# The rule of law on the Internet and in the wider digital world

Issue paper

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

# The rule of law on the Internet and in the wider digital world

**Issue paper published by the Council of Europe Commissioner for Human Rights**

Council of Europe

*The opinions expressed in this work are the responsibility of the author and do not necessarily reflect the official policy of the Council of Europe.*



Issue papers are published by the Commissioner for Human Rights to contribute to debate and reflection on important current human rights issues. Many of them also include recommendations by the Commissioner for addressing the concerns identified. The opinions expressed in these expert papers do not necessarily reflect the Commissioner's position.

Issue papers are available on the Commissioner's website: www.commissioner.coe.int

Cover photo: © Shutterstock
Cover: Documents and Publications Production Department (SPDP) Council of Europe
Layout: Jouve, Paris


Printed at the Council of Europe

Acknowledgements:
This issue paper was prepared by Professor Douwe Korff, Visiting Fellow, Yale University (Information Society Project), and Oxford Martin Associate, Oxford Martin School, University of Oxford, UK. He and the Commissioner are also grateful to Joe McNamee of European Digital Rights, EDRi, for the very useful comments and additions he provided to the draft version of this issue paper, in particular on privatised law enforcement.

# Contents

All the judgments and decisions of the European Court of Human Rights cited in this issue paper are available from the Court's case law database, HUDOC: http://hudoc.echr.coe.int/sites/eng/Pages/search.aspx#

# Abbreviations

| | |
|---|---|
| 5EYES | The intelligence partnership between the USA, the UK, Australia, Canada and New Zealand |
| CCTV | closed-circuit television |
| CFR | Charter of Fundamental Rights of the European Union |
| CJEU | Court of Justice of the European Union |
| DMCA | US Digital Millennium Copyright Act |
| DNS SEC | Domain Name System Security Extensions |
| DP | data protection |
| DPA | data protection authority |
| DP Convention | Council of Europe Data Protection Convention (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108) |
| DPI | deep packet inspection |
| ECHR | European Convention on Human Rights |
| EDRi | European Digital Rights |
| EFF | Electronic Frontier Foundation |
| EU | European Union |
| FISA | US Foreign Intelligence Surveillance Act |
| GCHQ | UK Government Communications Headquarters |
| HUMINT | human intelligence |
| I-ACHR | Inter-American Convention on Human Rights |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| ICCPR | International Covenant on Civil and Political Rights |
| ICJ | International Court of Justice |
| IGF | Internet Governance Forum |
| IP | Internet Protocol |

| | |
|---|---|
| ISP | Internet service provider |
| ITU | International Telecommunication Union |
| IWF | Internet Watch Foundation |
| MLATs | mutual legal assistance treaties |
| MNO | mobile network operator |
| NGO | non-governmental organisation |
| NSA | (US) National Security Agency |
| PII | personally identifiable information |
| PNR | passenger name record |
| RPKI | Resource Public Key Infrastructure |
| SEA-ME-WE-4 | South East Asia–Middle East–West Europe 4project |
| SIGINT | signals intelligence |
| T-CY | Cybercrime Convention Committee |
| UDHR | Universal Declaration of Human Rights |
| UNODC | United Nations Office on Drugs and Crime |

# Executive summary

This issue paper addresses a pressing question: how can we ensure that the rule of law is established and maintained on the Internet and in the wider digital world? Section 1 describes the range of online activities and the threats to this environment; section 2 discusses the emerging "Internet governance" principles, and notes the special control exercised over the digital world by the USA (and the UK, in respect of Europe), which could lead to fragmentation of the Internet in response. Section 3 sketches the international standards of the rule of law, and some problems in the application of law in this new environment. Section 4 looks in some more detail at the main issues emerging from the earlier sections – freedom of expression, privatised law enforcement, data protection, cybercrime and national security – and discusses the delicate balances that need to be struck.

The Council of Europe Commissioner for Human Rights has formulated a number of recommendations on the basis of the issues raised by this issue paper; these are set out after this executive summary.

## A new environment for human activities

We live in a global digital environment that has created new means for local, regional and global activities, including new types of political activism, cultural exchanges and the exercise of human rights. These activities are not virtual in the sense of "not truly real". On the contrary, they are an essential part of real citizens' lives. Restrictions on access to the Internet and digital media, and attempts to monitor our online activities or e-communications, interfere with our fundamental rights to freedom of expression and information, freedom of association, privacy and private life (and possibly other rights such as freedom of religion and belief, or the right to a fair trial).

The new global digital environment of course also creates a new space for unlawful behaviour: for the dissemination of hate speech or child pornography, incitement to violence, breaches of copyright ("piracy"), fraud, identity theft, money laundering and attacks on the e-communications infrastructure itself through malware (such as Trojans and worms) or "denial of service" attacks. Cybercrime and cybersecurity have become major concerns.

These threats are increasingly transnational, and there is a broad international consensus on the need to deal with cybercrime, cybersecurity and terrorism, but there is much less agreement on specifics – or even what constitutes a threat.

Four issues stand out. First, state actions aiming to counter cybercrime, threats to cybersecurity and threats to national security are increasingly intertwined; the boundaries between such activities are blurred, and the institutions and agencies dealing with them work more closely together. Second, states are now co-ordinating their actions in all these regards. Third, the work of national security and intelligence agencies increasingly depends on monitoring the activities of individuals and groups in the digital environment. Fourth, instead of *ex post facto* law enforcement, the emphasis is now on intelligence and prevention, with law-enforcement agencies using techniques – and technologies – previously reserved for secret services.

## The nature of the digital environment

### Dangerous data

In an age of "Big Data" (when data on our actions are shared and/or exploited in aggregate form) and the "Internet of Things" (when more and more physical objects – things – are communicating over the Internet), it is becoming difficult to ensure true anonymisation: the more data are available, the easier it becomes to identify a person. Moreover, the mining of Big Data, in ever more sophisticated ways, leads to the creation of profiles. Although these profiles are used to spot rare phenomena (e.g. to find a terrorist in a large set of data, such as airlines' passenger name records), they are unreliable and can unwittingly lead to discrimination on grounds of race, gender, religion or nationality. These profiles are constituted in such complex ways that the decisions based on them can be effectively unchallengeable: even those implementing the decisions do not fully comprehend the underlying reasoning.

The digital environment can by its very nature erode privacy and other fundamental rights, and undermine accountable decision making. There is enormous potential for undermining the rule of law – by weakening or destroying privacy rights, restricting freedom of communication or freedom of association – and for arbitrary interference.

### Global and private, but not in the sky

Because of the open nature of the Internet (which is its greatest strength), any end point on the network can communicate with virtually any other end point, following whatever route is calculated as being most efficient, the data flowing through all sorts of switches, routers and cables: the Internet's physical infrastructure. The electronic communications system is transnational, indeed global, by its very nature; and its infrastructure is physical and located in real places, in spite of talk of a Cloud. At the moment, many of these physical components are in the USA and many of them are managed and controlled by private entities, not by governmental ones.

The main infrastructure for the Internet consists of high-capacity fibre-optic cables running under the world's oceans and seas, and associated land-based cables and routers. The most important cables for Europe are those that run from continental Europe to the UK, and from there under the Atlantic to the USA. Given the dominance of the Internet and of the Cloud by US companies, these cables carry

a large proportion of all Internet traffic and Internet-based communication data, including almost all data to and from Europe.

## Who is in control?

### Internet governance

Important Internet governance principles have been put forward, by the Council of Europe and others, that stress the need to apply public international law and international human rights law equally online and offline, and to respect the rule of law and democracy on the Internet. These principles recognise and promote the multiple stakeholders in Internet governance and urge all public and private actors to uphold human rights in all their operations and activities, including the design of new technologies, services and applications. And they call on states to respect the sovereignty of other nations, and to refrain from actions that would harm persons or entities outside their territorial jurisdiction.

However, these principles still remain largely declaratory and aspirational: there is still a deficiency in actual Internet governance arrangements that can be relied on to ensure the application of these principles in practice.

Also, Internet governance must take account of the fact that – partly because of its corporate dominance, and partly because of historical arrangements – the USA has more control over the Internet than any other state (or even all other states combined). Together with its close partner, the UK, it has access to most of the Internet infrastructure.

The former US National Security Agency contractor Edward Snowden has revealed that the USA and the UK are using this control and access to conduct mass surveillance of the Internet and of global electronic communications systems and social networks. There are fears that states may respond to the Snowden revelations by fragmentation of the Internet, with countries or regions insisting that their data are routed solely through local routers and cables, and stored in local clouds. This risks destroying the Internet as we know it, by creating national barriers to a global network. Unless the USA improves compliance with international human rights standards in its activities that affect the Internet and global communication systems, the movement towards such a truncated Internet will be difficult to stop.

### Private-sector control

Much of the infrastructure of the Internet and the wider digital environment is in the hands of private entities, many of them US corporations. This is problematic because companies are not directly bound by international human rights law – that directly applies only to states and governments – and it is more difficult to obtain redress against such companies. In addition, private entities are subject to the national laws of the countries where they are established or active – and those laws do not always conform to international law or international human rights standards: they may impose restrictions on activities on the Internet (typically, on freedom of expression) that violate international human rights law; or they may impose or allow interference,

such as surveillance of Internet activity or e-communications, that is contrary to international human rights law; and such actions may be applied extraterritorially, in violation of the sovereignty of other states.

The application of national law to the activities of private entities controlling (significant parts of) the digital world is extremely complex and delicate. Of course states have a right, and indeed a duty, to counter criminal activity that uses the Internet or e-communication systems. In this, they naturally enlist the help of relevant private actors. Responsible companies will also want to avoid their products and services being used for criminal purposes. Nonetheless, in such circumstances, states should in their actions both fully comply with their international human rights commitments and fully respect the sovereignty of other states. In particular, states should not circumvent constitutional or international law obligations by encouraging restrictions on human rights through "voluntary" actions by intermediaries; and companies, too, should respect the human rights of individuals.

## The rule of law in the digital environment

### The rule of law

The rule of law is a principle of governance by which all persons, institutions and entities, public and private, including the state itself, are accountable to laws that are publicly promulgated, equally enforced, independently adjudicated and consistent with international human rights norms and standards. It entails adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in applying the law, separation of powers, participation in decision making, legal certainty, avoidance of arbitrariness and procedural and legal transparency.

### The basic "rule of law" tests developed by the European Court of Human Rights

The European Court of Human Rights has developed elaborate "rule of law" tests in its case law, and these have also been adopted by other international human rights bodies. To pass these tests, all restrictions on fundamental rights must be based on clear, precise, accessible and foreseeable legal rules, and must serve clearly legitimate aims; they must be "necessary" and "proportionate" to the relevant legitimate aim (within a certain "margin of appreciation"); and there must be an "effective [preferably judicial] remedy" against alleged violations of these requirements.

### "Everyone", without discrimination

It is one of the hallmarks of international human rights law since 1945, and one of its greatest achievements, that human rights must be accorded to "everyone", to all human beings: they are humans' rights, not just citizens' rights.

Thus, subject to very limited exceptions, all laws, of all states, affecting or interfering with human rights must be applied to "everyone", without discrimination "of any kind", including discrimination on grounds of residence or nationality.

Because of the unique place of the USA and US companies in the functioning of the Internet, the constitutional and corporate legal framework in the USA is of particular importance. However, in contrast to the above-mentioned principle of international human rights law, many of the human rights guarantees in the US Constitution and in various US laws relating to the digital environment apply only to US citizens and non-US citizens residing in the USA ("US persons"). Only "US persons" benefit from the First Amendment, covering free speech and freedom of association; the Fourth Amendment, protecting US citizens from "unreasonable searches"; and most of the (limited) protections against excessive surveillance provided by the main pieces of legislation on national security and intelligence (FISA Amendment and Patriot Acts).

## "Within [a contracting state's] [territory and] jurisdiction"

### The duty of states to comply with their responsibilities under international human rights law also when acting extraterritorially

The main international human rights treaties, including the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR), oblige states to "ensure" or "secure" the human rights laid down in those treaties to "everyone subject to their jurisdiction" (or "within their jurisdiction"). This requirement is increasingly given a functional rather than a territorial meaning – as has recently been reaffirmed by the Human Rights Committee and the European Court of Human Rights. In other words, each state must ensure or secure these rights to anyone under its physical control or whose rights are affected by its (or its agencies') actions.

Thus, states must comply with their international human rights obligations in any action they take that may affect the human rights of individuals – even when they act extraterritorially, or take actions that have extraterritorial effect.

This obligation has specific consequences for data – what the digital world is made of – and especially for personal data, as is recognised by European data-protection law, which protects all individuals whose data are processed by European controllers, irrespective of their place of residence, nationality or other status. However, the USA formally rejects this application of international human rights law. In view of the predominance of the USA (and of US corporations that are subject to that country's jurisdiction) in the digital environment, this poses a serious threat to the rule of law in that new environment.

### The difficulty of competing and conflicting laws applying simultaneously to online activities, with particular reference to freedom of expression

The problem of competing – and conflicting – application of different national laws to Internet materials and Internet activity is an issue that needs to be addressed urgently to guarantee the rule of law on the Internet.

The issue at stake is not the right of governments to take actions that comply with international law and that are necessary and proportionate in a democratic society. Within these limits, governments should of course remain free to make decisions on regulation within their jurisdiction. The issue is the ability and right of national governments or courts to take measures that have the effect of imposing restrictions in third countries where the individuals in question are acting in accordance with the laws of their own country of residence which, unlike foreign laws, should be known (or "knowable") to them and foreseeable in their application.

In principle, individuals and companies that make information available from their country of residence or establishment should have to comply only with the laws of that country; and individuals who access or download materials from foreign websites when they could and should know that the materials are illegal in their country of residence can be expected to adhere to the laws of the latter country. States should in principle only exercise jurisdiction over foreign materials that are not illegal under international law in limited circumstances, notably when there is a clear and close nexus between the materials or the disseminator and the state taking action.

## Human rights and private entities

### Human rights law and the Ruggie Principles and Council of Europe and other guidance

International human rights law essentially applies only to states, and to actions (or omissions) of public authorities. However, new international standards are emerging, intended to be applied by companies. The most important are the UN "Guiding Principles on Business and Human Rights" (the Ruggie Principles), drafted by the United Nations Secretary-General's Special Representative for Business and Human Rights, Professor John Ruggie. However, the Ruggie Principles still focus on the duty of host states to act against human rights violations by companies. They do not deal in detail with the converse situation, where states make demands of companies that would lead companies into violations of international human rights law.

It seems important that further guidance be developed, by the Council of Europe and others, on the responsibilities of businesses that face (or that put themselves in situations where they may well face) demands from governments, or from other private entities, to support measures that may violate international human rights law (as further detailed under the section on privatised law enforcement).

### Filtering and blocking by Internet and e-communications companies on the instructions of – or on the basis of "encouragement" by – states

Apart from criminalising material on the Internet – which increasingly happens when the materials are produced in another country, *ex post facto*, after the materials have been published and accessed – states are also increasingly trying to prevent (block) access to certain materials and information online. Such blocking or filtering is performed by software or hardware that reviews communications and decides on

the basis of pre-set criteria whether to prevent the materials from being forwarded to an intended recipient, often someone browsing the Internet.

It is perhaps not surprising that repressive states try to block access to opposition websites, and that theocratic regimes do the same with websites they deem to be blasphemous. But increasingly states that supposedly respect the rule of law – including Council of Europe member states – are also trying to block access to materials they regard as unacceptable. Or, in a more insidious and less accountable framework, they "encourage" the gatekeepers to the Internet (ISPs and MNOs) to do this "voluntarily", outside a clear public-law legal framework.

Usually, in democratic countries, blocking or filtering measures have, at least officially and initially, been mainly aimed at strongly legitimate targets: racist or religious "hate speech" or child pornography. However, the systems suffer from major flaws in the way they work:

- blocking is inherently likely to produce (unintentional) false positives (blocking sites with no prohibited material) and false negatives (when sites with prohibited material slip through a filter);
- the criteria for blocking certain websites, but not others, and the lists of blocked websites, are very often opaque at best, secret at worst;
- appeals processes may be onerous, little known or non-existent, especially if the decision on what to block or not block is – deliberately – left to private entities;
- blocking measures are easy to bypass, even for not very technically skilled people;
- crucially, in particular in relation to child pornography, blocking totally fails to address the actual issue: the abuse of the children in question.

The above problems are compounded by the fact that, once states have introduced blocking against the most serious issues such as child pornography and hate speech, they tend to extend it to all sorts of other matters that they disapprove of. Globally, including in Europe, there have been attempts by states to block sites containing not only hate speech and advocacy of terrorism, but also, for instance, political debate or information on sexual or minority rights.

It is useful to distinguish between two different situations: law-based and non-law-based blocking of content. It is unquestionably the case that there is certain content that is a legitimate target for blocking measures (law-based blocking of illegal content). However, the aim of the blocking measure and the actual technical means used to carry it out remain crucial to determining whether the measure is proportional and therefore lawful – for example, if there is no evidence of significant levels of accidental access to the content in question and if deliberate access remains easy after the blocking measure, the proportionality of the blocking is more questionable.

The matter gets more complicated if the decision of what sites to block is left to private entities, "encouraged" by states that nonetheless claim to bear no responsibility for the blocking (non-law-based blocking of content). Some countries, such as the UK and Sweden, have introduced blocking systems based on voluntary arrangements with ISPs. While all considerations concerning effectiveness and

proportionality of the measure remain relevant for this type of blocking, it raises a more general and fundamental question that needs to be addressed: how far are these blocking measures really voluntary and/or do they entail state responsibility? The fact that Article 10 of the ECHR only refers to interferences with this right "by public authorities" does not mean that the state can simply wash its hands of measures by private entities that have such effect – especially not if the state *de facto* strongly encouraged those measures. In such circumstances, the state is responsible for not placing such a system on a legislative basis: without such a basis, the restrictions are not based on "law".

In recent case law, the European Court of Human Rights has clearly noted the dangers of indiscriminate blocking. In its judgment in the case of *Yildirim v. Turkey*, the Court observed that the measure in question – blocking access to all websites hosted by Google Sites from Turkey in order to block a Google site that was regarded as disrespectful of Kemal Atatürk – had produced arbitrary effects and could not be said to be aimed solely at blocking access to the offending website, since it consisted in the wholesale blocking of all sites hosted by Google Sites. Moreover, the judicial review procedures concerning the blocking of Internet sites were deemed to be insufficient to meet the criteria for avoiding abuse, as domestic law did not provide for any safeguards to ensure that a blocking order in respect of a specific site was not used as a means of blocking access in general. The Court therefore found a violation of Article 10 of the ECHR.

### Indiscriminate deep packet inspection (DPI) by companies under court orders issued at the request of other companies, to enforce copyright

Intellectual property rights holders are increasingly asking for filters or blocks, similar to the ones described above, to be imposed on sites that are allegedly facilitating the sharing of pirated content; and are increasingly demanding access to Internet users' details in relation to such alleged sharing, including through the compulsory use of DPI by ISPs to detect probable (or possible) rights-infringers.

DPI requires the "inspector" to examine not just the broad metadata related to the origin or destination of the "packet", but also the content of those communications. "Packets" are singled out on the basis of a pattern or algorithm linked to specific content. For the intellectual property rights-holders, that will be the particular markers of a particular copyright-protected video or photograph. But the same technology allows for searches of essentially anything: a certain political speech, a certain revolutionary song, a trade union banner. These measures are highly intrusive, as they require surveillance of all users of an ISP (or mobile phone network), with the aim of trying to identify the few that are probably (or possibly) infringing copyright, and thus they raise serious issues of necessity and proportionality.

Both the European Court of Human Rights and the Court of Justice of the European Union have issued important judgments that strongly suggest that indiscriminate filtering of all the communications carried by an ISP (or an MNO) – that is, general monitoring or surveillance – for the purpose of identifying possible rights-infringers from the mass of innocent users is contrary to human rights law.

