women in the EU have experienced one or more forms of cyberstalking since the age of 15, and 2 % experienced it in the 12 months preceding the survey. Compared with an average 2 % prevalence of experiences of cyberstalking for all women, those in the youngest age group in the survey, 18–29, were most affected. For these women, cyberstalking accounted for the majority of their experiences of stalking in the 12 months before the survey.

The survey defined three specific behaviours as cyberstalking: sending emails, text messages (SMS) or instant messages that were offensive or threatening; posting offensive comments about the respondent on the internet; and sharing intimate photos or videos of the respondent on the internet or by mobile phone. To be considered stalking, these incidents had to take place repeatedly and the same person had to perpetrate them.

Outlook

The mass surveillance scandal that affected users' confidence in the internet and violated their privacy will influence policy development in 2014. How users' trust in information technologies and communications will be restored will dominate the debates linked to the information society, privacy and data protection. The Snowden revelations will necessarily result in calls for enhanced fundamental rights compliance in any discussions linked to internet governance. Follow-up initiatives, launched in 2013, will necessitate increased involvement of policy makers and the private sector, with private sector actors needing to engage more in fundamental rights enforcement.

At EU level, the data protection reform package will remain high on the EU legislature's agenda. The Council of the European Union and the post-election European Parliament will need to enter negotiations quickly to make it possible to adopt the reform by the end of 2014. CJEU judgments will also continue to provide guidance on how to amend legislation; those issued on the Data Retention Directive directly affected data protection safeguards and also clarified the independence required of data protection authorities.

Index of Member State references

Endnotes

All hyperlinks accessed on 30 April 2014.

1 Bigo, D., Carrera, S., Hernanz, N. Jeandesboz, J., Parkin, J., Ragazzi, F. and Scherrer, A. (2013), *Mass surveillance of personal data by EU Member States and its compatibility with EU law*, Centre for European Policy Study (CEPS) paper in *Liberty and Security in Europe*, No. 61, p. 2.

2 United Nations (UN), Human Rights Council (2013), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17 April 2013, para. 50 and 51, www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

3 UN, General Assembly (2013), Resolution 68/167 on the right to privacy in the digital age, 18 December 2013, www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167.

4 Council of Europe, Committee of Ministers (2013), Declaration of the Committee of Ministers on risks to fundamental rights stemming from digital tracking and other surveillance technologies, 11 June 2013, wcd.coe.int/ViewDoc.jsp?id=2074317&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

5 Council of Europe, The Council of Europe Commissioner's human rights comment (2013), *Human rights at risk when secret surveillance spreads*, http://humanrightscomment.org/2013/10/24/human-rights-at-risk-when-secret-surveillance-spreads/.

6 Council of Europe, Conference of Ministers responsible for Media and Information Society (2013), *Political declaration: Freedom of expression and democracy in the digital age, opportunities, rights, responsibilities*, 8 November 2013, www.coe.int/t/dghl/standardsetting/media/belgrade2013/Belgrade%20Ministerial%20Conference%20Texts%20Adopted_en.pdf.

7 *Ibid.*, p. 1.

8 European Parliament (2013), Resolution on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy, 4 July 2013, Brussels, www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN.

9 European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2014), Draft Report 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, www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-526.085%2b02%2bDOC%2bPDF%2bV0%2f%2fEN.

10 European Commission (2000), Decision 2000/520/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, Brussels, 26 July 2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

11 Council of the European Union (2013), Report on the findings by the EU Co-chairs of the ad hoc EU–US Working Group on Data Protection, Doc. 16987/13, Brussels, 27 November 2013.

12 European Commission (2013), Communication to the European Parliament and the Council: Rebuilding trust in EU–US data flows, COM(2013) 846 final, Brussels, 27 November 2013; European Commission (2013), Communication to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU, COM(2013) 847 final, Brussels, 27 November 2013.

13 European Commission (2013), Communication to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU, COM(2013) 847 final, Brussels, 27 November 2013.

14 European Commission (2013), Communication to the European Parliament and the Council: Rebuilding trust in EU–US Data Flows, COM(2013) 846 final, Brussels, 27 November 2013.