### Exercise of extraterritorial jurisdiction by states

A state that uses its legislative and enforcement powers to capture or otherwise exercise control over data that are not held on its physical territory but on the territory of another state – typically by using the physical infrastructure of the Internet and the global communications systems to extract those data from servers in the other state, or by requiring private entities that have access to such data abroad to extract those data from servers or devices in another country and hand them over to the state – is exercising its jurisdiction extraterritorially within the jurisdiction of the other state.

Under general public international law, in the absence of treaties that grant powers of extraterritorial enforcement jurisdiction to foreign agencies, it is not lawful for the first state to do this without the consent of the second state.

## The issues, and the balance between them

### The issues

Establishing the rule of law on the Internet and in the wider digital world will require clarification of the rules affecting freedom of expression, private entities (particularly corporations) and human rights, data protection and cybercrime; and then the question must be addressed: how are the balances between all of these to be struck in this new environment?

### Freedom of expression

National laws relating to activities on the Internet and the wider digital environment, especially laws relating to freedom of expression, often compete and conflict: under the laws of many states, persons making statements online or in electronic communications in, or from, one country can be held liable for that under the laws of another country if the statements violate the latter laws, even if they are lawful where they were made. This poses a fundamental threat to the rule of law on the Internet and in that environment. This has not yet been fully addressed in the case law of the European Court of Human Rights.

As suggested above, the only way to resolve this would be if states and national courts were to show clear restraint by not imposing their domestic legal standards on expressions and information disseminated over the Internet from abroad, unless these are unlawful under international law or present clear links that justify the exercise of the state's jurisdiction.

A further important issue is the liability of individuals or companies managing a website, or even ISPs, for content posted on a website. Here, too, the case law at European level has been limited to date. At the moment, private companies appear to be caught between clear obligations (remove content or face punishment) and unclear obligations (to guarantee access to lawful content to users). As a result, private companies may tend to choose over-compliance and prevent all users from accessing perfectly lawful materials while at the same time protecting themselves against possible claims from affected users by imposing on them loose terms and conditions. These are core issues that need to be resolved.

## Privatised law enforcement

The fact that the Internet and the global digital environment is largely controlled by private entities (especially, but not only US corporations) also poses a threat to the rule of law. Such private entities can impose (and be "encouraged" to impose) restrictions on access to information without being subject to the constitutional or international law constraints that apply to state limitations of the right to freedom of expression. These private entities can also be ordered by domestic courts, acting at the request of other private entities, to perform highly intrusive analysis of their data to detect probable (or just possible) infringements of private property rights, often intellectual property rights. They can be ordered to "pull" data, including governmental, commercial and personal data, from servers in other countries, for law enforcement or national security purposes, without obtaining the consent of the other country – or the consent of the companies or data subjects in the other country – in violation of the sovereignty of the other country, the commercial confidentiality that companies are entitled to, and the human rights of the data subjects.

The United Nations' Ruggie Principles, while indicating the importance of addressing these issues, do not provide the answers. As mentioned, new approaches and guidelines are therefore needed. The Council of Europe has made important contributions to this debate by suggesting that states could be held accountable for failing to ensure that private entities do not violate the human rights of their citizens and that states have an obligation to ensure that general terms and conditions of private companies that are not in accordance with international human rights standards must be held null and void.

## Data protection

European data-protection law is founded on a set of basic principles (fair processing; purpose specification and purpose limitation; data minimisation; data quality; and data security) and a set of rights (data subject rights) and remedies (supervision by independent data-protection authorities) that are special reflections of the general "rule of law" principles developed by the European Court of Human Rights. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108) and the EU rules on the matter specify how compliance with the general requirements of human rights law should be ensured in the specific context of the processing of personal data. The European data-protection model is increasingly being taken up outside the Council of Europe area: Convention No. 108 (currently under a process of modernisation) is becoming the global gold standard in guaranteeing the international rule of law in this specific respect, which is crucial for the Internet and the wider digital world.

European data protection has been further strengthened by a judgment of the Court of Justice of the European Union, which has rejected compulsory, suspicionless, untargeted data retention. In connection with the debate on the practices of intelligence and security services prompted by Edward Snowden's revelations, it is becoming increasingly clear that secret, massive and indiscriminate surveillance

programmes are not in conformity with European human rights law and cannot be justified by the fight against terrorism or other important threats to national security. Such interferences can only be accepted if they are strictly necessary and proportionate to a legitimate aim.

Data protection on European lines provides the first and most important cornerstone for the rule of law on the Internet and in the wider digital world. As a result, it will be crucial to ensure that the review (modernisation) of Convention No. 108, currently under way, does not lead to any lowering of the standards. Accession by the USA to Convention No. 108 would be particularly valuable, not just for US citizens, but as a move towards a more comprehensive global approach to respect for the fundamental right to data protection and the rights that it enables.

## Cybercrime

The Convention on Cybercrime (Cybercrime Convention, ETS No. 185) requires states parties to make certain acts – such as illegal access to computer systems (hacking), illegal interception of electronic communications, the sending of malware, copyright violations and the production or dissemination of child pornography – criminal under their national law; its Additional Protocol requires states parties to criminalise the dissemination of racist and xenophobic material (hate speech). It also makes extensive provision for international co-operation in fighting such crimes, including mutual legal assistance in investigation and preservation of evidence, extradition and similar matters. The convention is open to non-European states and has been ratified by five such states, including the USA.

While the need for an agreement to counter crime in the global digital environment is beyond doubt – and the Council of Europe is to be commended for initiating such a process – the convention is not yet fully geared to ensuring compliance with the rule of law in its implementation by states parties.

One reason for this is that the convention does not contain a comprehensive human rights clause, and so it does not provide protection against states imposing unduly wide criminal offences, or failing to include exceptions or defences in their substantive law (such as a public interest defence for whistleblowers); nor does it protect against double jeopardy or the provision of (formal or informal) assistance to states parties when this could violate human rights.

Another reason is that the convention is not linked to other major instruments developed by the Council of Europe that support the rule of law in digital and/or transnational contexts. Such a linkage seems all the more necessary because the convention is open to states that are not party to the ECHR or have not fully accepted the comparable requirements of the ICCPR (such as the USA in respect of its extraterritorial activities or the rights of "non-US persons"). From the perspective of the rule of law in Europe, accession to the Cybercrime Convention should require both full acceptance by states of their obligations under the ECHR and/or ICCPR and ratification of the Data Protection Convention, the European Extradition Convention, and the European Convention on Mutual Assistance in Criminal Matters.

Finally, Articles 26 and 32 of the convention appear to support the tendency of law-enforcement agencies to resort to "informal" means of information gathering, even across borders, without laying down clear safeguards (for instance, that such informal measures should not be used for intrusive information-gathering activities that normally, in a state under the rule of law, require a judicial warrant); and those two articles also seem to support the tendency of such authorities to increasingly "pull" data directly from servers in other countries, or to demand that companies within their jurisdiction – particularly the main Internet giants – do this for them, without recourse to formal, inter-state mutual legal assistance arrangements, arguably in violation of the sovereignty of the state where the data are found.

The principle – established in Article 16 of Convention No. 108 in relation to mutual assistance between data-protection authorities – that there are clear limitations to the circumstances in which personal data may be collected and/or passed on in transnational activities, should also better inform the Convention on Cybercrime. A number of recommendations and declarations of the Council of Europe Committee of Ministers provide useful guidance on how to strike the balance between upholding data-protection principles and allowing appropriate law enforcement. Compliance with these instruments by member states who are parties to the Convention on Cybercrime should be strengthened.

The drafting of the proposed new additional protocol to the Convention on Cybercrime provides an opportunity to resolve at least some of these issues. With these improvements, the Cybercrime Convention could provide a second cornerstone for the rule of law on the Internet and in the wider digital world.

## National security

The European Convention on Human Rights and the Council of Europe Data Protection Convention both in principle apply to all activities of the states that are party to them: although both include some special rules and exceptions, issues of national security are not explicitly excluded. In this, the mandate of the Council of Europe and the scope of these instruments differ from EU law, which expressly excludes national security from the competence and jurisdiction of the Union. This means that, when it comes to international legal regulation of the activities of national security and intelligence agencies, the Council of Europe must take the lead role, if not globally then at least in Europe.

The need to secure the rule of law in relation to the activities of national security and intelligence agencies has become obvious in the light of the revelations of Edward Snowden about the global surveillance operations of the USA's National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ) and their partners in the 5EYES group (Australia, Canada and New Zealand) in particular. These revelations have shown that these agencies are routinely tapping into the high-capacity fibre-optic cables that form the backbones of the Internet, and are also intercepting mobile and other communications worldwide on a massive scale, for instance by intercepting radio communications, using "back doors" they have installed in major communications systems and exploiting security weaknesses in such systems.

In European and international human rights law, national security is not a card that trumps all other considerations. Indeed, the very question of what legitimately can be said to be covered by the concept of "national security" is justiciable: it should be up to the courts to determine, in the light of international human rights law, what is – and what is not – legitimately covered by the term. Useful guidance on this is provided in the *Johannesburg Principles on National Security, Freedom of Expression and Access to Information,* drafted by the NGO Article 19 but endorsed by various international forums including the UN Special Rapporteur on Freedom of Opinion and Expression. These principles make clear that states can only invoke national security as a reason to interfere with human rights in relation to matters that threaten the very fabric and basic institutions of the nation. Sometimes, terrorism can reach this level, but in most cases it is a phenomenon that should be dealt with by law enforcement rather than within a national security paradigm. This also applies to actions of states that relate to the Internet and e-communications.

There is a lack of clear treaty rules governing the actions of national security and intelligence agencies, and the basis on which they operate and exchange data. In many countries, there are few clear, published laws regulating the work of these agencies. In some, there are no published rules at all. Until the rules are known under which these agencies and services operate – domestically, extraterritorially or in co-operation with each other – their activities cannot be said to be in accordance with the rule of law. Another matter of serious concern is the manifest ineffectiveness of many supervisory systems.

In other words, in relation to national security, there is as yet no real cornerstone to uphold the rule of law – although there are at least basic principles that could form the foundation of such an essential part of the universal human rights edifice.

Given the increased partnerships between law enforcement and intelligence and security agencies, this negation of the rule of law threatens to spread from the latter to the policemen and prosecutors. The absence of clear legal frameworks in this regard, domestically and internationally, is a further threat to the rule of law on the Internet and in the global digital environment.

# The Commissioner's recommendations

Taking into account the findings and conclusions of this issue paper, the Commissioner makes the following recommendations, with the aim of improving respect for the rule of law on the Internet and the wider digital environment.

## I. On the universality of human rights, and their equal application online and offline

1. The basic requirements of the rule of law apply, and should be made to apply in practice, equally online and offline. This means in particular that:

- the European Convention on Human Rights (ECHR) and all Council of Europe data-protection rules apply to all personal data-processing activities by all agencies of all Council of Europe member states, including the member states' national security and intelligence agencies;
- rule of law obligations, including those flowing from Articles 8 (right to respect for private and family life) and 10 (freedom of expression) of the ECHR, may not be circumvented through ad hoc arrangements with private actors who control the Internet and the wider digital environment;
- Council of Europe member states should strive to ensure that non-European states similarly comply with their international human rights obligations in anything they do that affects individuals using the Internet or otherwise active in the wider digital environment;
- no states (and none of their agencies, including their law enforcement and national security and intelligence agencies), European or otherwise, should access data stored in another country – or passing through the Internet and e-communications "backbone" cables running between countries – without the express consent of the other country or countries involved unless there is a clear, explicit and sufficiently circumscribed legal basis in international law for such access and provided that such access is fully compatible with international data protection and other human rights standards.

## II. On data protection

2. Member states which have not yet done so should ratify the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108). This convention is also open to non-member states and, if adopted widely, can become the most important cornerstone of the rule of law on the Internet and in the wider digital environment.

3. Member states which have already ratified this convention should ensure that it is fully implemented at the national level.

4. The review of Convention No. 108, currently under way, should not lead to any lowering of European or global data-protection standards. On the contrary, it should lead to a clarification and better enforcement of the rules, especially in relation to the Internet and the wider digital world, and in relation to surveillance for national security and intelligence purposes.

5. In the context of the current reform of the EU data-protection rules, existing rules which might undermine the rule of law, such as those relating to consent, profiling or foreign law-enforcement access to personal data, should be clarified and brought into line with international human rights obligations, including those flowing from Convention No. 108, and the relevant Council of Europe recommendations and guidance.

6. Suspicionless mass retention of communications data is fundamentally contrary to the rule of law, incompatible with core data-protection principles and ineffective. Member states should not resort to it or impose compulsory retention of data by third parties.

## III. On cybercrime

7. States parties to the Council of Europe Convention on Cybercrime must fully comply with their international human rights obligations in anything they do (or do not do) under the convention, be that in defining the relevant crimes (and elements, exceptions and defences relating to them), in any criminal investigations or prosecutions, or in relation to mutual legal assistance and extradition.

8. If any state party takes actions that affect individuals outside its territory, this does not exempt that party from its obligations under the Convention on Cybercrime or under international human rights treaties (in particular, the ECHR and the ICCPR); on the contrary, those obligations equally apply to such extraterritorial acts.

9. All states parties to the Convention on Cybercrime should also ratify and rigorously implement the Data Protection Convention, the European Extradition Convention and the European Convention on Mutual Assistance in Criminal Matters.

10. Member states, including their law-enforcement agencies, should implement Recommendation No. R (87) 15 of the Council of Europe Committee of Ministers regulating the use of personal data in the police sector, its Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data

in the context of profiling, and its 2013 Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies.

11. Member states should ensure that their law-enforcement agencies do not obtain data from servers and infrastructure in another country under informal arrangements. Rather, they should use the mutual assistance arrangements, and the special arrangements for expedited data preservation, created by the Convention on Cybercrime. Law-enforcement agencies in one country should not rely on the fact that private entities – such as Internet service providers, social networks or mobile network operators – in other countries have obtained authority to disclose their customers' data under their general terms and conditions.

## IV. On jurisdiction

12. There should be limits on the extraterritorial exercise of national jurisdiction in relation to transnational cybercrimes. These limits should take account of the effect of substantive limitations to the crimes, and of exceptions or defences, in the individual's home country (or the country where the acts were committed) in relation to jurisdiction claimed by other states that do not acknowledge such limitations, exceptions or defences.

13. In relation to the right to freedom of expression in particular, individuals and companies that make information available from their country of residence or establishment should in principle have to comply only with the laws of that country; while individuals who access or download materials from foreign websites (when they could and should know that the materials are illegal in their country of residence) should be expected to adhere to the laws of the latter country. Apart from content that is illegal under international law, states should only exercise jurisdiction over foreign digital materials in limited circumstances, notably when there is a clear and close nexus between the material and/or the disseminator and the country in question.

## V. On human rights and private entities

14. Member states should stop relying on private companies that control the Internet and the wider digital environment to impose restrictions that are in violation of the state's human rights obligations. To that end, more guidance is needed on the circumstances in which actions or omissions of private companies that infringe human rights entail the responsibility of the state. This includes guidance on the level of state involvement in the infringement that is necessary for such responsibility to be engaged and on the obligations of the state to ensure that the general terms and conditions of private companies are not at variance with human rights standards. State responsibilities with regard to measures implemented by private parties for business reasons, without direct involvement of the state, also need to be examined.

15. Building on the UN "Guiding Principles on Business and Human Rights" (the Ruggie Principles), further guidance should be developed on the responsibilities of business enterprises in relation to their activities on (or affecting) the Internet or in

the wider digital environment, in particular to cover situations in which companies may be faced with, or may have put themselves in situations in which they may well face, demands from governments that may be in violation of international human rights law.

## VI. On blocking and filtering

16. Member states should ensure that any restrictions on access to Internet content affecting users under their jurisdiction are based on a strict and predictable legal framework regulating the scope of any such restrictions and affording the guarantee of judicial oversight to prevent possible abuses. In addition, domestic courts must examine whether any blocking measure is necessary, effective and proportionate, and in particular whether it is targeted enough so as to impact only on the specific content that requires blocking.

17. Member states should not rely on or encourage private actors who control the Internet and the wider digital environment to carry out blocking outside a framework meeting the criteria described above.

## VII. On national security activities

18. The ECHR and Convention No. 108 must be applied to all activities of the states that are party to these conventions, including states' national security and intelligence activities.

19. Specifically, in order to achieve respect for the rule of law on the Internet and in the wider digital environment:

- states should only be allowed to invoke national security as a reason to interfere with human rights in relation to matters that threaten the very fabric and basic institutions of the nation;
- states that want to impose interferences with fundamental rights on the basis of an alleged threat to national security must demonstrate that the threat cannot be met by means of ordinary criminal law, compatible with international standards relating to criminal law and procedure;
- the above also applies to actions of states that relate to the Internet and e-communications.

20. Member states should bring the activities of national security and intelligence agencies within an overarching legal framework. Until there is increased transparency on the rules under which these services operate – domestically, extraterritorially and/or in co-operation with each other – their activities cannot be assumed to be in accordance with the rule of law.

21. Member states should also ensure that effective democratic oversight over national security services is in place. For effective democratic oversight, a culture of respect for human rights and the rule of law should be promoted, in particular among security service officers.

# Introduction

This issue paper addresses a very wide issue: the application of the rule of law to the Internet and the wider digital environment. In order to do this, it first provides a brief overview of the political, cultural and human rights activities that take place in this environment – and of the illegal behaviour for which it also provides a space – as well as developments in the approaches of states to such behaviour (section 1).

Next, section 2 looks at the nature of this new digital environment. It describes the enormous amounts of ever more intrusive and revealing data that are generated within it – and the dangers posed by this. It explains that the Internet and this new environment are global by nature, and the Cloud is not in the sky but very much linked to real territories and real states (the USA in particular). It also briefly describes the real, physical backbones of the Internet and of global communications systems.

After that, we ask "who is in control?" We discuss the vexed question of Internet governance, and the Internet governance principles formulated by the Council of Europe, before noting that much of the Internet and the digital environment is controlled more by private entities (many of them US corporations) than by states.

Only then do we turn to the central issue of the rule of law (section 3). We describe the basic "rule of law" tests developed by the European Court of Human Rights and now also adopted by other international human rights bodies, as well as the important principle that, under the international rule of law, human rights safeguards should be ensured for "everyone" irrespective of where the person is, their residence status or place of residence, or their nationality. In that connection, we discuss the rules in international human rights treaties on the duty of states to ensure human rights to everyone "within their jurisdiction" – and note that this concept is now given a functional, rather than a simply territorial meaning. We also note the developing international human rights standards applicable to the behaviour of private-sector entities, particularly companies and corporations.

After that, in section 4, we bring together the core issues especially regulated by the Council of Europe – freedom of expression, privatised law enforcement, data protection and international co-operation between law-enforcement agencies in relation to cybercrime – and one issue that is still manifestly insufficiently regulated, the activities of national security and intelligence agencies. We end section 4 with a discussion of the delicate balances, still largely unresolved, that need to be struck in relation to these issues: how to provide proper, high-level data protection while also allowing effective law enforcement in relation to activities on the Internet and in the wider digital environment, and how to link that activity (or not) to national security.

Although this issue paper is written from a European perspective, it has been necessary in various sections to refer to the practices of US corporations and the laws of the USA, because the digital world described in section 2 is to quite a considerable extent controlled by US corporations, and because US law (and, sometimes, the non-application of US legal requirements or safeguards) has a major impact on this new world. Nothing has made this clearer than the revelations by Edward Snowden about the global Internet and e-communications surveillance activities of the US National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ) and their partners.

Chapter 1

# A new environment for human activities

## 1.1. Political, social, cultural and human rights activities

We live in a new global digital environment that has created new means for local, regional and global activities: for new types of political activism, cultural exchanges and the exercise of human rights. These activities are not "virtual" in the sense of "not truly real". On the contrary, they are an essential, real part of real citizens' lives. We protest by signing online petitions; we experience art, and access and share culture and information on the Internet; we associate on social media sites; and we organise street protests, and report on police actions, through our mobile phones.[1]

The UN Special Rapporteur on Freedom of Expression rightly stresses that access to the Internet and other digital means of communication has become essential to full and free participation in social, cultural and political life.[2] Indeed, as the European Court of Human Rights put it, referring to its extensive comparative research:[3]

> The right to Internet access is considered to be inherent in the right to access information and communication protected by national Constitutions, and encompasses the right for each individual to participate in the information society and the obligation for States to guarantee access to the Internet for their citizens. It can therefore be inferred from all the general guarantees protecting freedom of expression that a right to unhindered Internet access should also be recognised.