15 Finland, 'Kyllä me voimme: Laki sananvapauden ja yksityisyydensuojan kansainvälisestä turvaamisesta (Lex Snowden)'https://www.kansalaisaloite.fi/fi/aloite/442, www.kansalaisaloite.fi/fi/aloite/442.

16 Germany, Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2013), 'Entschließung: Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen', Resolution, 5 September 2013, www.datenschutz.bremen.de/sixcms/detail.php?gsid=bremen236.c.9292.de.

17 Demonstration ‚Freiheit statt Angst' (2013), *Bündnispartner 2013*. See: http://blog.freiheitstattangst.de/bundnispartner-2013/.

18 Spiegel Online (2013), 'NSA-Protest in Berlin. Freiheit unterm Alu-Hut', 7 September 2013, www.spiegel.de/netzwelt/netzpolitik/freiheit-statt-angst-2013-demonstration-gegen-nsa-ueberwachung-a-920927.html.

19 Demonstration 'Freiheit statt Angst' (2013), 'Unsere Forderungen', http://blog.freiheitstattangst.de/unsere-forderungen/.

20 Spiegel Online (2013), 'Proteste am Dagger Complex. Mit Lampions gegen die NSA', 1 September 2013; Deutsche Welle, 'Verhaltener Protest gegen NSA-Überwachung', 30 July 2013, www.dw.de/verhaltener-protest-gegen-nsa-%C3%BCberwachung/a-16986575.

21 Deutsche Welle (2013), 'Cryptoparties boom following NSA scandal', 20 July 2013, www.dw.de/cryptoparties-boom-following-nsa-scandal/a-16964049.

22 France, Loi n° 2013-1168 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, 18 December 2013, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte=&categorieLien=id.

23 Hungary, *Egyes törvényeknek a nemzetbiztonsági ellenőrzés új szabályainak megállapítása érdekében szükséges módosításáról szóló 2013. évi LXXII. törvény.*

24 Untersinger, M. (2013) 'Surveillance d'Internet: Inquiétudes autour de la loi de programmation militaire', *Le Monde*, 26 November 2013, www.lemonde.fr/technologies/article/2013/11/26/surveillance-d-internet-inquietudes-autour-de-la-loi-de-programmation-militaire_3518974_651865.html. See also: Hungary, *Társaság a Szabadságjogokért*, http://tasz.hu/adatvedelem/megfigyelessel-korrupcio-ellen.

25 France, Conseil National du Numérique (2013), *Avis sur les libertés numériques n° 2013-5*, 6 December 2013, www.cnnumerique.fr/libertes-numeriques/.

26 Hungary, Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH-4867-4/2012/J, response letter provided for the purposes of the present report by the National Authority for Data Protection and Freedom of Information to data request, 24 November 2013.

27 Hungary, Alkotmánybíróság, *32/2013. (XI. 22.) AB határozat*, 22 November 2013.

28 Germany, Bundesregierung (2013), 'NSA-Aufklärung. Deutschland ist ein Land der Freiheit', Press release, 19 July 2013, www.bundesregierung.de/ContentArchiv/DE/Archiv17/Artikel/2013/07/2013-07-19-bkin-nsa-sommerpk.html.

29 The Netherlands, Commissie evaluatie Wiv 2002 (2013), *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002*, www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/12/02/rapport-evaluatie-wiv-2002.html.

30 Slovenia, Ministrstvo za pravosodje, 'Sporočila za javnost po 35. redni seji Vlade RS', Press release, 28 November 2013, www.mp.gov.si/si/novinarsko_sredisce/novica/select/sporocilo_za_javnost/article/12447/6713/592f3cdc597266ddb17c10a531c7e0e6/?tx_ttnews%5Byear%5D=2013&tx_ttnews%5Bmonth%5D=11.

31 Finland, Helsińska Fundacja Praw Człowieka (2013), '100 pytań o inwigilację do polskich władz', Press release, 16 October 2013, www.hfhr.pl/100-pytan-o-inwigilacje-do-polskich-wladz.

32 The Helsinki Foundation for Human Rights (HFHR) complained against the Central Anti-Corruption Bureau's refusal to provide some of the requested information and asked the other intelligence agencies which refused to provide information to reconsider this request.