1. Ian Brown and Douwe Korff, "Social media and human rights", chapter 6 in *Human rights and a changing media landscape* (Council of Europe 2011), pp. 175-206, at www.coe.int/t/commissioner/source/prems/MediaLandscape2011.pdf.
2. See the second report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, dated 10 August 2011, UN Document A/66/290, paras. 10ff. and 78, available at: www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf.
3. *Yildirim v. Turkey*, Application No. 3111/10, judgment of 18 December 2012, para. 31. The Court carried out a survey of 20 Council of Europe member states (ibid.). For an example of a domestic constitutional case (referred to by the European Court of Human Rights in Yildirim, para. 32) see the French Constitutional Court ruling on the anti-copyright-infringement law, HADOPI, where that court ruled that the Internet and other means of electronic communication had become so important that the right to freedom of expression, as guaranteed by Article 11 of the French Declaration of Human Rights of 1789, should be read as implicitly including a right of access to those services ("ce droit implique la liberté d'accéder à ces services"). Constitutional Court Decision No. 2009-580 DC of 10 June 2009, para. 12, available at: www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/2009/decisions-par-date/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html.

In fact, restrictions on access to the Internet and digital media, and any monitoring of our online activities or e-communications, interfere with our fundamental rights to freedom of expression and information, freedom of association, privacy and private life (and possibly other rights such as freedom of religion and belief or the right to a fair trial). In the next section, we discuss when, and subject to what safeguards, such interferences can be regarded as lawful and legitimate under international law – and when not.

## 1.2. Cybercrime, cybersecurity, terrorism and national security

The new global digital environment of course also creates a new space for illegal behaviour: for the dissemination of hate speech or child pornography, incitement to violence, breaches of copyright, fraud, identity theft, money laundering and attacks on e-communications infrastructure itself through malware such as Trojans and worms or by "denial of service" attacks. "Cybercrime" – though still insufficiently clearly defined (how big does the "cyber" element of a crime need to be, for it to be a "cyber" crime?)[4] – has become a major concern.

The new digital environment can also be used to attack a country's critical services, including banking, electricity and the physical infrastructure that is increasingly monitored and managed via digital channels. Cybersecurity is another major concern, closely related to cybercrime but more focused on protecting a country's assets rather than the assets of individuals.

Cybercrime and cybersecurity are increasingly closely linked to concerns regarding terrorism and national security – although these concepts, too, remain dangerously ill defined. Hate speech shades into promoting violent extremism, and further into recruitment of fighters; violent political organisations use crime and money laundering to finance their operations.

These threats are all increasingly transnational and global. Criminals in Russia or Nigeria can attempt fraud against bank-card holders in France; hackers in the UK can attack US Pentagon computers; websites run by Saudi or Yemeni nationals can incite young people in Germany to fight in Syria. States, and the international community, must of course respond to such threats. However, different countries may take different views on specific issues. For instance, recreational hacking by a lone individual in one country, which might be regarded as a minor (cyber-) offence in that country, can be treated as a national security crime in another country, if the loner manages to penetrate the systems of the latter country's national defences, even if little real damage is done.[5] Online statements and writings that are regarded as legal in one country (and even constitutionally protected) may be regarded as illegal in another.

Thus, although there may be an international consensus on the need to deal with cybercrime, cybersecurity and terrorism in broad terms, there is much less agreement when it comes to specifics – or even as to what constitutes such threats.

4. See section 4.5, below.
5. Cf. the well-known case of Gary McKinnon: https://en.wikipedia.org/wiki/Gary_McKinnon. For a more recent case, see: www.usnews.com/news/articles/2013/10/28/british-man-arrested-for-hacking-nasa-pentagon, from October 2013.

Four issues stand out in this regard. First, state actions aimed at countering cybercrime, threats to cybersecurity and threats to national security are increasingly intertwined. The boundaries between such activities are increasingly blurred, and the institutions and agencies dealing with them are working ever more closely together.[6] In the UK, the Government Communications Headquarters had until recently a mainly technical, supporting role in relation to cybercrime and the work of the police. However, it now seems to be more directly involved, for instance in relation to the fight against the sharing of child pornography on the Internet.[7]

Second, unsurprisingly given that the threats are global, states are increasingly co-ordinating their actions in all these regards. The Council of Europe Cybercrime Convention[8] seeks to provide an international framework for this co-operation. However, there are also other, less well-known arrangements. For instance, the five English-speaking countries working together in a close national security/intelligence partnership since shortly after the Second World War, the USA and the UK, Australia, Canada and New Zealand – the so-called "5EYES" – are now also working together more broadly as a "Strategic Alliance Group", which in turn has led to the establishment of a "Strategic Alliance Cyber Crime Working Group".[9]

Third, the work of these agencies on all these issues increasingly depends on monitoring the activities of individuals and groups in the new digital environment – and on data mining and "profiling" as means to identify cybercriminals, cyber-attackers (hackers) and global or regional terrorists.

Fourth, the emphasis is increasingly on intelligence and prevention rather than *ex post facto* law enforcement. This has always been the case in relation to national security, but it has also become the main attitude to countering cybercrime (aspects of which clearly overlap with countering threats to national security) – and it is also increasingly predominant in law enforcement. The police and the secret agencies are no longer just looking for people who have committed crimes, who hacked into the PCs of others or perpetrated acts of violence; rather, they want to find people who may, or are likely to, commit such acts, and "deal" with them before they can act. Moreover, this "preventive policing" relies much more than traditional law enforcement on

---

6. A page on the FBI website, "Addressing threats to the nation's cybersecurity", expressly notes that the FBI is charged with protecting the USA's national security and with being the nation's principal law-enforcement agency, adding that "These roles are complementary, as threats to the nation's cybersecurity can emanate from nation-states, terrorist organizations, and transnational criminal enterprises; with the lines between sometimes blurred." See www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity. It has changed an FBI Fact Sheet to describe its "primary function" as no longer "law enforcement", but now "national security". See *The Cable*, 5 January 2014: http://thecable.foreignpolicy.com/posts/2014/01/05/fbi_drops_law_enforcement_as_primary_mission#sthash.4DrWhlRV.dpbs. For the dangers inherent in such blurring of the lines, see: www.foreignpolicy.com/articles/2013/11/21/the_obscure_fbi_team_that_does_the_nsa_dirty_work.
7. See: www.theguardian.com/technology/2013/nov/18/david-cameron-gchq-child-abuse-images.
8. The Cybercrime Convention (ETS No. 185), also known as the Budapest Convention, is further discussed in section 4.5, below.
9. See the FBI website: www.fbi.gov/news/stories/2008/march/cybergroup_031708. On the treaties underpinning international co-operation between the 5EYES (and others), see section 4.5, below.

secret intelligence gathering, SIGINT and HUMINT (signals intelligence and human intelligence) – meaning interception of communications with other forms of electronic surveillance, infiltrators and informants. This in turn leads to ever closer co-operation between law enforcement and the secret intelligence services.

While the latter have always acted in this twilight zone, shifting the activities of law-enforcement agencies to such operations fundamentally affects their civic role.

Chapter 2

# The nature of the digital environment[10]

## 2.1. Dangerous data

The digital world comprises the Internet, the various electronic communication tools and systems, and the sensors and devices linked to them, through which most of us now carry out many of our daily activities.

In most of Europe, nearly all households can access at least basic Internet services, and high-speed access is increasing rapidly.[11] Internet access is moving away from fixed personal computers to mobile devices – laptops, tablets and especially "smart" mobile phones. More and more goods and services, even government services, are provided online or via mobile phone: we are moving from electronic e-communications, e-commerce and e-government to mobile m-communications, m-commerce and m-government. Our real, offline lives and virtual, online lives are ever more intertwined.

In addition, more and more physical objects ("things") are communicating over the Internet: detailed energy use is reported by "smart" electricity and gas meters; mobile phones constantly track movements and contacts; cars can report details of their speed and location; and public and private bodies and manufacturers increasingly install sensors that report on the environment or on the operation of technical systems ("The Internet of Things").

Sensors in the new environment – CCTV cameras, but also audio recorders and access and authentication systems – increasingly use biometrics to not just see and hear but also identify: security cameras now hear us and/or can identify us from our face, gait or even irises. Doors are opened not by a key or by typing in a code that is shared by all employees, but by a face scan that shows exactly who went where and when. Increasingly, this is then recorded and kept for future reference, "just in case" it might prove useful.

10. This section draws on a draft report for the Council Europe by Douwe Korff, "The use of the Internet & related services, private life & data protection: trends & technologies, threats & implications" (March 2013), available at: www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/KORFF%20-%20Trends%20report%20(final)%20-%20March2013%20(14%2005%202013).pdf.
11. Source: http://point-topic.com/press-and-events/2013/europe-superfast-broadband-digital-agenda-scoreboard-update/. The study to which this refers notes that, for many, their broadband access was still rather basic. However, in Malta, the Netherlands, Belgium, Switzerland and Luxembourg, high-speed Next Generation Access (NGA) coverage had already exceeded 90% by the end of 2012.

Even leaving out state surveillance for now, most of our online activities are constantly monitored for profit: surveillance is the business model for the Internet.[12] As former US vice-president Al Gore put it: "We have a stalker economy."[13] The data relating to our own actions, and the data generated and reported on by "things", are also increasingly shared and/or exploited in aggregate form, as so-called Big Data. This can include medical data in supposedly de-identified formats,[14] the number of crimes in a specific area, demographics and school results. Companies and governments are keen to exploit these data resources to the fullest extent.

There are two main problems with this. First, it is increasingly difficult to ensure true anonymisation of such data: the more data there are, even in supposedly de-identified form, the more difficult it is to really prevent re-identification in practice.[15]

Second, the analyses and mining of the Big Data resources, in ever more sophisticated ways (to turn Big Data into Smart Data), tend to lead to the creation of "profiles": algorithms derived from the data that establish statistical correlations between often seemingly unrelated facts. Once created, these profiles are then applied to the real world and to individual people: to identify risk factors so that people susceptible to certain diseases can be called in for preventive checks; or to increase their insurance premiums; or to identify the effects of street design and lighting on crime levels, to improve planning; or to direct police resources; or indeed to identify people who may be wanting to commit suicide by throwing themselves under a train (as is done in the London Underground) or who may be terrorists.

In this new environment, we – and the "things" around us – all generate extremely detailed personal or quasi-personal data trails, even if we are only half-aware of them. These data can be used to map social networks: the spiders' webs of contacts linked to contacts, linked to further contacts. Combined with Big Data and profiles, they can be surprisingly revealing of each man and woman's life, beliefs, inclinations, health and activities – at least with a high degree of probability. Just a few "likes" on Facebook suffice to predict the religion, race or sexual orientation of the user with

---

12. Bruce Schneier, *Surveillance as a business model*, at: https://www.schneier.com/blog/archives/2013/11/surveillance_as_1.html.
13. "Former US vice-president Al Gore predicts lawmakers will rein in surveillance", The Canadian Press, 7 November 2013, available at: www.vancouversun.com/news/Former+vicepresident+Gore+predicts+lawmakers+will+rein/9129866/story.html. On the fundamental threat this poses to the Internet, see: http://m.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/2/.
14. For instance, "MedRed BT Health Cloud will provide public access to aggregated population health data" extracted from the UK National Health Service's databases: www.informationweek.com/healthcare/electronic-health-records/feds-praise-open-data-health-cloud-launch/d/did/1112224?goback=.gde_2181454_member_580765269962104832 1# (November 2013).
15. For an easy-to-read summary of the issues, see the submission by the Foundation for Information Policy Research to the UK Government consultation on Making Open Data Real, October 2011, available at: www.fipr.org/111027opendata.pdf. This refers to the seminal paper on the problem: Paul Ohm, "Broken promises of privacy: responding to the surprising failure of anonymization", 57 *UCLA Law Review* (2010) 1701, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

high degrees of accuracy;[16] and just a few innocent purchases (of unscented body oils) have been used to identify women who were likely to be in the second trimester of pregnancy, but who had never revealed this fact.[17]

However, the algorithms and profiles are not infallible: they suffer from inbuilt limitations and defects. In particular, they cannot be relied on to identify rare incidents or phenomena (for example, to single out a terrorist from all the passengers passing through an airport) and they can unwittingly lead to discrimination on grounds of race, gender, religion or nationality. Yet, by their very sophistication, decisions based on them can be effectively unchallengeable: even those implementing the decisions are unable to fully comprehend the underlying reasoning.

In other words, the digital environment can by its very nature erode privacy and other fundamental rights, and undermine accountable decision making. The potential for undermining the rule of law – through the weakening or destruction of privacy rights, restrictions on freedom of communication or freedom of association, and the potential for arbitrary interferences – is enormous, because "entering into the cyberspace requires going through certain private gatekeepers who control the content and the access to the public space of information and discussion".[18]

## 2.2. Global and private, but not in the sky

To understand these threats, and before discussing the legal issues, it is crucial to note the main, inherent aspects of the new digital environment. Communications systems are transnational, indeed global, by their very nature. The infrastructures on which they rely are physical and located in real locations, in spite of talk of a Cloud. They are managed and controlled much more by private entities than by governmental ones. Arrangements for Internet governance are still far from settled (and some attempts to fix them pose dangers to the Internet and global freedoms in themselves).

### 2.2.1. Global by nature

When we visit a website using a web browser such as Chrome, or make a phone call using Skype or another Internet-based calling system, our PCs or mobiles send data through the Internet to the relevant destination. Because of the open design of the Internet (which is its greatest strength), any end point on the network can communicate with virtually any other end point, following whatever route is calculated

16. See, for example: www.dailymail.co.uk/sciencetech/article-2291749/How-Facebook-likes-reveal-clues-sexuality-political-beliefs-religion.html and www.nbcnews.com/science/gay-conservative-high-iq-your-facebook-likes-can-reveal-traits-1C8805606. The academic research underpinning these findings, by Michal Kosinski of Cambridge University, UK, is reported here: www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions.
17. See: www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/. The background is explained in greater detail in Charles Duhigg, *The power of habit: why we do what we do in life and business*, Random House 2014.
18. Yves Poullet, "Internet of the future: achieving transparency, pluralism and democracy", available at www.crids.eu/recherche/publications/textes/internet-of-the-future/at_download/file (November 2009).

as being most efficient, the data flowing through all sorts of switches, routers and cables: the Internet's physical infrastructure. This infrastructure is inherently global: if you access the website of a company in your own country or even the website of your own country's government, or email them, if you Skype-call a friend in your own country, or "chat" with them on a social network, the data may still travel all around the world. The main Internet companies – giants like Google, Microsoft, Yahoo, Facebook and Twitter – all use massive facilities and servers through which such data are routed. At the moment, many of these are physically located in the USA (though the ongoing NSA spying scandal, discussed below, has already led to significant moves by countries and companies away from relying on Cloud providers and information and communications technology companies in the USA).[19]

### 2.2.2. The Cloud that is not in the sky

Companies store their data in vast data warehouses – often mirrored (i.e. duplicated) for practical or security reasons in different countries or even continents[20] – and increasingly in the Cloud, which means on servers managed by the Internet giants, who rent out the storage space and processing capabilities of their systems to companies. This can create useful flexibility and security, but it also means that data are increasingly stored and processed in different and multiple countries, and thus in different and multiple jurisdictions, from the place of establishment of the data controller and the data subjects (the individuals whose data are thus moved around). The Cloud is in reality still mostly in the USA and firmly anchored to the ground – under US jurisdiction.[21]

Even when the Cloud infrastructure is not physically in the USA, American courts have not been bashful when it comes to claiming jurisdiction. For example, in a case concerning a Microsoft email account, the U.S. District Court for the Southern District of New York ruled that data stored by Microsoft in Dublin (Ireland) could be subject to a US warrant by means of an order issued on 25 April 2014.[22] The judge justified this on the basis that the warrant should be considered more like a subpoena than a warrant and "the burden on the government would be substantial if they had to co-ordinate with foreign governments to obtain this sort of information from Internet service providers (ISPs) such as Microsoft and Google".[23]

Microsoft's response is also worthy of note. The company's deputy counsel provided the following analysis in a blog post: "A U.S. prosecutor cannot obtain a U.S. warrant to search someone's home located in another country, just as another country's prosecutor cannot obtain a court order in her home country to conduct a search in the United States. That is why the U.S. has entered into many bilateral agreements

19. "NSA spying risks 35 billion in U.S. technology sales", Bloomberg, 26 November 2013: www.bloomberg.com/news/2013-11-26/nsa-spying-risks-35-billion-in-u-s-technology-sales.html.
20. A highly revealing example of this is the worldwide processing of airline passenger name records (PNRs) through outsourced Computerized Reservation Systems (CRSs), as described by Edward Hasbrouck in these slides: http://hasbrouck.org/IDP/IDP-PNR-BRU-8APR2010.pdf (April 2010).
21. Hasbrouck (*ibid*.) notes that as a result "standard airline business processes completely bypass" the US-EU PNR agreement.
22. The memorandum and order are available at: www.nysd.uscourts.gov/cases/show.php?db=special&id=398.
23. BBC News, "Microsoft 'must release' data stored on Dublin server", 29 April 2014, available at www.bbc.com/news/technology-27191500.

establishing specific procedures for obtaining evidence in another country. We think the same rules should apply in the online world, but the government disagrees."[24]

The response of the European Commission to this analysis is equally clear. In particular, Commission Vice-President Viviane Reding stated that "the Commission remains of the view that where governments need to request personal data held by private companies and located in the EU, requests should not be directly addressed to the companies but should proceed via agreed formal channels of co-operation between public authorities, such as the mutual legal assistance agreements or sectorial EU-US agreements authorising such transfers".[25]

In the above case, the question did not come up as to whether, if Microsoft's terms of service had included a provision that gave theoretical consent to hand over data to unspecified law-enforcement authorities, that would have been sufficient to make the disclosure lawful.[26]

The Snowden revelations are spurring a rush (started earlier by reports about the Patriot Act) to create non-US clouds,[27] but these government efforts to bring services into specific jurisdictions threaten the open nature of the Internet itself.[28] It must be always remembered that the core functionality of the Internet is the ability of any end point on the Internet to communicate with any other end point or set of end points. Protection of this functionality must, therefore, remain a key policy priority.

### 2.2.3. The real backbones

The main infrastructure for the Internet consists of high-capacity fibre-optic cables running under the world's oceans and seas, and the associated land-based cables and routers.[29] For instance, the South East Asia–Middle East–West Europe 4project (SEA-ME-WE-4) is a "next generation submarine cable system linking South East Asia to Europe via the Indian Sub-Continent and Middle East";[30] the Georgia–Russia Optical Fibre Submarine Cable System connects Novorossisk in Russia and Poti in Georgia, but provides onwards access to and from western Europe and, *inter alia*, China, Japan, Iran and Central Asia.[31] The most important cables for Europe are those

24. David Howard, "One step on the path to challenging search warrant jurisdiction", 25 April 2014, available at http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/04/25/one-step-on-the-path-to-challenging-search-warrant-jurisdiction.aspx.
25. Out-law.com, "Reding: US authorities wrong to ask Microsoft to hand over customer data stored in the EU", 2 July 2014. Available at www.out-law.com/en/articles/2014/july/reding-us-authorities-wrong-to-ask-microsoft-directly-to-hand-over-customer-data-stored-in-the-eu/.
26. In section 3.4.5, below, we discuss the provision in the Cybercrime Convention that might allow such disclosures (but which is contentious).
27. See, for example, "Deutsche Telekom wants 'German Cloud' to shield data from U.S.", Bloomberg, 13 September 2011, at www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-to-shield-data-from-u-s-.html. In December 2013, a partnership of Deutsche Telekom and T-Systems announced it was offering Cloud services through "T-Systems' data centres in Germany [which] are subject to the strict German regulations for data privacy and compliance" – and thus not subject to US surveillance laws: www.telekom.com/media/enterprise-solutions/210306.
28. See section 2.3.1 below.
29. See the map at: www.submarinecablemap.com/.
30. See www.seamewe4.com/. The NSA tapped into the cable: http://rt.com/usa/nsa-top-unit-tao-954/ (1 January 2014).
31. Source: www.georgia-russia.dk/.

that run from continental Europe to the UK, and from there, under the Atlantic, to the USA. Given the dominance of the Internet and the Cloud by US companies (as just described), these cables carry a large proportion of all Internet traffic and Internet-based communication data, including almost all data to and from Europe.

## 2.3. Who is in control?

### 2.3.1. Internet governance

As the Council of Europe's Committee of Ministers recognised:[32]

> The Internet is an aggregate of a vast range of ideas, technologies, resources and policies developed on the assertion of freedom and through collective endeavours in the common interest. States, the private sector, civil society and individuals have all contributed to build the dynamic, inclusive and successful Internet that we know today. The Internet provides a space of freedom, facilitating the exercise and enjoyment of fundamental rights, participatory and democratic processes, and social and commercial activities.

In other words: there is no Internet government. No single state or international body is formally in overall charge of ensuring compliance with the law in respect of the way the Internet works. Indeed, there is no single law or set of laws, nor any overall treaty applicable to the Internet – although there are of course national laws and international treaties that are applicable to activities on the Internet.[33] Here, two broader matters should be noted: the principles of Internet governance to which the international community aspires; and the practical reality of extensive US control.

The basic Internet governance principles have been widely stated and affirmed by international forums, including the Council of Europe. For the purpose of this issue paper, the following are paramount.[34]

- The existing frameworks of general public international law and of international human rights law are equally applicable online and offline.[35]

---

32. Declaration by the Committee of Ministers on Internet governance principles, adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies, para. 1. On Internet governance generally and the various bodies involved, such as the Internet Corporation for Assigned Names and Numbers (ICANN) in Los Angeles, the UN-sponsored World Summit on the Information Society (WSIS), held in Tunis, and the Internet Governance Forum (IGF) set up there, see this *Wikipedia* entry and graph: https://en.wikipedia.org/wiki/Internet_governance and https://upload.wikimedia.org/wikipedia/commons/e/ed/Who-Runs-the-Internet-graphic.png.
33. In section 3, we look at the legal difficulties that arise in this respect.
34. Other major principles, reflected in IGF and Council of Europe documents alike, relate to the need to retain the decentralised, multi-stakeholder, culturally diverse approach to Internet governance, as well as the universality, openness, integrity and neutrality of the Internet; cf. the Internet Governance Principles in the Committee of Ministers Declaration (see n. 32 above) in particular. All these are indeed crucial to maintaining the essential, empowering features of the Internet as it was originally envisaged and developed, but this issue paper has a narrower focus, on ensuring the rule of law on the Internet; the selection of principles in the text reflects this.
35. See Council of Europe Internet Governance Strategy 2012-2015, Executive Summary, second paragraph. The same notion is affirmed in the UN General Assembly Resolution on "Privacy in the Digital Age", adopted without a vote on 18 December 2013, which says that "the same rights that people have offline must also be protected online, including the right to privacy".

- Internet governance arrangements must ensure the protection of all fundamental rights and freedoms, and affirm their universality, indivisibility, interdependence and inter-relation in accordance with international human rights law.
- They must also ensure full respect for democracy and the rule of law, and should promote sustainable development.
- The multi-stakeholder nature of Internet governance should also be promoted.
- All public and private actors should recognise and uphold human rights and fundamental freedoms in their operations and activities, as well as in the design of new technologies, services and applications. They should be aware of developments leading to the enhancement of, as well as threats to, fundamental rights and freedoms, and fully participate in efforts aimed at recognising newly emerging rights.[36]
- States have rights and responsibilities with regard to international Internet-related public policy issues. In the exercise of their sovereignty rights, states should, subject to international law, refrain from any action that would directly or indirectly harm persons or entities outside their territorial jurisdiction. Furthermore, any national decision or action amounting to a restriction of fundamental rights should comply with international obligations and in particular be based on law, be necessary in a democratic society and fully respect the principles of proportionality and the right of independent appeal, surrounded by appropriate legal and due process safeguards.[37]

The first point to make about the above principles is that they largely remain merely declaratory and aspirational: actual Internet governance arrangements still cannot be relied on to ensure their application. As shown in section 3 below, several important elements of international law and international human rights law need further clarification or affirmation; and several treaties contain important limitations and ambiguities that stand in the way of full achievement of the principles.

Second, the USA has much more control over the Internet than any other country, or even the rest of the world put together. For many years, this was seen as almost entirely beneficial, particularly in view of the USA's strong domestic protections of freedom of speech, but the almost unfettered global spying revealed by Edward Snowden has undermined this trust. Not only is it now clear that the US authorities feel they have no international legal duty to respect the privacy of non-US citizens living outside the USA,[38] but other states are becoming worried about the strategic

36. The principles in the second, third and fourth bullet points are from the first principle in the Council of Europe Internet Governance Principles (see n. 32 above) on Human rights, democracy and the rule of law. Note in particular the express statement that private actors such as companies have a duty to "recognise and uphold" human rights. The next bullet point makes clear that the duties referred to in the fourth one also apply to states (if anything, a fortiori).
37. Third principle in the Council of Europe Internet Governance Principles, on Responsibilities of States. The reference to state actions causing "harm" must of course be read as including any state actions that violate the human rights of "persons or entities outside the [State's] territorial jurisdiction".
38. See the discussion in section 3.4 under "Within [a contracting state's] [territory and] jurisdiction".

implications of US dominance over the Internet. The USA's effective control over technologies like DNS SEC (Domain Name System Security Extensions) or RPKI (Resource Public Key Infrastructure)[39] could in theory be abused by the USA to cut countries off from the Internet.[40]

It is worth noting that several important guarantees in the US Constitution, including the First and Fourth Amendments, essentially cover only US citizens and people physically on US territory. Also, the constitution effectively constrains only the organs of the US Government and not any actions of private parties that come about as a result of government encouragement.

Even before the Snowden revelations, Russia, China and other countries were trying to wrestle control over the Internet away from the USA. Russia proposed an intergovernmental structure within an ITU/UN framework – but appears to have back-pedalled on the idea[41] – with the support of, *inter alia*, China, Tajikistan and Uzbekistan.[42] For instance, in 2012 China "propose[d] a way to alter Internet standards to partition the Internet into autonomously administered national networks, using the domain name system".[43] These proposals, if implemented, would have[44]

> authorize[d] [ITU] member nations, with UN blessing, to inspect and censor incoming and outgoing Internet traffic on the premise of monitoring criminal behavior, filtering spam, or protecting national security.

These proposals were defeated, but of course we have since learned that "inspect[ing] … Internet traffic on the premise of … protecting national security" has been done on an unprecedented scale by the USA itself. Following the Snowden leaks, in particular the revelation that the US had been spying on the Brazilian president, Brazil's government published "ambitious plans to promote its own networking technology, encourage regional Internet traffic to be routed locally, and even set up a secure national email service."[45]

There are fears that such responses to the Snowden revelations, and similar responses of European states and EU officials, may lead to fragmentation of the Internet.[46] That could destroy the Internet as we know it, because efforts to bring key services under national control would facilitate the "sovereign right to manage the Internet within

---

39. On details of these technical matters, see: www.icann.org/en/about/learning/factsheets/dnssec-qaa-09oct08-en.htm and https://en.wikipedia.org/wiki/Resource_Public_Key_Infrastructure.
40. See www.circleid.com/posts/20131027_nobody_has_proposed_sustainable_model_for_internet_governance_yet/ (October 2013) – but, the author argues, the current system is unsustainable.
41. See http://news.cnet.com/8301-13578_3-57551442-38/russia-demands-broad-un-role-in-net-governance-leak-reveals/ (November 2012) and http://content.netmundial.br/contribution/themes/133 (submitted prior to Netmundial, in April 2014).
42. See http://content.netmundial.br/files/67.pdf (September 2011).
43. See www.internetgovernance.org/2012/06/18/proposed-new-ietf-standard-would-create-a-nationally-partitioned-internet/.
44. See http://news.cnet.com/8301-13578_3-57551442-38/russia-demands-broad-un-role-in-net-governance-leak-reveals/.
45. Ian Brown, "Will NSA revelations lead to the Balkanisation of the internet", *The Guardian*, 1 November 2013, at www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet.
46. Ibid.

their national territory" proposed by the Russian Federation (and strongly resisted by civil society groups) at the UN World Conference on International Telecommunications and backed by other countries, including China.[47] This approach would create national barriers to a global network that is now an indispensable asset for democracy worldwide. Dismantling the Internet's biggest asset – its open and global nature – is not the way to solve problems with one government's unwelcome attitude to it. However, unless the USA changes its stand on complying with international human rights law in relation to its activities that affect the Internet and global communication systems, the movement towards such a truncated Internet will be difficult to stop.

### 2.3.2. Private-sector control

Leaving aside the significant control that the USA, as a state, has over the Internet, and over the Internet giants, it should be noted that ISPs and e-communication service providers – telecoms and mobile network operators (MNOs) – are in any case private companies, subject to the laws of the countries in which they operate.

This creates two problems, to which we return in section 3, especially 3.5. First, as private entities, such companies are not directly bound by international human rights law, which applies only to states and governments. It is thus more difficult to obtain redress against such companies. This is particularly problematic when companies on a "voluntary" basis take action that limits full enjoyment of fundamental rights by individuals using their services – for example, when ISPs block access to certain sites because the ISPs believe, or are told, that the sites contain, or provide access to, illegal content such as child pornography, pirated videos or terrorist material – or are simply unwelcome. If the major ISPs in a country jointly agree to such measures, this can effectively block access to the targeted sites for the vast majority of ordinary Internet users in that country. This is even worse when viewed from the opposite perspective – if a major ISP in a country voluntarily blocks your site, then your right to impart information to much of the population of that country is removed by an entity with which you have no business relationship.

The problem is aggravated if such measures (e.g. blocking) are "encouraged" by the state, but not legally or formally required by the state in question. An example of such state "encouragement" was the US vice-president's description of Wikileaks founder Julian Assange as "like a hi-tech terrorist".[48] Subsequently, the major payment-service providers (on the basis of their broad terms of service) removed payment services from Wikileaks, and Amazon Web Services chose (also on the basis of a broad interpretation of their terms of service) to remove web-hosting services from the organisation. Similarly, the US company Tableau Software publicly admitted that it removed services from Wikileaks after pressure from US Senator Joe Lieberman.[49]

---

47. White Paper issued by the Information Office of the State Council of the People's Republic of China in 2010.
48. Ewan MacAskill, "Julian Assange is like a hi-tech terrorist", *The Guardian*, 19 December 2010. Available at www.theguardian.com/media/2010/dec/19/assange-high-tech-terrorist-biden.
49. *The Guardian*, "Wikileaks cables visualisation pulled after pressure from Joe Lieberman", 3 December 2013. Available at www.theguardian.com/world/blog/2010/dec/03/wikileaks-tableau-visualisation-joe-lieberman.

Such restrictions would almost certainly be impossible to impose by law in the USA, due to constitutional safeguards for free speech, but were possible with the very flexible and unpredictable terms of service of the service providers.

Second, private entities are subject to the national laws of the countries in which they are established or active – and those laws do not always conform to international law or international human rights standards: they may impose restrictions on activities on the Internet (typically, on freedom of expression) that violate international human rights law; or they may impose or allow interference, such as surveillance of Internet activity or e-communications, that is contrary to international human rights law; and they may be applied extraterritorially, in violation of the sovereignty of other states.

A major example of this is Google's global enforcement of the US Digital Millennium Copyright Act (DMCA). Under this act, if an appropriately formatted complaint is delivered to Google, the company will render the resource in question un-findable by any Google service worldwide, regardless of local laws or procedures. A report by the US NGO Electronic Frontier Foundation (EFF), "Unintended consequences: fifteen years under the DMCA", extensively analyses the domestic damage done by the DMCA.[50] It can be debated whether the DMCA would meet the principle of "prescribed by law",[51] but it is clearly unpredictable and non-transparent for non-US citizens to be subject to a foreign law in this manner.

Companies in states that have adopted such laws often feel obliged – and can be legally forced – to assist those states in applying them. Under those laws, they can sometimes be required to keep their compliance secret, even from their customers and/or the individuals (the data subjects) affected.

Thus, under US law, US companies can be required by the US National Security Agency to "pull" certain data from their servers and hand those data to the NSA to support the latter's national security operations, even if the data are held in servers outside the USA and relate to companies and individuals in another country; the US companies in question can at the same time be ordered not to reveal these disclosures to their non-US clients or to any non-US individuals whose personal data may have been passed on, or to governmental bodies (such as data-protection authorities or communications regulators) in the other country.

These matters are complicated further when states try to impose restrictions on the Internet activities of individuals who live in other countries, by requiring companies that are subject to their jurisdiction to give effect to those restrictions, when those activities are lawful under the law of the country of residence of these individuals. For instance, in the Yahoo! Nazi memorabilia case, the US company was asked to restrict access to its site in order to comply with French restrictions on the sale of such memorabilia.[52]

---

50. See https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca.
51. On this requirement, see section 3.2.1, below.
52. On the Yahoo! case and related issues, see section 3.4.2 below (with references to that case in notes 109-111).

Another complication arises if, in this, the relevant states discriminate between nationals or residents and non-nationals or non-residents, and force the companies to do so too.

The application of national law to private entities controlling (significant parts of) the digital world is therefore extremely complex and delicate. On the one hand, states have a right, and indeed a duty, to counter criminal activity that uses the Internet or e-communication systems. In this, they naturally enlist the help of relevant private actors. Responsible companies will also want to avoid their products and services being used for criminal purposes. Nonetheless, in such circumstances, states should in their actions both fully comply with their international human rights commitments and fully respect the sovereignty of other states. In particular, states should not circumvent constitutional or international law obligations by encouraging restrictions on human rights through "voluntary" actions by intermediaries; and companies, too, should respect the human rights of individuals.

In section 3, we discuss both the international legal requirements of the rule of law that arise in this respect and the (so far, limited) arrangements and new principles that should cover such activities by states and companies alike.

Chapter 3

# The rule of law in the digital environment

## 3.1. The rule of law

The Secretary-General of the United Nations has explained the concept of the rule of law in the following terms:[53]

> For the United Nations, the rule of law refers to a principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency.

This chimes well with the approach to the rule of law taken by the European Court of Human Rights (hereinafter the Court) under the European Convention on Human Rights (hereinafter the Convention or ECHR). This emphasises that the main aim of the Convention is to prevent arbitrariness, seen as the opposite of the rule of law. The case law on legitimate restrictions of human rights focuses on the following requirements, very similar to those named above by the UN Secretary-General:[54]

- the need for all restrictions on or limitations of, or interferences with, human rights to be based on "law" (as expressly stipulated in Articles 8-11 of the Convention, but as also mentioned in the other substantive articles),[55] with that law having to be accessible, and of a certain "quality";

53. See the UN Secretary-General's report "The rule of law and transitional justice in conflict and post-conflict societies", S/2004/616 (23 August 2004), para. 6, at: www.unrol.org/doc.aspx?n=2004+report.pdf. For further references and more on the UN's extensive work on the rule of law, see www.un.org/en/ruleoflaw/.

54. The tests listed here are part of the Court's standard approach to issues under Articles 8-11 of the Convention, but are also applied *mutatis mutandis* under the other articles, as summarised in Douwe Korff, *The standard approach under Articles 8-11 ECHR and Article 2 ECHR*, available at http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf. For the specific application of each of these tests under each specific article, see the Council of Europe Human Rights Handbooks on Articles 2, 8, 9 and 10 ECHR (there is as yet no handbook on Article 11) and Article 1 of the First Protocol, available at www.coe.int/en/web/human-rights-rule-of-law/human-rights-handbooks.

55. Cf. the first sentence of Article 2(1), which if anything is stricter in this regard, and the references to "lawful" in all three sub-clauses of Article 2(2); the 12 references to "law", "lawful" or "legal" in Article 5(1); the references to "law" in Articles 6 and 7; and the reference to "laws" in Article 12.

- the need for all restrictions to serve a "legitimate aim" (for Articles 8-11, one of the aims specifically listed in the relevant article) and to be "necessary" and "proportionate" to that aim (subject to a certain "margin of appreciation" within which the state can decide what is "necessary" and "proportionate", but which goes "hand in hand with European supervision" by the Court);
- the need for all restrictions to be "compatible with the rule of law", which essentially means that they must be compatible with the other requirements and the general scheme of the Convention, including the prohibition on discrimination, and, especially, not "arbitrary"; and
- as particularly important safeguards against such arbitrariness, there must not be excessive discretion and there must be an "effective remedy", preferably a judicial one, against any (alleged) violation of a Convention right.

Below, we briefly look at each of these basic rule-of-law requirements. Here, it may be noted that this "standard" approach of the European Court of Human Rights is also followed by the Court of Justice of the European Union (CJEU) in appropriate cases,[56] by the Human Rights Committee in its rulings ("views" and "general comments") under the UN International Covenant on Civil and Political Rights,[57] and by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.[58] The typical, standard requirements first adduced by the Court have become accepted as not just European, but also globally recognised essential elements of the rule of law.

After these "standard" issues, we look at three further core issues for modern human rights law and the international legal order since the Second World War:

- the need to ensure the basic rights, and these basic rule-of-law requirements, for "everyone", without discrimination;
- the need to ensure these rights and requirements also in relation to exercise of a state's powers outside its national territory; and
- the need to ensure these rights and requirements also in relation to activities of private entities, in particular national and transnational corporations.

---

56. This applies in particular to the principles of legality and proportionality (which in EU law is seen as incorporating the requirement of necessity). On the principle of legality, see *Opel Austria v. the Council*, 22 January 1991, Case T-115/94, paras. 124 (with references to earlier cases) and 130, at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&numdoc=61994A0115&lg=en. On the principle of (necessity and) proportionality, see what is still the leading case, Fedesa and Others, 13 November 1990, C-331/88, para. 10, at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=en&numdoc=61988J0331.
57. Cf. in particular the Human Rights Committee's General Comment No. 31 on The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, adopted on 29 March 2004 (UN Document CCPR/C/21/Rev.1/Add. 13), para. 6, at: http://ccprcentre.org/doc/ICCPR/General%20Comments/CCPR.C.21.Rev1.Add13_%28GC31%29_En.pdf.
58. See in particular the first report of the Special Rapporteur dated 20 April 2010, UN Document A/HRC/14/23, section C (permissible restrictions and limitations on freedom of expression), paras. 74-81, at www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf.

## 3.2. The basic "rule of law" tests developed by the European Court of Human Rights

### 3.2.1. "Law"

According to the European Court of Human Rights, the following are two of the requirements that flow from the expression "prescribed by law":

> Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. Those consequences need not be foreseeable with absolute certainty: experience shows this to be unattainable. Again, whilst certainty is highly desirable, it may bring in its train excessive rigidity and the law must be able to keep pace with changing circumstances. Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice.[59]

Secret rules, or secret guidelines on or interpretations of the rules, that an affected person cannot know, are not "law".[60] Neither are laws or subsidiary rules that give the authorities excessive discretion: such laws do not protect against arbitrary exercise of the powers in question. The scope and manner of exercise of any discretion granted must therefore be indicated (in the law itself, or in binding, published guidelines) with "reasonable clarity", so that, again, individuals can reasonably foresee how the law will be applied in practice.[61] Moreover,[62]

> Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident.

Such secret powers must therefore be subject to especially clear and precise, strict rules and especially close and strong oversight.