33 Finland, Helsińska Fundacja Praw Człowieka (2013), 'Amerykański program PRISM – odpowiedzi na wnioski o informację publiczną', Press release, 6 December 2013, www.hfhrpol.waw.pl/precedens/aktualnosci/amerykanski-program-prism-odpowiedzi-na-wnioski-o-informacje-publiczna.html.

34 Poland, Rzecznik Praw Obywatelskich, 'Wystąpienie do Prokuratora Generalnego w sprawie zapobiegania sytuacjom nieautoryzowanego przetwarzania danych osobowych polskich internautów', RPO/738662/13/I/115.2 RZ, Press release, 23 September 2013.

35 Poland, Prokurator Generalny (2013), PG Ko$_1$ 2353/13, 19 November 2011.

36 Irish Times (2013), 'Facebook decision can be reviewed', 24 October 2013, www.irishtimes.com/business/sectors/technology/facebook-decision-can-be-reviewed-1.1571049.

37 Luxembourg, Commission nationale pour la protection des données (2013), 'Pas de violation constatée en matière de protection des données de la part de Skype et Microsoft au Luxembourg', Press release, 18 November 2013, www.cnpd.public.lu/fr/actualites/national/2013/11/skype-microsoft/index.html.

38 European Court of Human Rights (ECtHR), *Big Brother Watch and others v. the United Kingdom*, No. 58170/13, communicated on 9 January 2014; see also European Court of Human Rights (ECtHR), *Centrum för Rättvisa v. Sweden*, No. 35252/08.

39 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281.

40 European Commission (2012), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012.

41 European Commission (2012), Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25 January 2012.

42 Council of the European Union (2008), Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Data Protection Framework Decision), OJ 2008 L 350.

43 European Data Protection Supervisor (2013), *Additional EDPS comments on the data protection reform package*, 15 March 2013, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf.

44 Article 29 Working Party (2013), *Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive*, WP 201, 26 February 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp201_en.pdf.

45 Article 29 Working Party (2013), *Working Document 01/2013: Input on the proposed implementing acts*, WP 200, 22 January 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp200_en.pdf.

46 Financial Times, 4 February 2013.

47 European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2013), Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 16 January 2013.

48 European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2012), Draft report on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 20 December 2012.

49 FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: The role of national data protection authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Publications Office of the European Union (Publications Office); see also FRA (2012), *FRA opinion on the proposed data protection reform package*, Vienna, 1 October 2012; and FRA (2014), *Access to data protection remedies in EU Member States*, Luxembourg, Publications Office.

50 FRA and Council of Europe, European Court of Human Rights (2014), *Handbook on European data protection law*, Luxembourg, Publications Office.

51 Court of Justice of the European Union (CJEU), C518/07, *European Commission v. Federal Republic of Germany*, 9 March 2010; CJEU, C614/10, *European Commission v. Republic of Austria*, 16 October 2012.

52 Austria, *83. Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2014)*, 23 May 2013, www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2013_I_83/BGBLA_2013_I_83.html.

53 CJEU, C288/12, *European Commission v. Hungary*, Advocate General's Opinion, 10 December 2013.

54 Latvia, *Likumprojekts 'Grozījumi Fizisko personu datu aizsardzības likumā'*, http://titania.saeima.lv/LIVS11/saeimalivs11.nsf/0/B0CA8FC1A876870BC2257C310050C997?OpenDocument.

55 Lithuania, LR Vyriausybė (2013), *Nutarimas dėl Valstybinės duomenų apsaugos inspekcijos administracijos struktūros tvirtinimo*, No. 1082, 27 November 2013.

56 Slovakia, *Zákon č. 122/2013 Z.z. o ochrane osobných údajov*, 30 April 2013.

57 FRA (2010), *Data Protection in the European Union: The role of national data protection authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Publications Office.

58 Hungary, National Authority for Data Protection and Freedom of Information (2013), *Key to the World of the Internet!*, www.naih.hu/files/2013-projektfuzet-internet.pdf.

59 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105.

60 Belgium, *Koninklijk besluit tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie/Arrêté royal portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques*, 19 September 2013, www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2013091920&table_name=loi.