### 3.2.2. "Necessary [and proportionate]" in relation to a "legitimate aim"

Restrictions on the exercise of the main Convention rights set out in Articles 8-11 of the ECHR are only compatible with the Convention if they are "necessary" for a legitimate aim, which for these rights must be one of the aims specifically listed in the article in question. These aims are quite broadly phrased: they include public safety, prevention of crime, protection of morals and of the rights of others, and

---

59. *The Sunday Times v. the United Kingdom (No. 1)*, Application no. 6538/74, judgment of 26 April 1979, para. 49. This has become the standard interpretation.
60. *Silver v. the UK*, Applications nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75 and 7136/75, judgment of 25 March 1983; *Petra v. Romania*, Application no. 27273/95, judgment of 23 September 1998.
61. See *Petra v. Romania* (see n. 60 above), paras. 37-38. In *Malone v. the UK*, Application no. 8691/79, judgment of 2 August 1984, para. 68, the Court used the expression "sufficient clarity".
62. *Malone v. the UK* (see note 61 above), para. 67.

national security. It is notable, however, that the right to manifest one's religion or beliefs may not be limited or interfered with on grounds of national security.[63]

The Court has clarified the meaning of the term "necessary" by saying that,[64]

> whilst the adjective "necessary" … is not synonymous with "indispensable" …, neither has it the flexibility of such expressions as "admissible", "ordinary" …, "useful" …, "reasonable" … or "desirable".

If a measure that interferes with a right is to be judged "necessary", it has to correspond to a "pressing social need" and it must be "proportionate" to that need.[65] Subject to the "margin of appreciation" doctrine, discussed below, the Court makes its assessment of the necessity and proportionality of a measure "in the light of all the circumstances". However, some measures deserve closer scrutiny than others. Therefore:[66]

> Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.

### 3.2.3. The "margin of appreciation" doctrine

In assessing whether a measure that interferes with a Convention right is "necessary" and "legitimate", the Court leaves to the state a certain "margin of appreciation". Under this doctrine (which was first developed in relation to the derogation clause, Article 15),[67]

> it is for the national authorities to make the initial assessment of the reality of the pressing social need implied by the notion of "necessity" in [the context of the specific case].

However,

> The Court … is empowered to give the final ruling on whether a "restriction" or "penalty" is reconcilable with [the right in question]. The domestic margin of appreciation thus goes hand in hand with a European supervision. Such supervision concerns both the aim of the measure challenged and its "necessity"; it covers not only the basic legislation but also the decision applying it, even one given by an independent court.

The width of the margin of appreciation depends on various factors. In some contexts, such as morals and national security, the Court tends to grant states a wide margin of appreciation, whereas in others the margin can be quite narrow. The latter is especially the case if the issue is largely objective, or if there is a large measure of

---

63. Note that the actual holding of beliefs may not be limited or interfered with at all: this is part of a person's "inner sanctum", into which the state may not intrude. Only "manifestations" of a religion or belief may be limited (to the extent necessary).
64. *Handyside v. the UK*, Application no. 5493/72, judgment of 7 December 1976, para. 48.
65. Ibid., paras. 48 and 49.
66. *Klass and Others v. Germany*, Application no. 5029/71, judgment of 6 September 1978, para. 42.
67. *Handyside v. the UK* (see n. 64 above), para. 48.

convergence in law and practice in European states, or if there are accepted global or Europe-wide standards in the relevant area.

### 3.2.4. "An effective [preferably judicial] remedy"[68]

According to Article 6 ECHR,

> In the determination of his civil rights and obligations *[droits de caractère civil]* or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law.

In other words, in all civil and criminal cases, there is a right to a full judicial trial before a proper court. This right of course also applies to anyone sued in a civil court or tried in a criminal court, in relation to something that a person did online.[69]

Apart from the above, according to Article 13 ECHR,

> Everyone whose rights and freedoms as set forth in this Convention are violated should have an effective remedy before a national authority notwithstanding that the violation has been committed by a person acting in an official capacity.

Generally, the right to a remedy under Article 13 is "absorbed" in the right to a fair trial under Article 6, and Article 13 therefore (with rare exceptions) only applies to cases that are neither about civil law nor about a criminal charge.[70]

In spite of the text, individuals can rely on Article 13 – that is, they must be offered a remedy – whenever they have an "arguable claim" that one of their rights under the Convention has been violated; they do not have to prove an actual violation has taken place before they can access a remedy: that would render the guarantee largely meaningless.[71]

The "national authority" competent for providing the remedy need not be a judicial authority, but the powers and procedural guarantees of an authority must be taken into account in determining whether a particular remedy is effective. The Court has held in several cases relating to secret surveillance that, in that very special context, non-judicial remedies could suffice.[72] However, even in such cases, the Court looks carefully at the level of independence, impartiality and competence of the authority in question. Basically, a remedy under Article 13 should be as close to a full judicial remedy as possible; any departures from the trappings of a proper judicial forum must be justified by the special context.

---

68. For an overview of this right, see the Venice Commission's Report on the Effectiveness of National Remedies in respect of Excessive Length of Proceedings, 2006 (published in 2007), at www.venice.coe.int/webforms/documents/CDL-AD(2006)036rev.aspx.
69. When domestic courts can or should assume they have jurisdiction in transnational cases is a different question, dealt with under 3.6 "Sovereignty, non-interference and extraterritorial acts" below.
70. The main exception is alleged excessive length of proceedings; see the Venice Commission report (see n. 68 above), paras. 42-47.
71. *Klass and Others v. Germany* (see n. 66 above), para. 64.
72. Ibid., para. 67; *Leander v. Sweden,* Application no. 9248/81, judgment of 26 March 1987, para. 83.

## 3.3. "Everyone", without discrimination

### 3.3.1. The principle of non-discrimination in international law

It is one of the hallmarks of international human rights law since 1945, and one of its greatest achievements, that human rights must be accorded to "everyone", to all human beings. That is a departure from previous practice, in which such rights were still often seen as pertaining only to citizens of a state, not to foreigners (except perhaps foreign residents), and/or based on reciprocity. That approach was explicitly rejected in Articles 1 and 2 of the Universal Declaration of Human Rights (UDHR):

> All human beings are born free and equal in dignity and rights. …
> Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.

This is not just aspirational. On the contrary, this approach was confirmed by, and under, the binding international human rights treaties adopted to implement the UDHR, including the UN ICCPR and the ECHR:[73]

> In general, the rights set forth in the Covenant apply to everyone, irrespective of reciprocity, and irrespective of his or her nationality or statelessness.[74]

The application of the human rights guarantees in the ECHR and ICCPR to "everyone", irrespective of nationality or national status, has been consistently affirmed in the case law of the European Court of Human Rights and by the Human Rights Committee.[75] As the latter expressly states, after listing all the rights that must be granted also to aliens, including freedom of expression and opinion, and freedom from arbitrary or unlawful interference with their privacy, family, home or correspondence, "There shall be no discrimination between aliens and citizens in the application of these rights."[76]

### 3.3.2. US law

Because of the unique place of the USA and US companies in the functioning of the Internet, the constitutional and corporate legal framework in the USA is of particular importance. However, in contrast to the above-mentioned principle of international human rights law, many of the human rights guarantees in the US Constitution and in various US laws relating to the digital environment apply only to US citizens and non-US

---

73. Note that the ECHR, too, is expressly inspired by the Universal Declaration of Human Rights; see the first two preambular considerations.
74. Human Rights Committee, General Comment No. 15 on "The position of aliens under the Covenant", adopted 11 April 1986 (UN Document HRI/GEN/1/Rev.9 (Vol. I)), para. 1, available at http://ccprcentre.org/doc/ICCPR/General%20Comments/HRI.GEN.1.Rev.9%28Vol.I%29_%28GC15%29_en.pdf.
75. On the situation under the ECHR, see Hélène Lambert, *The position of aliens in relation to the European Convention on Human Rights*, Council of Europe Human Rights Files No. 8, Council of Europe 2007, at www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-08(2007).pdf.
76. Human Rights Committee, General Comment No. 15 (see n. 74 above), para. 7.

citizens residing in the USA. Only "US persons" benefit from the First Amendment, covering free speech and freedom of association,[77] the Fourth Amendment, protecting US citizens from "unreasonable searches",[78] and most of the (limited) protections against excessive surveillance in the FISA Amendment and Patriot Acts.[79]

Most notoriously, paragraph 1881a of FISA (introduced by the FISA Amendment Act in 2008), allows the US Attorney General and Director of National Intelligence to jointly authorise "the targeting of persons reasonably believed to be located outside the United States" in order "to acquire foreign intelligence information". "Foreign intelligence information" is sweepingly defined in paragraph 1881, in relation to non-US persons, as including any "information with respect to a foreign power … that relates to … the conduct of the foreign affairs of the United States"; and the term "foreign power" includes any "foreign-based political organization", including political entities associated with the state (such as political parties) and any politically active non-governmental organisation. Consequently, as Bowden et al. put it, "it is lawful in the US to conduct purely political surveillance on foreigners' data accessible in US clouds".[80] It also allows for economic espionage, and Snowden has confirmed that such espionage takes place.[81] These authorisations are subject to very limited review by the FISA Court, which operates in secret; the review is essentially limited to a verification that not too much information on "US persons" is incidentally obtained under such an order.[82]

---

77. "[T]he interests in free speech and freedom of association of foreign nationals acting outside the borders, jurisdiction, and control of the United States do not fall within the interests protected by the First Amendment" (*DKT Memorial Fund Ltd. v. Agency for International Development*, 1989, quoted in *Chevron Corporation v. Steven Donziger et al.*, US District Judge Kaplan order of 25 June 2013).
78. The Fourth Amendment does not apply if the person affected by a "search" (which includes online searches) has no "significant voluntary connection with the United States": *US v. Verdugo-Urquidez*, 1979. This was confirmed to the EU-US Working Group on Data Protection, set up to investigate the US surveillance activities exposed by Snowden: see Report on the Findings by the EU Co-chairs of the Ad hoc EU-US Working Group on Data Protection, 27 November 2013, section 2, para. 2.
79. See Caspar Bowden et al., report to the European Parliament, "Fighting cybercrime and protecting privacy in the cloud", 2012, and the article by Caspar Bowden and Judith Rauhofer, "Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud", 2013, available at www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050 and http://ssrn.com/abstract=2283175.
80. Bowden et al., "Fighting cybercrime and protection privacy in the cloud" (see n. 79), p. 34.
81. "Snowden says NSA engages in industrial espionage", Reuters, 26 January 2014 (reporting on a televised interview with Snowden), available at www.reuters.com/article/2014/01/26/us-security-snowden-germany-idUSBREA0P0DE20140126.
82. "Reform the FISA court: privacy law should never be radically reinterpreted in secret", Electronic Frontier Foundation, 10 July 2013, at https://www.eff.org/deeplinks/2013/07/fisa-court-has-been-radically-reinterpreting-privacy-law-secret. Cf. "In secret, court vastly broadens powers of N.S.A.", *New York Times*, 6 July 2013, at www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?pagewanted=all&_r=0. A rare non-secret ruling is reported here: www.nytimes.com/2009/01/15/world/americas/15iht-15fisa.19390748.html. "Court grants secrecy for memo on phone data", 3 January 2014, *New York Times*, reports a ruling by the US Court of Appeals for the District of Columbia Circuit, upholding "a broad conception of the executive branch's power to keep secret its interpretation of what the law permits it to do": www.nytimes.com/2014/01/04/us/court-backs-shielding-of-legal-memo-on-phone-records.html?ref=us&_r=1&. Actual court ruling at www.cadc.uscourts.gov/internet/opinions.nsf/BA847AE67CFA826785257C550053C612/$file/12-5363-1473387.pdf. See also the Common Dreams report, "Secret court to NSA: keep up the spying – FISA court ruling continues pattern of reauthorizing the NSA's 'almost Orwellian' bulk telephone metadata collection", 4 January 2014, at https://www.commondreams.org/headline/2014/01/04.

This means that the USA does not ensure that the actions of its own agents and agencies in relation to non-US-resident foreigners, such as European citizens, comply with the ICCPR or international human rights law generally. Moreover, because the USA does not seek itself to protect the human rights of foreigners, except for foreign residents, it also does not feel obliged to ensure that US corporations respect the rights of foreigners – see the discussion of the "indirect horizontal effect" (*Drittwirkung*) in section 3.5.1, below.

This non-application of human rights protections to non-US citizens outside the USA is in line with the US view (discussed in section 3.4.1) that – contrary to what has been held by the Human Rights Committee and the International Court of Justice – it is not bound by its obligations under the ICCPR in respect of acts done outside its physical territory.[83] This is particularly troubling in relation to the US's global Internet and communications surveillance programmes, revealed by Edward Snowden, but in view of the still dominant role of the USA on the Internet and in global communications (and their infrastructure) it has wider implications for the global rule of law in the new digital environment, as discussed below in section 4.

## 3.4. "Within [a contracting state's] [territory and] jurisdiction"[84]

### 3.4.1. The duty of states to comply with their responsibilities under international human rights law also when acting extraterritorially

#### Questions of jurisdiction

The only caveat to the above analysis with regard to the duty in terms of binding human rights treaty law lies in the text of Article 2(1) of the ICCPR and Article 1 ECHR (the non-discrimination requirements are spelled out separately in Article 14). The two articles state:

> Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognised in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. (Article 2(1) ICCPR)
>
> The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in [the substantive part of] this Convention. (Article 1 ECHR)

At first glance, these provisions may seem to suggest that states are only required to "respect", "ensure" or "secure" the rights in the international human rights treaties

83. See section 3.4.1, below.

84. Section 3.4 draws on Douwe Korff, "Note on European & international law on trans-national surveillance", prepared for the Civil Liberties Committee of the European Parliament, to assist the Committee in its enquiries into USA and European States' surveillance, August 2013, available at: www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_korff_/note_korff_en.pdf. Note that this section is limited to the transnational issues arising under international human rights law. The issue of the compatibility with wider public international law of actions of a state outside its territory, or actions that have effects outside its territory, is discussed in section 3.7, below.

on their own territory. It is certainly true that, at the time of drafting these treaties, sovereignty and jurisdiction were still primarily seen as territorial concepts[85] and, as is clear from the judgment quoted below, the European Court of Human Rights also regards the concept of "jurisdiction" as "primarily territorial".

However, in the Court's case law, and in the case law of the other international human rights adjudicating bodies, and indeed in the case law of the International Court of Justice, it has become clear that the concept of jurisdiction is shifting to a more functional one, at least in special cases, such as when agents of a state are acting outside the state and exercise control outside the state. Thus, as the European Court of Human Rights put it:[86]

> It follows from Article 1 [ECHR] that Contracting States must answer for any infringement of the rights and freedoms protected by the Convention committed against individuals placed under their "jurisdiction".
> The exercise of jurisdiction is a necessary condition for a Contracting State to be able to be held responsible for acts or omissions imputable to it which give rise to an allegation of the infringement of rights and freedoms set forth in the Convention ….
> The established case law in this area indicates that the concept of "jurisdiction" for the purposes of Article 1 of the Convention must be considered to reflect the term's meaning in public international law …
> From the standpoint of public international law, the words "within their jurisdiction" in Article 1 of the Convention must be understood to mean that a State's jurisdictional competence is primarily territorial …, but also that jurisdiction is presumed to be exercised normally throughout the State's territory. However, the concept of "jurisdiction" within the meaning of Article 1 of the Convention is not necessarily restricted to the national territory of the High Contracting Parties … In exceptional circumstances the acts of Contracting States performed outside their territory or which produce effects there ("extra-territorial act") may amount to exercise by them of their jurisdiction within the meaning of Article 1 of the Convention.
> According to the relevant principles of international law, a State's responsibility may be engaged where, as a consequence of military action – whether lawful or unlawful – that State in practice exercises effective control of an area situated outside its national territory. The obligation to secure, in such an area, the rights and freedoms set out in the Convention derives from the fact of such control, whether it be exercised directly, through its armed forces, or through a subordinate local administration …
> It is not necessary to determine whether a Contracting Party actually exercises detailed control over the policies and actions of the authorities in the area situated outside its national territory, since even overall control of the area may engage the responsibility of the Contracting Party concerned …
> Moreover, a State may also be held accountable for violation of the Convention rights and freedoms of persons who are in the territory of another State but

85. Cf. the Lotus judgment of the Permanent Court of International Justice (forerunner of the International Court of Justice), 7 September 1927, pp. 18-19, at www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.

86. *Issa and Others v. Turkey*, Application no. 31821/96, judgment of 16 November 2004, paras. 66-71; references to other cases omitted.

> who are found to be under the former State's authority and control through its agents operating – whether lawfully or unlawfully – in the latter State …. Accountability in such situations stems from the fact that Article 1 of the Convention cannot be interpreted so as to allow a State party to perpetrate violations of the Convention on the territory of another State, which it could not perpetrate on its own territory …

It is notable that the Court, in the final paragraph just quoted, expressly refers not only to its own case law, but also to a decision of the Inter-American Commission of Human Rights, *Coard et al. v. the United States*,[87] and to the views adopted by the Human Rights Committee in the cases of *Lopez Burgos v. Uruguay* and *Celiberti de Casariego v. Uruguay*,[88] showing that this shift towards a more functional approach to the obligations of states has broad support in the international human rights forums.

This is confirmed by the Human Rights Committee in its General Comment on *The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, where it says:[89]

> States Parties are required by Article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party. As indicated in General Comment 15 adopted at the twenty-seventh session (1986), the enjoyment of Covenant rights is not limited to citizens of States Parties but must also be available to all individuals, regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers and other persons, who may find themselves in the territory or subject to the jurisdiction of the State Party. This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained, such as forces constituting a national contingent of a State Party assigned to an international peace-keeping or peace-enforcement operation.

Most of the ECHR and ICCPR cases concern the exercise of state power by state agents such as soldiers on the soil of other states. If soldiers of a state that is party to the ICCPR, the I-ACHR or the ECHR exercise "effective control" of an area in another country, and put a person in that area under their authority – for instance, by detaining them or killing or injuring them – then the state under whose control they are operating is responsible for those actions under international human rights law: such victims are "within the jurisdiction" of the state concerned.[90]

The International Court of Justice similarly held that Israel had violated its obligations under the ICCPR in its building of a wall in occupied Palestinian territory, even though

87. Decision of 29 September 1999, Report No. 109/99, case No. 10.951, §§ 37, 39, 41 and 43.
88. Case nos. 52/1979 and 56/1979, both of 29 July 1981, at §§ 12.3 and 10.3 respectively.
89. General Comment No. 31 (see n. 57 above), para. 10.
90. For more such cases, see the European Court of Human Rights Factsheet on "Extra-territorial jurisdiction of ECHR States Parties" (December 2013) at www.echr.coe.int/Documents/FS_Extra-territorial_jurisdiction_ENG.pdf.

Israel had argued that the wall was not on its territory and that its obligations under the ICCPR did not apply extraterritorially.[91]

However, in recognition of the broad principle quoted above, that states should not be allowed to perpetrate violations of international human rights law on the territory of another state that they could not perpetrate on their own territory, the concept of "extraterritorial acts" that come within the "jurisdiction" of a state is wider than just physical acts on permanently or temporarily occupied foreign soil.[92]

### Jurisdiction in the digital world

The reference by the European Court of Human Rights to acts that "produce effects" in other states is important for the new digital environment, which (see section 1 above) is by its nature transnational. Thus, if a state intercepts, extracts copies of and analyses communications of individuals and organisations outside that state, it "produces effects" on those concerned, and on their rights, even if they are ("foreigners" and) not physically on the territory of the state concerned. Moreover, it would be perverse to argue that, if a state explicitly legislates to authorise such surveillance, it is not exercising its "jurisdiction" in that respect: bringing certain matters (such as electronic communications, or Internet or social network activities) within the legal rules of a country, making those activities subject to the legal order of a country, is perhaps the most conspicuous way to exercise a country's jurisdiction. In international legal terms, in adopting such a law, the country is exercising "prescriptive jurisdiction" over the data. If it then seeks to enforce the law, it is exercising "enforcement jurisdiction". Finally, if it seeks to apply and enforce the law outside its own territory, it exercises these forms of jurisdiction extraterritorially.[93]

This is the case even if the exercise of that jurisdiction would violate the sovereignty of another state, for example, because it concerned data physically located in another country (see the discussion in section 3.5, below) and was not subject to a specific international law exception or lacked clear ties to the jurisdiction in question. In the Yahoo! case in Belgium, the Belgian Supreme Court ruled that a company providing electronic communications services (defined very broadly – essentially the making available of a website on the territory of the country) in Belgium is under an obligation

91. International Court of Justice, *Advisory Opinion on the legal consequences of the construction of a wall in the occupied Palestinian territory,* 9 July 2004, paras. 134 and 137, available at: www.icj-cij.org/docket/files/131/1671.pdf.

92. *Issa and Others v. Turkey* (see n. 86), para. 68. Martin Scheinin, the first United Nations Special Rapporteur on human rights and counter-terrorism (2005-11), draws the same conclusion from his analysis of the Human Rights Committee's case law, presented to the US Privacy and Civil Liberties Oversight Board's hearing on the NSA surveillance programme on 19 March 2014: "As [the cases] demonstrate, in respect of human rights violations such as discrimination or preventing someone from leaving a country, the relationship between the violating state and the individual need not amount to effective control over a territory or a person. It is sufficient that a state has control over someone's rights, or authority over a person or context. The situation is the same with privacy." See: www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0085.

93. On the question of jurisdiction and limitations to it in international law generally, see: Vaughan Lowe, "Jurisdiction", chapter 10 in Malcolm Evans (ed.), *International Law*, Oxford University Press, 2003. See also 3.6, below.

to provide personal data to a public prosecutor, regardless of the physical location of the data in question.[94] Of course, following the logic of the New York court in the Microsoft case mentioned above, the data would also be under US jurisdiction. One can also imagine some less extreme cross-border access cases, for example where all parties (the state, the plaintiff and the defendant, the communications provider) are in one jurisdiction and the data happen to be in another jurisdiction.

A state that uses its legislative and enforcement powers to capture or otherwise exercise control over personal data that are not held on its physical territory but on the territory of another state, for example, by using the physical infrastructure of the Internet and global e-communications systems to extract those data from servers, personal computers or mobile devices in the other state, or by requiring private entities that have access to such data abroad to extract those data from the servers or devices in another country and hand them over to the state, is bringing those data – and in respect of those data, the data subjects – within its "jurisdiction" in the sense in which that term is used in the ECHR and in the ICCPR. Such a state must, in this extraterritorial activity, comply with its obligations under those treaties.

## The US Government and the ICCPR

By contrast, the US Government (unlike most other states, and notwithstanding the common view in the international adjudicatory forums) has consistently maintained that "the obligations assumed by a State Party to the International Covenant on Civil and Political Rights (the Covenant) apply only within the territory of the State Party"[95] and that it is therefore not legally required to comply with the ICCPR in relation to its surveillance over non-US communications or Internet activities.

In the context of discussions on the (then draft) UN General Assembly Resolution on privacy in the digital age, submitted in response to the Snowden revelations,[96] a briefing note was leaked that confirms that the USA still believes that it is not under any legal duty to comply with international human rights law outside its own geographical territory. Indeed, it considered this to be a red line that it would not cross. Its very first instruction was that the US negotiators should:[97]

> Clarify that references to privacy rights are referring explicitly to States' obligations under ICCPR and remove suggestion that such obligations apply extra-territorially.

---

94. A brief analysis is at www.huntonprivacyblog.com/uploads/file/Belgian_Yahoo_Case.pdf and the ruling is available at http://jure.juridat.just.fgov.be/view_decision?justel=N-20110118-1&idxc_id=249937&lang=fr (in French, Dutch and German).
95. The USA stated this position in the first, second and third periodic reports under the ICCPR (submitted in 1995 and 2005), in its 2007 Observations regarding the Human Rights Committee's General Comment 31, and again in its fourth periodic report (2011), though the latter acknowledged that its position is at odds with the views of the Human Rights Committee, the International Court of Justice and "positions taken by other States parties" (para. 505). For the documentation relating to the 2011-14 review of the USA, see http://tbinternet.ohchr.org/_layouts/treatybodyexternal/SessionDetails1.aspx?SessionID=625&Lang=en.
96. See the UN General Assembly Resolution on "Privacy in the digital age", adopted without a vote on 18 December 2013.
97. "Right to privacy in the digital age – U.S. redlines", at http://columlynch.tumblr.com/post/67588682409/right-to-privacy-in-the-digital-age-u-s.

The Human Rights Committee firmly rejected this position in its Concluding Observations on the 4th USA report, listing the issue first under the heading "Principal matters of concern and recommendations":[98]

> **Applicability of the Covenant at national level**
> The Committee regrets that the State party continues to maintain the position that the Covenant does not apply with respect to individuals under its jurisdiction, but outside its territory, despite the interpretation to the contrary of Article 2, paragraph 1, supported by the Committee's established jurisprudence, the jurisprudence of the International Court of Justice and State practice. The Committee further notes that the State party has only limited avenues to ensure that state and local governments respect and implement the Covenant, and that its provisions have been declared to be non-self-executing at the time of ratification. Taken together, these elements considerably limit the legal reach and practical relevance of the Covenant (Art. 2).
>
> **The State party should:**
> **(a) Interpret the Covenant in good faith, in accordance with the ordinary meaning to be given to its terms in their context, including subsequent practice, and in the light of the object and purpose of the Covenant, and review its legal position so as to acknowledge the extraterritorial application of the Covenant under certain circumstances, as outlined, *inter alia*, in the Committee's general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant;**
> (original emphasis in bold)

The Committee added a little later, under the heading "National Security Agency surveillance":

> **The State party should:**
> **(a) take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including Article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of the individuals whose communications are under direct surveillance;**
> (original emphasis in bold)

The US Government's view, that the USA's obligations under the ICCPR do not apply to any extraterritorial activities of US agents or agencies, is incompatible with the modern approach to human rights as pertaining to everyone, irrespective of who or where they are, and with the view that states must comply with their international human rights obligations whenever and wherever they are exercising their sovereign powers. In view of the predominance of the USA (and of US corporations that are subject to that country's jurisdiction) in the digital environment, this poses a serious threat to the rule of law in that new environment.

---

98. Human Rights Committee Concluding Observations on the 4th USA report (CCPR/C/USA/CO/4, March 2014), para. 4 (p. 2), available at: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4&Lang=en.

### 3.4.2. The difficulty of competing, conflicting laws applying simultaneously to online activities, with particular reference to freedom of expression[99]

There is a further issue relating to sovereignty and jurisdiction, relevant to the new digital environment. This is the question of when a state can or should – or should not – apply its substantive domestic law to the activities of individuals who are not nationals of that state and who live outside its territory. The issue arises in particular in relation to freedom of expression and predictability of "law". The challenge, in a broadly borderless global online environment, is to ensure that laws are implemented as closely as possible to the actual infringement.

The first point to recall here is that, as a result of the "margin of appreciation" doctrine,[100] there can be significant differences even between Council of Europe member states as to what acts, and in particular what forms of expression, are lawful or unlawful. A statement that is defamatory or held to constitute "support for terrorism", or a book, picture or video that is considered obscene and illegal in one country, may be perfectly legal in another – with neither country being in breach of the ECHR. Some states – including some Council of Europe member states – are much stricter than others with regard to expressions "glorifying jihadism" or "separatism", or "supporting terrorism", or denying the Holocaust, or infringing privacy, or insulting a head of state. Any measure implemented with transborder effect while relying on a "margin of appreciation" will collide with the freedom of expression and legal certainty of individuals in the second country whose rights are thereby restricted and, indeed, with the opposing "margin of appreciation" of the second country.

This raises the question of what states may do about statements, books, pictures or videos that are put online in a country where they are legal, by a resident of that country, but that can be accessed in another country where they are illegal.

#### The Handyside case

One only needs to transpose the facts in the famous Handyside case[101] to the current context to see the problem. In that case, the so-called Little Red Schoolbook, released in various formats in different translations in many European countries and not held to be unlawful anywhere else, was held to be obscene and unlawful under English law, with the publisher of the British version convicted of a criminal offence; the unsold copies of that version of the book were seized and destroyed. In

99. This section focuses on jurisdictional issues relating to freedom of expression on the Internet, and elaborates the discussion in Douwe Korff and Ian Brown, "Social media and human rights", chapter 6 in *Human rights and a changing media landscape* (Council of Europe 2011), available at www.coe.int/t/commissioner/source/prems/MediaLandscape2011.pdf, pp. 175-208, particularly pp. 195-9. The specific problems of competing and conflicting jurisdictions relating to cybercrime are discussed in section 4.5.2, below, with reference also to the important study for the Council of Europe by Prof. Kaspersen on that issue (see n. 217).
100. The "margin of appreciation" doctrine is discussed in section 3.2.3, above.
101. *Handyside v. the UK*, Application no. 5493/72, judgment of 7 December 1976, cited in n. 64.

the subsequent case in Strasbourg, the European Court of Human Rights famously ruled *in abstracto* that the right to freedom of expression includes the right to "shock, offend or disturb" – but then held that, in spite of this, and given that states deserved a wide "margin of appreciation" in respect of obscenity, *in concreto* there had been no violation of the Convention: the English courts could rule the book to be obscene, even if it was not regarded as obscene in any other European country (nor in Scotland, or even in Northern Ireland).

If a book were to be published now, online, in e-book format, in a jurisdiction in which it were to be a perfectly legal publication, but banned in another jurisdiction, the courts in the latter jurisdiction might well issue injunctions ordering their domestic ISPs to block the dissemination of the e-book to web users in that country, and indeed could convict the author and/or publisher of the book for breaching its domestic law (on say, obscenity, or incitement, or defamation). Under the Handyside approach of the Strasbourg Court, the ban and conviction in one country could be in accordance with the Convention, even though no such ban was imposed on the book anywhere else in Europe, or anywhere else in the world. This is far from a theoretical or abstract issue. For instance, the law in the USA is much more tolerant (under the First Amendment to its Constitution) of freedom of expression than are the laws of many European countries.

## The Perrin case

There has been one case before the Court that more or less follows this scenario, and it raises more questions than it gives answers, but might still hold a kernel of a solution. The case of *Perrin v. the United Kingdom*[102] concerned the conviction by a UK court of the applicant, who was French but lived in the UK, for the publishing of material on a US-based website by a US-registered company of which the applicant was a majority shareholder. The UK courts asserted jurisdiction on the basis that the website could be accessed from the UK, and held the contents of the website to breach UK obscenity laws, even though apparently there was no dispute that the website complied with all the local (Californian) laws in the USA. At the start of his criminal trial, the applicant entered an admission, through his counsel, that he was legally responsible for the publication of the web pages. The sole issue for the jury was whether those pages were obscene within the meaning of section 2 of the 1959 Obscene Publications Act (the act under which Handyside had been convicted).

On appeal, the applicant had argued, *inter alia*, that English courts should only be able to convict when the major steps towards publication took place within their jurisdiction.[103] On this point, the UK Court of Appeal ruled that this proposition

102. *Perrin v. the United Kingdom*, Application no. 5446/03, inadmissibility decision of 18 October 2005. This is one of a number of cases listed in a European Court of Human Rights Factsheet on New technologies (October 2013) at: http://echr.coe.int/Documents/FS_New_technologies_ENG.pdf.

103. We are not discussing here the issue of whether the Obscene Publications Act is sufficiently clear to be regarded as "law" in terms of the Convention, nor whether the applicant's conviction was disproportionate.

would undermine the aim of the UK law by encouraging publishers to take the steps towards publication in countries where they were unlikely to be prosecuted. It added:

> There is, as [counsel for the applicant] submits, difficulty with the worldwide web, but it is through the worldwide web that people are able to make very substantial profits.[104]

The "difficulty" was not otherwise addressed. Before the European Court of Human Rights, the applicant submitted the same arguments about "major steps" in the UK being required to bring the case within the jurisdiction of the UK courts.[105] The Strasbourg Court dismissed this argument in the following terms:

> In the present case, the Court notes that the applicant was a resident of the United Kingdom. As a result, he cannot argue that the laws of the United Kingdom were not reasonably accessible to him. Moreover, he was carrying on a professional activity with his Internet site and could therefore be reasonably expected to have proceeded with a high degree of caution when pursuing his occupation and to take legal advice.[106]

In this, the Court referred to the case of *Chauvy and Others v. France*,[107] in which it had held, *inter alia*, that as professional book publishers at least two of the applicants, a publisher and a publishing company, "must at least have been familiar with the legislation and settled case law that was applicable in this sphere and could have sought advice from specialist counsel."[108] However, that case concerned a hard-copy, offline publication, in France, by French applicants, without any international or transnational ramifications.

It is regrettable that the Court did not more directly address the crucial jurisdiction issue in the Perrin case, and accepted the applicability of UK law to the applicant without detailed reasoning. It may have been that the Court felt that the use by Perrin of a US company was mainly a device to bypass UK obscenity law. However, by so simply dismissing the jurisdictional point, the Court missed an opportunity to clarify the application of the ECHR to Internet publications. Specifically, it failed to seriously examine the closeness or otherwise of the link between the applicant, the US company and the UK, in terms of visitors to the website, for example.

As it stands, all one can do is note the emphasis which the Court placed on the fact that the applicant was a resident of the UK. This could suggest that the Court might have ruled differently if the applicant had lived in France (his country of nationality), or if the website had been an entirely US enterprise, operating from California and managed and run by US nationals only. Similarly, one could ask whether the UK courts would have taken a different view in such circumstances. Would they have prosecuted a senior officer (say, the CEO) of the US company if he happened to visit the UK? If they had, under UK law as it stands, the US CEO would in all likelihood have been convicted too.

---

104. *Perrin* v. *the United Kingdom* (see n. 102), p. 3.
105. Ibid., p. 5.
106. Ibid., p. 6.
107. *Chauvy and Others v. France*, Application no. 64915/01, judgment of 29 June 2004.
108. Ibid., para. 48.

If that case had reached Strasbourg, would the European Court of Human Rights there have held that CEOs of US online publishers "carrying out a professional activity with [their] Internet sites" could be "reasonably expected" to have checked the law – any domestic law – that might be ruled to be applicable?

There is no evidence in the Perrin case that the UK courts ordered the taking down or blocking of Perrin's US company's website. But of course the conviction of Perrin meant that the material on the website was illegal under UK (or at least English) law, and if UK ISPs knew this, or were told about it, yet failed to block access to the site, they might be (in fact, probably would have been) held responsible for knowingly facilitating access to illegal materials (although they could have submitted the counter-argument that the blocking technologies available would have been ineffective, see below).

## The Yahoo! case

Similar issues were raised in the well-known French Yahoo! case, referred to earlier, in which a French court ordered the US company to block access by identifiably French users to sales of Nazi memorabilia on its US-based auction site. In that case, Yahoo! argued, *inter alia*, that "a coercive measure instituted against it [by French courts] could have no application in the United States given that it would be in contravention of the First Amendment of the United States Constitution which guarantees freedom of opinion and expression to every citizen." But the order was imposed nevertheless. The case was not taken to the European Court of Human Rights, and the US courts have refused to deal with the issues of principle involved. Following advice from a committee of experts, the French court ruled that individuals with a French IP address should be prohibited from accessing the Nazi memorabilia auctions, even though this measure was recognised by the court as being easy to bypass.[109] The experts guessed that – without any efforts by users to circumvent the measures – about 90% of visits of French individuals could be blocked.[110]

Ultimately, the French court's rather messy compromise was made redundant by an agreement between Yahoo! and the plaintiffs in the case, whereby Yahoo! changed its terms of service to completely prohibit the sale of the content in question on their platforms. This point is very important: whereas it was always completely out of the question that a US court would impose such a ban, Yahoo! was put in a position by the ruling of a foreign court in a foreign jurisdiction that led it to decide "voluntarily"

---

109. Yaman Akdeniz, "Case analysis of *League Against racism and Antisemitism (LICRA), French Union of Jewish Students v. Yahoo! Inc. (USA), Yahoo France*, Tribunal de Grande Instance de Paris (County Court of Paris), Interim Court Order, 20 November, 2000", *Electronic Business Law Reports* 1(3) (2001) 110-20. As this case summary notes: "The French approach … is similar to the German approach in which Compuserve was found liable under German criminal law for the distribution of illegal content over the Internet (mainly child pornography). The [German] decision came despite the efforts of the Prosecution who agreed with the defence that 'it was technically impossible to filter out all such material' over the Internet." Local court (*Amtsgericht*) Munich, English version of the case at: www.cyber-rights.org/isps/somm-dec.htm. See also Juan Carlos Perez, "[US] Court throws out Yahoo appeal in Nazi memorabilia case", 12 January 2006, infoworld.
110. Out-law.com, "Yahoo! Ordered to block French users from Nazi auctions". November 2002. Available at www.out-law.com/page-1179.

to impose a ban on US citizens using its US-based services to buy and/or sell Nazi memorabilia, a ban that US courts could most probably not have imposed.

## The problem of conflicting jurisdictions

This jurisdictional issue is a central one in relation to freedom of expression and communication, and thus to political activism, online. It can no longer be dismissed as a mere "difficulty": it is a core problem. As a legal note put it a decade ago:[111]

> [German courts have] gone so far as to say that any website accessible from Germany is subject to German law. If this principle were to govern in all countries with Internet access, the implication is that websites would be subject to the laws of every country. This would leave Internet governance to an uncoordinated, anarchic set of laws fraught with contradictions and uncertainties.
> … In the case of Nazi memorabilia, only a handful will protest the removal of such unpopular content. But will it be acceptable if China outlaws Falun Gong sites that are legal in France? What about a US ban on offshore gambling sites? A Russian ban on a Chechen rebel web page?
> If every country is allowed to place restrictions on Internet content and levy fines on companies for non-compliance, the legal infrastructure that the Internet is built upon will crumble under the weight of unlimited and unsolvable conflict. On the other hand, if countries are unable to regulate the content of the Internet, cyberspace can undermine the fragile social compromises reflected in the domestic constitutions and statutes like those governing pro-Nazi media in France and Germany. The challenge in establishing a governance system for the Internet lies in determining when a foreign court can make a valid, binding ruling over an Internet company and when it cannot. The conflicts surrounding the Yahoo case foreshadow the difficulties ahead.

The dilemma so neatly put in the latter paragraph remains unresolved. Guidance on the issue is now urgently required. It could come from the European Court of Human Rights or could be provided through the adoption of guidelines at Committee of Ministers level, or even a treaty. The issue at stake is not the right of governments to take actions that comply with international law and that are necessary and proportionate in a democratic society. Within these limits, governments remain free to make decisions on regulation within their jurisdiction. The issue is the ability and right of national governments or courts to take measures that have the effect of imposing restrictions in third countries where the individuals in question are acting in accordance with laws of their own country of residence which, unlike foreign laws, should be known (or "knowable") to them and foreseeable in their application.

Given the crucial importance of the Internet today, and the need to preserve its openness, neutrality and limited regulation (all principles strongly supported by the Council of Europe),[112] the national-state-friendly approach of the Strasbourg Court,

---

111. Tim Fitzpatrick, "Establishing personal jurisdiction in cyberspace: can anyone govern Yahoo?", *UCLA Journal of Law and Technology* (2001) Notes 1, at www.lawtechjournal.com/notes/2001/01_010417_fitzpatrick.php.

112. See in particular the Declaration by the Committee of Ministers on Internet governance principles, adopted by the Council of Europe Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies, para. 1; and Council of Europe Recomendation CM/Rec(2007)6.

implicit in its "margin of appreciation" doctrine, cannot be retained without modification in this context: it leads inevitably to the imposition of the kinds of "unlimited and unsolvable conflict[s]" which Fitzpatrick rightly said would destroy the Internet. In an age of global communication and information exchanges, states should no longer be given a "margin of appreciation" that is so broad that it undermines legal certainty outside its jurisdiction.

That is not to say that there are easy solutions. But the pretence that states can stop the sea of information at their virtual borders by court order is unsustainable. German courts may well feel that Germans should not download *Mein Kampf*, but in that case the law should be directed at those in Germany who download it. Measures, such as obligations on intermediaries, are often proposed and enacted by individual countries, but little if any effort is made to investigate whether or not the measures are actually effective (and, consequently, proportionate and legal). Often, as in the Yahoo! France case, the obligations are complex and burdensome, leading the intermediaries to "voluntarily" take more restrictive measures for the sake of legal certainty or cost.