61 Poland, *Ustawa o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw*, 16 November 2012.

62 Denmark, Politi og Strafferetsafdelingen, *Report on various questions regarding the Danish data retention regulations*, case no. 2012-187-0020, document no. 549331, www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf.

63 Slovenia, *Zakon o elektronskih komunikacijah*, ZEKom-1, 20 December 2012.

64 Slovenia, *Ustavno sodišča Republike Slovenije*, Ul65/1316, 26 September 2013,.

65 CJEU, C293/12, Reference for a preliminary ruling from the High Court of Ireland, lodged on 11 June 2012, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General*, 25 August 2012.

66 CJEU, C594/12, Reference for a preliminary ruling from the Austrian Constitutional Court, lodged on 19 December 2012.

67 France, Commission nationale de l'informatique et des libertés (CNIL) (2014), *Délibération n° 2013420*, 3 January 2014, www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000028450267&fastReqId=2000051504&fastPos=1.

68 United Kingdom, Information Commissioner's Office (ICO) (2013), 'ICO statement regarding investigation into Google privacy policy', 2 April 2013, www.ico.org.uk/news/latest_news/2013/ico-statement-investigation-google-privacy-policy-02042013.

69 United Kingdom, ICO (2013), 'ICO update on Google privacy policy', 4 July 2013, www.ico.org.uk/news/latest_news/2013/ico-update-on-google-privacy-policy-04072013.

70 Spain, Agencia Española de Protección de Datos (AEPD) (2013), 'The AEPD sanctions Google for serious violation of the rights of the citizens', Press release, 19 December 2013.

71 Germany, Bundesgerichtshof (2013), 'Bundesgerichtshof entscheidet über die Zulässigkeit persönlichkeitsrechtsverletzender Suchergänzungsvorschläge bei "Google"', Press release No. 87/2013, 14 May 2013, http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=64071&linked=pm.

72 CJEU, C131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 25 June 2013, http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1090622.

73 Slovenia, Informacijski pooblaščenec (2013), 'Snemanje ulic za storitev Google Street View', Press release, 2 July 2013, www.ip-rs.si/novice/detajl/snemanje-ulic-za-storitev-google-street-view/?cHash=2113761ece703e0badf20352fa2faa35.

74 See: Internet Governance Forum, www.intgovforum.org/cms/.

75 Internet Governance Forum (2013), 8th meeting of the Internet Governance Forum: Chair's summary, p. 16, www.intgovforum.org/cms/Chair's%20Summary%20IGF%202013%20Final.Nov1v1.pdf.

76 UN, Human Rights Council (2012), Resolution 20/8 on the promotion, protection and enjoyment of human rights on the Internet, http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement; UNESCO (2013), First WSIS+10 Review Event, Final Recommendations, 27 February 2013, p. 3, www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_recommendations_en.pdf. In November 2013 (195 UNESCO states endorsed the Final Recommendations). See also: UN, General Assembly (2013), Resolution 68/167 on the right to privacy in the digital age, 18 December 2013, www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167.

77 Council of Europe, Committee of Ministers (2011), Internet Governance Strategy 2012–2015, CM(2011) 175 final, 15 March 2012.

78 European Commission (2013), *Cybersecurity strategy of the European Union: an open, safe and secure cyberspace*, Joint COM(2013) 1 final, Brussels, 7 February 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:EN:PDF.

79 *Ibid.*

80 Proposal for a Regulation of the European parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, COM(2013) 0627 final, https://ec.europa.eu/digital-agenda/en/news/regulation-european-parliament-and-council-laying-down-measures-concerning-european-single.

81 European Commission (2012), Code of EU Online Rights, Brussels, https://ec.europa.eu/digitalagenda/sites/digitalagenda/files/Code%20EU%20online%20rights%20EN%20final%202.pdf.

82 Internet Rights and Principles Coalition (2013), Charter for Human Rights and Principles for the internet, (version 2.0), http://internetrightsandprinciples.org/site/wpcontent/uploads/2013/10/IRP_booklet_final1.pdf.

83 See: Internet Governance Forum, www.intgovforum.org/cms/.

84 Internet Rights and Principles Coalition (2011), 'Ten internet rights and principles', http://internetrightsandprinciples.org/images/IRPflyer.pdf.

85 Council of Europe, Committee of Ministers (2011), Internet Governance Strategy 2012–2015, CM(2011) 175 final, 15 March 2012.

86 Council of Europe, Committee of Experts on Rights of Internet Users (2013), *Draft recommendation of the Committee of Ministers to member states on a guide on human rights for Internet users*, MSI DUI (2013)07Rev7, 6 December 2013.

87 UN, Office of the High Commissioner for Human Rights (2011), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, New York and Geneva.

88 European Commission (2011), Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A renewed EU strategy 2011–14 for corporate social responsibility, COM(2011) 681 final, Brussels, 25 October 2011.

89 European Commission (2013), *ICT sector guide on implementing the UN Guiding Principles on Business and Human Rights*, June 2013, www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf.

90 European Court of Human Rights (ECtHR), *Delfi AS v. Estonia*, No. 64569/09, 10 October 2013, pending before a Grand Chamber of the ECtHR.

91 Poland, *Naczelny Sąd Administracyjny, I OSK 1666/12*, 21 August 2013.

92 Poland, *Ustawa* o *świadczeniu usług drogą elektroniczną,* 18 July 2012.

93 United Kingdom, Court of Appeal (2013), *Tamiz v. Google*, EWCA Civ 68, www.bailii.org/ew/cases/EWCA/Civ/2013/68.html.

94 The FRA EU LGBT survey was conducted online in the 27 EU Member States and Croatia between April and July 2012. The survey collected information from 93,079 people aged 18 and above who identified as lesbian, gay, bisexual or transgender, and who lived in the EU or Croatia.

95 FRA (2013), *EU LGBT survey: Results at a glance,* Luxembourg, Publications Office, p. 23, http://fra.europa.eu/en/publication/2013/eu-lgbt-survey-european-union-lesbian-gay-bisexual-and-transgender-survey-results.

96 FRA (2014 forthcoming), *EU LGBT survey: Main results*, Luxembourg, Publications Office.

97 The FRA survey on violence against women interviewed 42,000 women (face-to-face interviews), who were between 18 and 74 years old and lived in any of the 28 EU Member States (approximately 1,500 per country). The respondents were selected based on random sampling. The data were collected between April and July 2012. FRA (2014), *Violence against women: An EU-wide survey – main results,* Luxembourg, Publications Office, http://fra.europa.eu/en/publication/2014/vaw-survey-main-results.

98 The survey defined three specific behaviours as cyberstalking: sending emails, text messages (SMS) or instant messages that were offensive or threatening; posting offensive comments about the respondent on the internet; and sharing intimate photos or videos of the respondent on the internet or by mobile phone. To be considered stalking, these incidents had to take place repeatedly and the same person had to perpetrate them.

99 The FRA survey on discrimination and hate crimes against Jews was conducted online in eight EU Member States – Belgium, France, Germany, Hungary, Italy, Latvia, Sweden and the United Kingdom – in September and October 2012. The survey covered 5,847 self-identified Jews aged 16 and over. FRA (2013), *Discrimination and hate crime against Jews in EU Member States: Experience and perceptions of antisemitism*, Luxembourg, Publications Office, http://fra.europa.eu/sites/default/files/fra-2013-discrimination-hate-crime-against-jews-eu-member-states_en.pdf.

100 United Kingdom, BBC News, 'Two guilty over abusive tweets to Caroline Criado-Perez', 7 January 2014, www.bbc.com/news/uk-25641941.

101 See: Beirat für Informationsgesellschaft, www.bka.gv.at/site/4293/default.aspx.

102 European Commission (2010), *A digital agenda for Europe*, COM(2010) 245 final, Brussels, 26 August 2010, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245:EN:NOT.

103 European Commission (2013), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Telecommunications Single Market, COM(2013) 634, Brussels, 11 September 2013, https://ec.europa.eu/digital-agenda/en/news/communication-commission-european-parliament-council-european-economic-and-social-committee-a-o.

104 See: European Dialogue on Internet Governance, www.eurodig.org/.

105 See: www.gouvernement.fr/premier-ministre/le-gouvernement-presente-la-feuille-de-route-pour-le-numerique.