Perrin's conviction could be more easily accepted as compatible with the Convention if the Court had required the respondent government to show that he had personal, primary responsibility for the materials on the US website of the US company of which he was a major shareholder, that that website specifically targeted or clearly attracted UK visitors in significant numbers and that no measures were in place to dissuade UK visitors from entering the site, for instance, a warning on the lines of:

> The materials on this website comply with [relevant US/Californian] law. If you are not a US visitor, accessing the materials on this website may be unlawful under your national law. Do not visit this website if this is the case.

If materials are unlawful under international law – child abuse images,[113] incitement to racial hatred and so on – all states should take action against all those involved in it, and should co-operate in doing so, particularly when human dignity or safety is at stake. However, if material is unlawful in one country but not in others, states should exercise great restraint in imposing their own domestic standards on information disseminated from foreign websites, unless there is a clear and close nexus between the material or the disseminator and the country considering whether to assume jurisdiction. Clear guidelines and legal rules are urgently required.

The issue of competing – and conflicting – application of different national laws to Internet material and Internet activity is an issue that needs to be addressed urgently to guarantee the rule of law on the Internet. In principle, individuals and companies that make information available from their country of residence or establishment should have to comply only with the laws of that country, whereas individuals who access or download materials from foreign websites when they could and should know that the materials are illegal in their country of residence can be expected

113. Even here there are limits. The Cybercrime Convention's provisions on "apparently" illegal material are in line with the EU approach, but not in line with the US approach. Similarly and more importantly, the optional exception (created in the convention) for procurement and possession of illegal child abuse materials generates the potential for further disharmony of approaches.

to adhere to the laws of the latter country. States should in principle only exercise jurisdiction over foreign materials that are not illegal under international law in limited circumstances, notably when there is a clear and close nexus between the materials and/or the disseminator and the state taking action. They should respect the right of other states to draw the lines on freedom of expression differently from themselves, within the limits of international human rights law. However, further guidance on this issue, starting from this proposed principle, and spelling out any proposed exceptions to this principle, is urgently needed.

## The protection of conflicting rights

The issue of jurisdiction partly overlaps with a second set of questions, namely how to deal with ensuring adequate protection when rights are in conflict. This can be seen in the recent European Court of Justice case C-131/12 involving Google and Spain, somewhat misleadingly known as the "right to be forgotten" case.[114] Both sides in the case had legitimate human rights arguments. The plaintiff felt that the processing of his personal data by Google, leading to searches for his name producing prejudicial results, was unfair and that he should have the right to object. Google, on the other hand, felt that there should be no restrictions imposed on the results of searches performed through the service and that any such restrictions would amount to a restriction on freedom of communication.

The European Court of Justice (CJEU) characterised the initial complaint as follows:

> [W]hen an internet user entered Mr Costeja González's name in the search engine of the Google group ("Google Search"), he would obtain links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts. (§14)

However, the specific question referred by the Spanish court was significantly more restrictive. Namely:

> may the [AEPD, the Spanish data-protection authority], protecting the rights embodied in [Article] 12(b) and [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, directly impose on [Google Search] a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located? (§20)

There is a crucial difference here. The complainant's request is significantly narrower than that of the referring court. The plaintiff asked for searches based on his name to be dissociated from a particular prejudicial result being produced by Google. The Spanish court asked whether there is a considerably more far-reaching right, namely

114. *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, case C-131/12, 13 May 2014. For a discussion of the link between the "right to be forgotten" as clarified in this case and the question of jurisdiction, see: www.ejiltalk.org/the-territorial-reach-of-the-eus-right-to-be-forgotten-think-locally-but-act-globally/.

to require a de-indexing of the page in question, meaning that it would no longer be findable by Google, regardless of the search term used.

The response from the CJEU is exemplary on one level. Its ruling focuses entirely on the least restrictive alternative, concluding that unfair, prejudicial search results based on an individual's name may be removed. In that way, the obligation placed on Google has the smallest possible effect on freedom of communication online while achieving the clearly proportionate goal of removing unfair and prejudicial search results, when these are based on an individual's name.

However, the CJEU then left it entirely up to Google to process and adjudicate on any complaints that it received from users, despite the fact that the court had acknowledged a fluid set of criteria for assessing such complaints and a potential undermining of the right of the public to have access to certain information. This created a legal environment where Google had a clear incentive to react positively to complaints and little or no counterbalancing incentive (or guidance from the court to decide how, if and when) to turn down complaints. The result, one could argue, was to create a restriction on freedom of communication that is not in line with the obligations of the ICCPR, the Convention on Human Rights and the Charter of Fundamental Rights of the European Union.

Indeed, in the weeks following the ruling, Google told journalists that it had not only completely de-indexed some content (in excess of the CJEU's demands), but it had also chosen to de-index some other content, an action which appears to completely ignore the (very limited) guidance of the CJEU on maintaining searches that have a public interest element.[115] The basic problem is that the CJEU imposed a liability on Google for not acting in relevant cases, but left Google free to over-implement the decision by as much or as little as it chose, for its own business interests. This resulted in the creation of a non-law-based restriction on information that is in the public interest, despite the fact that the need to retain such access had been specifically mentioned in the Court ruling.

## 3.5. Human rights and private entities[116]

### 3.5.1. Human rights law, the Ruggie Principles and Council of Europe and other guidance

International human rights law essentially applies only to states, and to actions or omissions of public authorities. Sometimes it can be given what is (somewhat

115. Andrew Orlowski, "Google de-listing of BBC article 'broke UK and Euro public interest laws' – so WHY do it?", 4 July 2014. Available at www.theregister.co.uk/2014/07/04/google_peston_bbc_delisting_not_compliant_w_public_interest_law_says_expert/. See also: www.bbc.com/news/business-28130581.

116. This section in part draws on Ian Brown and Douwe Korff, *Digital freedoms in international law*, Global Network Initiative (GNI), 2012, available at https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf. See also the recent EDRi booklet, "Human rights and privatised law enforcement: Abandoning rights – abandoning democracy – abandoning law", EDRi, February 2014, at http://edri.org/wp-content/uploads/2014/02/EDRi_HumanRights_and_PrivLaw_web.pdf.

mistakenly) referred to as "horizontal effect" (*Drittwirkung*) by being applied indirectly to actions or omissions of private actors; even then, the relevant obligations still rest on the state. The state is, in such cases, held responsible for the fact that it did not control the actions of the relevant private actors that impinged on the human rights of individuals. Individual victims cannot invoke international law rules against private parties.[117]

The recent Council of Europe "Guide to human rights for Internet users"[118] suggests that states have an obligation to ensure that any "general terms and conditions" of private-sector entities that are not in accordance with international human rights standards must be held null and void in the domestic legal systems of Council of Europe member states.[119] The guide also endorses the UN Ruggie Principles, discussed below.[120]

The non-applicability (or, at most, indirect applicability) of international human rights law to private entities is problematic in the context of the issues addressed in this paper, particularly in relation to use of the Internet and mobile technology. As already noted, the relevant technologies are mainly managed by private-sector entities, and some of the human rights violations in the new digital environment have their origin in demands by governments that those private-sector entities co-operate with them in law enforcement, national security or anti-terrorist measures (or at least measures claimed to be for those purposes). In addition, the private entities controlling the Internet and wider digital environment are increasingly subjected to demands from other private entities to assist the latter in asserting their civil-legal rights, especially intellectual property rights. We discuss these issues in the next sections.

Here it is important to note that new international standards are emerging that are intended to be applied by companies. The most important are the Ruggie Principles: the UN "Guiding Principles on Business and Human Rights", drafted by the United Nations Secretary-General's Special Representative for Business and Human Rights, Professor John Ruggie.[121] However, the Ruggie Principles still

---

117. See *Harris, O'Boyle and Warbrick, Law of the European Convention on Human Rights*, 2nd edn (2009), chapter 1, section 5, "Negative and positive obligations and *Drittwirkung*", particularly pp. 19-21. Note also the "Multistakeholder Statement" of NETmundial (formerly the Global Multistakeholder Meeting on the Future of the Internet Governance) of 24 April 2014, which stresses, *inter alia*, that "Governments have primary, legal and political accountability for the protection of human rights" (Internet Governance Process Principles, under the heading "*Accountable*"), available at: http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

118. Guide to human rights for Internet users, contained in an Appendix to Recommendation of the Council of Europe's Council of Ministers CM/Rec(2014)6 of 16 April 2014, available at: https://wcd.coe.int/ViewDoc.jsp?id=2184807.

119. See para. 2 of Recommendation CM/Rec(2014)6, which stipulates that: "The obligations of States to respect, protect and promote human rights include the oversight of private companies. Human rights, which are universal and indivisible, and related standards, prevail over the general terms and conditions imposed on Internet users by any private sector actor."

120. See para. 5.5 of Recommendation CM/Rec(2014)6.

121. Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises: John Ruggie, "Guiding principles on business and human rights: implementing the United Nations 'Protect, Respect and Remedy' Framework", UN Human Rights Council Document A/HRC/17/31, 21 March 2011, at www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

mainly focus on the duty of "host" states to take measures against human rights violations by companies. They do not deal in detail with the converse situation, where states make demands of companies that would lead companies into violations of international human rights law. However, the Special Rapporteur does suggest that:[122]

> The responsibility to respect human rights is a global standard of expected conduct for all business enterprises wherever they operate. It exists independently of states' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations. And it exists over and above compliance with national laws and regulations protecting human rights.

In other words, in principle, companies faced with state demands and laws that violate human rights should refuse to do so where they can, and minimise the extent of any such co-operation to the least possible in the circumstances. However, if a state either does not respect or actively circumvents its international legal obligations, there is little other than moral rectitude or public relations pressure that can create incentives for online intermediaries to defend human rights.[123]

The UN Special Representative also refers, in several instances, to the possibility of a company becoming complicit in human rights violations by "other entities" – but those principles appear to be dealing only with situations in which those other entities are other companies, and in particular other companies with which the company has business relationships.

Finally, we should mention the ongoing work in the Steering Committee for Human Rights (CDDH) of the Council of Europe on the elaboration of instruments on "business and human rights" – though it should be noted that, at least for now, this work is aiming only at non-binding instruments in this area.[124]

It seems important that further guidance be developed, by the Council of Europe and others, on the responsibilities of business enterprises that are faced with (or that put themselves in a situation where they may well face) demands from governments, or from other private entities, to support measures by those governments or entities that may violate international human rights law. Such guidance could include a recommendation that a legal duty be imposed on companies to undertake a human rights risk assessment before entering certain countries, and the imposition of civil or (in extreme cases) criminal liabilities on companies that fail to take their responsibilities in this respect seriously, as was proposed in a report by the Global Network Initiative.[125]

---

122. Ibid., Part II, The corporate responsibility to respect human rights, para. 11 (commentary on the first "foundational principle").
123. See Section 4.3 below for more analysis, particularly of the Council of Europe report on ICANN.
124. See the report on the Steering Committee meeting of 14 February 2014, at: www.coe.int/t/dghl/standardsetting/hrpolicy/Other_Committees/HR_and_Business/Documents/Web_CDDH-CORP(2014)R2_en.pdf.
125. Brown and Korff, *Digital freedoms in international law* (see n. 116).

### 3.5.2. Filtering and blocking by Internet and e-communications companies on the instructions of – or on the basis of "encouragement" by – states[126]

#### The trends

Apart from criminalising material on the Internet *ex post facto*, that is, after material produced in another country has been published,[127] states are also increasingly trying to prevent or block access to certain material and information online. Such blocking (or filtering) is performed by software or hardware that reviews communications and decides on the basis of pre-set criteria whether to prevent the material from being forwarded to an intended recipient, such as someone browsing the Internet.[128]

No one will be surprised that repressive states try to block access to opposition websites and theocratic regimes try to block websites they deem to be blasphemous. But even states supposedly respectful of the rule of law – including Council of Europe member states – are increasingly trying to block access to material they regard as unacceptable. Or, in a more nebulous and less accountable framework, they "encourage" the gatekeepers to the Internet (ISPs and MNOs) to do this "voluntarily", outside a clear public-law legal framework.

Usually, in democratic countries, such measures have, at least officially and initially, been mainly aimed at strongly legitimate targets: racist or religious hate speech, or child pornography,[129] but the systems suffer from major flaws in the way they work.

First, blocking is inherently likely to produce unintentional false positives (blocking sites with no prohibited material) and false negatives (when sites with prohibited material slip through the filter). From the point of view of freedom of expression, the most problematic is widespread over-blocking: the blocking of access to sites that are not in any way illegal, even by the standards supposedly applied.[130]

- For example, an Internet filtering law in Pennsylvania, introduced to counter child pornography, was struck down in 2004 partly because blocking

126. For a detailed discussion: C. Callanan et al., "Internet blocking: balancing cybercrime responses in democratic societies", Aconite/OSI 2009, at: www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf and summary at www.aconite.com/sites/default/files/Internet_Blocking_and_Democracy_Exec_Summary.pdf. Blocking activities of some states have been extensively analysed, for example, in Ian Brown, "Internet filtering – be careful what you ask for" in S. Kirca and L. Hanson (eds), *Freedom and prejudice: approaches to media and culture*, Bahcesehir University Press, Istanbul, 2008, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1026597.
127. See section 3.4.2, above.
128. For a brief description of filtering methods (by DNS, IP or URL) and their relative (in)effectiveness, see *CDT v. Pappert*, 337 F.Supp.2d 606, section E, paras. 108-43, at www.yale.edu/lawweb/jbalkin/telecom/cdtvpappert.pdf.
129. We use this term here because it is short and used in the Cybercrime Convention (Article 9). However, it is increasingly felt that the term "child sexual abuse images" is more appropriate.
130. See Callanan et al., "Internet blocking", Aconite/OSI 2009 (n. 126 above), Executive Summary, pp. 18-19, with a useful chart on p. 17, indicating the characteristics of the various blocking strategies discussed; the likelihood of over- and under-blocking; the resources and maintenance effort required for each; and the intrusiveness in terms of deep packet inspection (DPI) requirements.

supposedly targeted at 400 sites had in fact prevented access to almost 1.2 million other sites.[131]

- In the Yildirim case, discussed below, the European Court of Human Rights found that Turkey, in trying to stop access to one Google site (Google Sites is a web-hosting service) with content that allegedly insulted the founder of the state, Kemal Atatürk, had blocked access to all (tens of thousands of) Google Sites, including the site of the applicant, who used this to disseminate his academic – and in no way illegal – publications.

Second, the criteria for blocking certain websites, but not others, and the lists of blocked websites are very often opaque at best, secret at worst:[132]

> In all the countries studied, Freedom House found arbitrariness and opacity surrounding decisions to block content: "in most non-democratic settings there is little government effort to inform the public what content is censored and why." The authorities often avoid confirming that a website has been blocked and instead remain silent or cite technical problems: "even in more transparent, democratic environments, censorship decisions are often made by private entities and without public discussion, and appeals processes may be onerous, little known, or non-existent".
>
> Thus, no one knows what is on the blocking lists of what Freedom House calls "partially free" Azerbaijan, Georgia, Russia or Turkey. In these and other European countries, the criteria for blocking are totally unclear. The application of blocking is unforeseeable, and effectively unchallengeable.

Third, it is not as if questions of legality and illegality are straightforward, even within one country. In the UK, the law would seem to make it a serious criminal offence for an 18-year-old boy to possess a sexually explicit picture of his 16-year-old girlfriend if she appears to be 15.[133] There are similar issues about bestiality: there are many classical paintings on display in museums the world over of *Leda and the Swan* or *Europa and the Bull* that technically appear to fall foul of the law. Questions of when certain statements or materials on a website can be regarded

---

131. *CDT v. Pappert* (see n. 128 above), para. 189.
132. The quotation, from Ian Brown and Douwe Korff, *Digital freedoms in international law*, GNI 2012 (see n. 116 above), p. 180, refers to S. Kelly and S. Cook (eds), *Freedom on the net 2011: a global assessment of Internet and digital media*, Freedom House, Washington DC 2011, pp. 4-5, at www.freedomhouse.org/sites/default/files/FOTN2011.pdf.
133. Protection of Children Act 1978, section 7: "If the impression conveyed by a [pseudo-]photograph is that the person shown is a child [a person under the age of 16], the [pseudo-]photograph shall be treated for all purposes of this Act as showing a child and so shall a [pseudo-]photograph where the predominant impression conveyed is that the person shown is a child notwithstanding that some of the physical characteristics shown are those of an adult" – see www.legislation.gov.uk/ukpga/1978/37/section/7. This approach is EU-wide since the adoption of Directive 2011/92/EC, whose definitions now cover content that "appears" to be of children, whereas the relevant US legislation permits (in line with the exceptions in Article 9.4 Cybercrime Convention) pornographic material that appears to show minors engaged in sexually explicit conduct, as long as records are kept to prove that the individuals were, in fact, not minors. This means that images on US websites that are demonstrably not child abuse images are defined as child pornography under EU law and criminalised in line with Article 9 of the Cybercrime Convention. For more detail on the US legislation, see www.gpo.gov/fdsys/pkg/BILLS-109hr4472enr/pdf/BILLS-109hr4472enr.pdf.

as constituting "incitement to racial hated", or "promoting jihadism" or Holocaust denial, are similarly notoriously difficult to answer.

Fourth, this makes the issue of notice and remedies crucially important. However, as just noted, Freedom House found, in its extensive study, that all too often "appeals processes may be onerous, little known, or non-existent".[134] This is seriously aggravated if the decision on what to block or not block is – deliberately – left to private entities, as discussed below.

Fifth, blocking measures are easy to bypass, even for not very technically skilled people.[135] As Brown and Korff put it, "this is good news for political activists in repressive countries, but bad news for states, officials and private entities hoping to use blocking to stop dissemination of child abuse images or hate speech".[136] Indeed, people who access the Internet using privacy-enhancing technologies (promoted by the EU and the Council of Europe) may find that it unintentionally results in circumvention of blocking systems.[137]

Finally, blocking is addressing yesterday's problem: commercial pornographic websites are increasingly uninterested in material that causes them problems, while the kind of people who want to access or share the worst kinds of material (in particular child pornography, but also jihadist material) are decreasingly using openly accessible websites. They share their material through peer-to-peer networks, chat rooms, encrypted webspaces, image hosting sites or hacked sites[138] – or even reportedly in online games or virtual spaces. Blocking access to generally accessible (or even paid-for) webpages does not affect them.

### Why blocking is used

Crucially, in particular in relation to child pornography, blocking totally fails to address the actual issue: the abuse of the children in question. Indeed, it would appear that states resorting to blocking schemes tend to do this instead of tackling the actual abuse. As European Digital Rights (EDRi) put it:[139]

> We are morally (and under international law legally) obliged to take all possible action to ensure that the sites are deleted, the victims are identified and rescued, and the criminals involved are prosecuted.

Blocking websites simply does not achieve any of this. As Brown and Korff say:[140]

> A more effective response would be to remove images from the Internet, criminally investigate producers and save children from such situations. Blocking does none of that.

---

134. Kelly and Cook, *Freedom on the net 2011*, Freedom House (see n. 132 above), p. 5.
135. See *CDT v. Pappert* (cited in n. 128 above), paras. 197-203.
136. Brown and Korff, *Digital freedoms in international law* (cited in n. 116), p. 180, with reference to Richard Clayton, "Failures in a hybrid content blocking system", Proceedings of the 5th Workshop on Privacy Enhancing Technologies, Dubrovnik, May 2005, at www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf.
137. Joe McNamee "Internet blocking", EDRi, p. 8, at www.edri.org/files/blocking_booklet.pdf (2010).
138. Ibid.
139. Ibid, p. 6.
140. Brown and Korff, *Digital freedoms in international law* (cited in n. 116), p. 179.

Of course, it is possible to imagine theoretical situations where urgent, targeted, time-limited blocking of content might be useful as a flanking measure. However, available evidence shows blocking is almost never used in this way. Instead, the apparently complete lack of analysis of the effectiveness of blocking measures suggests that usefulness is not a priority criterion. Indeed, at the same time as the European Commission was proposing EU-wide mandatory Internet blocking measures for child abuse images, it also pointed out the ineffectiveness of blocking of YouTube in Turkey.[141]

Indeed, even in their own terms, blocking measures against child pornography are demonstrably much less effective than take-down measures adopted by industry to fight copyright infringements or financial phishing websites.[142]

The above problems are compounded by the fact that states – including states which are generally regarded as long-standing democracies – tend to extend blocking, introduced to combat only the most serious issues such as child pornography and clear incitement of violence and hate speech, to all sorts of other matters that the state disapproves of. Globally, including in Europe, there have been attempts by states to block sites containing not only hate speech and advocacy of terrorism, but also political debate, information on sexual or minority rights, alleged defamation and even the "sacred texts" of Scientology.[143]

Research by the Open Rights Group in the UK suggests that the default filters that the UK Government would like to see installed would block access to the following information (albeit subject to an opt-in):[144]

- pornography;
- violent material;
- extremist and terrorist-related content;
- anorexia and eating-disorder websites;
- suicide-related websites;
- alcohol;
- smoking;
- web forums;
- esoteric material;
- web-blocking circumvention tools.

---

141. Mandatory web blocking was in the Commission's draft Child Exploitation Directive (proposal, 10 March 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0094:FIN:EN:PDF); EU Commissioner Stefan Füle said in August 2010 that "many people in Turkey" were successfully circumventing the block. See www.europarl.europa.eu/sides/getAllAnswers.do?language=EN&reference=E-2010-4620.
142. EDRi booklet on Internet blocking (see n. 137 above), p. 5, referring to Tyler Moore and Richard Clayton, *The impact of incentives on notice and take-down*, Seventh Annual Workshop on Economics and Information Security (WEIS08), Dartmouth NH, 25-28 June 2008, in M. E. Johnson (ed.), *Managing information risk and the economics of security*, Springer, New York, 2008, pp. 119-223.
143. See Ian Brown, "Internet filtering – be careful what you ask for" (see n. 126 above).
144. See https://www.openrightsgroup.org/blog/2013/sleepwalking-into-censorship (2013).

This is of course extremely wide. Moreover, the decision on what constitutes such matters is left to the ISP in question. As the Open Rights Group puts it, these approaches lead us to "sleepwalk into censorship", including supposedly freely chosen self-censorship.

### Blocking decisions by private entities

The matter gets worse if the decision of what sites to block is effectively left to private entities like the UK Internet Watch Foundation (see below), "encouraged" by states but with the states at the same time claiming they bear no responsibility for the blocking.

The problem is that if such a private entity-led system becomes really effective, it leads to a situation in which access to selected websites for the vast majority of the population is determined, not on the basis of public law, but on the basis of decisions by private-law entities that are not directly subject to human rights law. In particular, ISPs can stipulate in their general terms and conditions that they are free to decide, by themselves, whether to block access to specific sites if they deem those sites (at their own discretion) to be contrary to company policies. Rather than (like human rights law) allowing information to be accessible to their users even if it "shocks, offends or disturbs" (to use the words of the European Court of Human Rights),[145] ISPs are more likely to seek to avoid controversy by blocking anything they deem to be controversial. Such over-compliance, as in the Yahoo! France and Google Spain cases described above, therefore also extends to situations where intermediaries are seeking to comply with what they assume that the government – or the press – may demand in the future. Yet their actions are not subject to the kind of judicial review that is available against decisions and actions by public bodies that affect fundamental rights, including the right of access to information of the users of the ISP and the right to impart information of the blocked websites.[146]

Blocking mechanisms are increasingly intrusive using deep packet inspection[147] and automatic picture or video recognition.[148] While these may seem attractive in

145. Cf. *Handyside v. the UK*, Application no. 5493/72, judgment of 7 December 1976, para. 49.

146. As noted in section 3.5.1 above, individuals and webhosts affected by such policies adopted under an ISP's general terms and conditions could at most try to take action against the relevant government for failing to have those terms and conditions ruled null and void – arguing that the state failed to adopt the policy suggested by the Council of Europe Recommendation on the Guide to human rights for Internet users (see nn. 118 and 119). But that is a very tortuous and ineffective way to protect freedom of access to information as a fundamental right.

147. Any file transmitted over the Internet is broken down into packets, which are (re)assembled by the recipient. In order to transmit it, the network "reads" the top layers of the packet – information such as the origin IP address, recipient IP address and data to enable reassembly of the file. Deep packet inspection (DPI) looks more deeply into the packet to read information on its content.

148. Microsoft has developed a photo recognition tool called PhotoDNA while, according to a report in *The Guardian*, "Google has developed a Video ID tool which uses digital fingerprinting technology to identify and block child abuse videos, even if they have been edited and repurposed. Microsoft says it is looking at implementing Video ID on its own video services, and has a similar tool for photos called Photo DNA": www.theguardian.com/technology/2013/nov/18/microsoft-google-summit-halt-child-abuse-images.

the specific context of child pornography, there is a clear danger that – with the "mission creep" of blocking and filtering mechanisms, just noted – they will lead to ever more intrusive surveillance of Internet activities.[149] Not surprisingly, leading experts, including campaigners against child abuse and child pornography, are increasingly rejecting blocking and filtering as an appropriate response to child sexual abuse.[150]

In summary, several different issues arise in this context, depending on whether the blocking is law-based (specifically provided for in domestic law) or non-law-based (implemented by private entities outside any specific domestic legal framework).

### Issues relating to law-based blocking of illegal content

Unquestionably, there is certain content that is a legitimate target for such measures. However, the fact that something is a legitimate target does not mean that it is appropriate to use any means to target it. The first test must surely be whether the means chosen are reasonably effective or, to use the more legally relevant term, suited to achieve the desired result. In order to apply that test, it is crucial to first clearly define the (legitimate) aim of the measure.

However, throughout the legislative process of adopting the EU's child exploitation Directive (2011/93/EC), no effort was made by the European Commission to explain the goal of its mandatory blocking proposal. In particular, it was left unclear whether it was seeking to prevent deliberate access to illegal content, or accidental access to the content. No evidence was produced – for example, from countries that currently use blocking – to show that one or other legitimate aim, or both aims (or a different aim) would be achieved to any appreciable extent.

The EU Directive also did not seek to explain how the block was to be imposed. The range of options is very broad – IP address blocking is cheap, non-intrusive and extremely likely to block unrelated content; domain blocking is cheap, non-intrusive and somewhat less likely to block unrelated content; Cleanfeed[151] (a hybrid system developed by British Telecom) is somewhat more intrusive but very narrowly targeted; deep packet inspection is vastly intrusive and a major restriction on privacy rights, but also the most accurate. However, all of these measures are trivial to circumvent.[152] This is why the target of the blocking is important – if there is no evidence of significant levels of accidental access to the content in question and if deliberate access remains easy, the suitability/proportionality calculation is much more difficult than it first seems.

---

149. This is further addressed in section 3.5.3, below.
150. See Joe McNamee "Internet blocking", EDRi, p. 10, at www.edri.org/files/blocking_booklet.pdf (2010). For a feminist view opposing blocking, see Jane Fae, "Comment: Three embarrassing truths about Cameron's porn filter", 19 December 2013, at www.politics.co.uk/comment-analysis/2013/12/19/comment-three-embarrassing-truths-about-david-cameron-s-porn.
151. See http://wiki.openrightsgroup.org/wiki/Cleanfeed.
152. See http://www.cnet.com/how-to/how-to-use-vpn-to-defeat-deep-packet-inspection/ for example.

## Issues relating to non-law-based blocking of content

Countries like the UK and Sweden have introduced blocking systems based on "voluntary" arrangements with ISPs. All the considerations concerning effectiveness and proportionality noted above remain relevant, but serious questions need to be asked about how far these activities are really voluntary and/or whether they entail state responsibility. The UK's "voluntary" system can be traced back to a letter from Metropolitan Police chief inspector Stephen French stating that

> [w]e trust that with your co-operation and self-regulation it will not be necessary for us to move to an enforcement policy.[153]

UK Government backing greatly increased in 2013 when the minister responsible hosted a summit in Westminster with leading ISPs and web companies, including Google, Facebook, BT, Sky and Virgin Media. As a result of strong encouragement from the government, the main ISPs agreed to contribute a total of £1 million to fund the Internet Watch Foundation (IWF), which operates a child pornography hotline and creates lists of allegedly illegal websites. The IWF, a private body,[154] receives complaints from members of the public and provides a "notice and take-down service to advise ISPs in partnership with the Police Services in the UK to effect … removal [of potentially criminal online content]." In practice this "advice" is seen by almost all UK ISPs as effectively binding, not least because the UK Government strongly demands compliance with IWF "advice" and threatens ISPs that, if they do not "voluntarily" co-operate with the IWF, it will bring in legislation to force them to do so.

The web companies agreed to "report to [the government] within a month on how they will provide technical and expert support for the IWF's new proactive approach." The government, for its part, promised to obtain assurances from the Director of Public Prosecutions to ensure that the IWF could look for illegal materials on the Internet without itself facing prosecution (because such searches technically fall within the criminal law).[155] However, the government continues to insist that the IWF is a purely private entity and that the arrangement between the IWF and the ISPs is a purely "voluntary", private one – which implies that the government feels that it is not responsible for measures taken under the "voluntary" (but strongly government-"encouraged") system.

There are serious doubts as to whether a blocking system that effectively imposes a restriction on most ordinary people's access to online information will ever be in accordance with the rule of law when it is chosen and operated by private parties, in the absence of public scrutiny, in the absence of a democratic debate, in the absence of a predictable legal framework, in the absence of clear goals or targets, in the absence of evidence of effectiveness, necessity and proportionality, and in the absence, either before or after the system is launched, of any assessment of possible counter-productive effects.

---

153. C. J. Davies, "The Hidden Censors of the Internet", *Wired*, 20 May 2009. Available at www.wired.co.uk/magazine/archive/2009/06/features/the-hidden-censors-of-the-internet.
154. See www.iwf.org.uk/. The IWF is a UK "company limited by guarantee". See the UK company register: http://data.companieshouse.gov.uk/doc/company/03426366.html.
155. See: www.telegraph.co.uk/news/politics/10127862/Internet-Watch-Foundation-given-powers-to-police-child-porn.html.

In addition, there is the question whether governments that encourage (or even just allow) such systems can claim not to be responsible for them, or for the restrictions on information that are the practical results of the systems, simply because those systems are not underpinned by law. In terms of international human rights law, states are responsible if, within their jurisdiction, there are systems in place that effectively restrict the freedom to seek, receive and impart information and ideas regardless of borders for most of its inhabitants. The fact that Article 10 of the ECHR only refers to interferences with this right "by public authorities" does not mean that the state can simply wash its hands of measures by private entities that have such effect – especially not if the state *de facto* strongly encouraged those measures. In such circumstances, the state is responsible for not placing such a system on a legislative basis: without such a basis, the restrictions are not based on "law".

## The law

In the case of Yildirim, already mentioned,[156] the European Court of Human Rights has clearly noted the dangers of indiscriminate blocking.

In June 2009, a Turkish court ordered the blocking of a Google site that was regarded as disrespectful of the country's founder, Kemal Atatürk, but the public authority in charge of implementing the ban found that it could not do so except by blocking access to all websites hosted by Google Sites from Turkey, and the courts endorsed that arrangement. The applicant, Mr Ahmet Yildirim, had a different Google site from the one suspected of containing the offending material, on which he published academic work that was not in any way illegal. He sought to have the broad blocking measures lifted, or at least limited, but the Turkish courts rejected his request.

In its judgment in the case, the European Court of Human Rights ruled that the Turkish law in question failed to ensure that the Turkish courts would weigh up the various interests at stake. In particular, the law:[157]

> did not lay down any obligation for the domestic courts to examine whether the wholesale blocking of Google Sites was necessary, having regard to the criteria established and applied by the Court under Article 10 of the Convention. Such an obligation, however, flows directly from the Convention and from the case-law of the Convention institutions. In reaching their decision, the courts simply found it established that the only means of blocking access to the offending website in accordance with the order made to that effect was to block all access to Google Sites … However, in the Court's view, they should have taken into consideration, among other elements, the fact that such a measure, by rendering large quantities of information inaccessible, substantially restricted the rights of Internet users and had a significant collateral effect. …
>
> The Court further observes that the measure in question produced arbitrary effects and could not be said to have been aimed solely at blocking access to the offending website, since it consisted in the wholesale blocking of all the sites hosted by Google Sites. Furthermore, the judicial review procedures concerning the blocking of Internet sites are insufficient to meet the criteria for avoiding

156. For details, see note 3 above.

157. Yildirim judgment (see n. 3), paras. 66, 68 and 69, cross-reference omitted.

> abuse, as domestic law does not provide for any safeguards to ensure that a blocking order in respect of a specific site is not used as a means of blocking access in general.
> Accordingly, there has been a violation of Article 10 of the Convention.

The opening sentences of the above citation are worthy of note with regard to "voluntary" measures that have been introduced as a direct or indirect result of state pressure. The obligations mentioned by the Court do not suddenly disappear because the state in question has avoided using a legal framework.

The European Commission takes the opposite view, however. It argued, in a letter to EDRi, that state responsibility under the EU Charter is not (and apparently cannot be) triggered by voluntary measures, even with regard to "support for such actions by Member States".[158]

The final sentences of the above quotation are also important – a voluntary system, almost by definition "does not provide any safeguards to ensure that a blocking order in respect of a specific site is not used as a means of blocking access in general".

More generally, as EDRi points out, measures that have an impact on fundamental rights, more specifically blocking and filtering of Internet sites, cannot ever be said to be "necessary" and "proportionate" to a "legitimate aim" in a "democratic society" if they are unsuited to achieve that aim, excessive in their effect and lacking in procedural safeguards.[159] This applies manifestly to the measures described above, which (i) do not stop either sexual abuse of children or even the sharing of images of such abuse (or other targeted material, such as "jihadist propaganda") between paedophiles or other criminals; (ii) do stop access by the large majority of the population to sites that are in no way illegal; (iii) are based on opaque or even secret criteria or lists that clearly do not have the quality of a "law" in the ECHR sense; and (iv) are not subject to adequate and appropriate systems of appeal and remedy. All of this applies a fortiori if the measures are imposed by private entities (with the "encouragement" of the state) and are adopted by such a wide range of ISPs and MNOs that ordinary citizens who are not specifically trying to avoid the blocks will not get access to either the rightly blocked sites (which is not a problem) or the wrongly blocked sites. This harms the rights to freedom of expression and information both of those whose sites are wrongly blocked and of those who are effectively missing out on what may well be relevant, or even important, information (for instance, on sexual or gender problems or sexual health).

### 3.5.3. Indiscriminate deep packet inspection (DPI) by companies under court orders issued at the request of other companies, to enforce copyright

#### The trends

Intellectual property rights holders are increasingly asking for filters or blocks similar to those described in section 3.5.2 to be imposed on sites that allegedly facilitate

158. See http://edri.org/files/priebe_response.pdf.
159. EDRi booklet, "Internet blocking" (see n. 137 above), *passim*.

the sharing of illegally copied ("pirated") content, and are increasingly demanding access to Internet users' details in relation to such alleged sharing, by means including the compulsory use of DPI by ISPs to detect probable or possible rights infringers.[160]

The intrusiveness comes from the technology itself. DPI requires the "inspector" to examine not just the broad metadata on the origin or destination of the "packet", but also the content of those communications. "Packets" are singled out on the basis of a pattern or algorithm linked to specific content. For the intellectual property rights holders, that will be the particular markers of a particular copyright-protected video or photograph. But the same technology allows for searches of essentially anything: a certain political speech, a certain revolutionary song, a trade union banner.

Such demands are typically made in private legal (civil law) procedures, in which rights holders seek court orders requiring ISPs (and in future undoubtedly also MNOs) to use such technologies to this effect. The main feature of such measures is that they require intrusive surveillance of all users of an ISP (or mobile phone network), with the aim of trying to identify the few that are probably (or possibly) infringing copyright. It is important to note the latter: the technologies cannot determine with full certainty whether the passing on of an item – even an item (or a part or snippet of an item) that is identified as copyright-protected – is lawful or not: that may depend on whether any exemptions apply to the right, such as exemptions for visually-impaired people or exemptions relating to parody or education.

This clearly raises serious issues of necessity and proportionality: the measure is very intrusive, yet inconclusive, and it affects many more innocent people than guilty ones. It also suffers from inherent (and statistically unavoidable) false positive and false negative results.

## The law

There are, as yet, few national and even fewer international court rulings on such issues.[161] However, both the European Court of Human Rights and the Court of Justice of the European Union (CJEU) have issued important judgments that are relevant to the issue.

First of all, as the European Court of Human Rights noted in Yildirim, the CJEU has given important guidance on the matter in its Sabam ruling. To use the summary of the Strasbourg Court:[162]

> Case C-70/10, examined by the Court of Justice of the European Union (CJEU), concerned a reference for a preliminary ruling following an order issued by

160. For a brief overview, see Ian Brown, "Internet self-regulation and fundamental rights", *Index on Censorship*, March 2010, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1539942.
161. But note the Dutch court ruling that a previously imposed block on the "Pirate Bay" website was "disproportionate, ineffective, and hinders the Internet providers' entrepreneurial freedoms": http://torrentfreak.com/isps-no-longer-have-to-block-the-pirate-bay-dutch-court-rules-140128/.
162. Yildirim (see n. 3), paras. 28 and 29.

a Belgian court requiring an Internet service provider to install a permanent monitoring system blocking all online activity liable to infringe intellectual property rights.
In its judgment of 24 November 2011 the CJEU held that the holders of intellectual property rights should have the possibility of applying for an injunction against an intermediary who carried a third party's infringement of a protected work or other subject-matter in a network, and that the arrangements governing such injunctions should be left to national law. However, the national rules had to observe the limitations arising from European Union law and in particular from Directive 2000/31/EC on electronic commerce, which prohibited national authorities from adopting measures which would require an Internet service provider to carry out general monitoring of the information that it transmitted on its network. The CJEU took the view that injunctions of the kind issued in the case under consideration did not respect the requirement that a fair balance be struck between the right to intellectual property on the one hand and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information on the other. Accordingly, it concluded that European Union law, and in particular Directive 2000/31/EC and the applicable fundamental rights, precluded an injunction imposed on an Internet service provider to introduce a system for filtering all electronic communications passing via its services, applied indiscriminately to all its customers, as a preventive measure, exclusively at its expense and for an unlimited period.

As we have seen, in Yildirim, the Strasbourg Court held a law to be contrary to the Convention which did not envisage restricting state-authorised blocking to specific sites with illegal content. This suggests that the Court might also concur with the CJEU that indiscriminate filtering of all the communications carried by an ISP (or an MNO) – that is, general monitoring or surveillance – for the purpose of identifying possible copyrights infringers from the mass of innocent users is contrary to the ECHR.

The situation would become more complicated if, as in the case of the draft EU Child Exploitation Directive, the measure (blocking) was enshrined in law, but the mechanism was left open. In that case, the ECHR would be faced with trying to find a balance between effectiveness, legitimacy and proportionality: in other words, would a less invasive but less effective tool be preferable to a more effective but more intrusive tool, and what criteria would be used to make such an assessment?

## 3.6. Exercise of extraterritorial jurisdiction by states

Quite separate from the question of whether a state must respect the human rights of non-citizens not residing in the country, discussed above (section 3.3), there is the question of the extent to which any country may, in international law, do things against, or that affect the rights of, such non-nationals in other countries. This is an issue not of human rights law but of general public international law.

This is not the place to address the complex issues of the international legal duty of all states to respect the sovereignty of all other states, and not to intervene in the

internal affairs of other countries, and the (limited) exceptions to this principle.[163] However, we should note that:[164]

> The governing principle is that a state cannot take measures on the territory of another state by way of enforcement of national laws without the consent of the latter.

More specifically, as the International Law Commission said:[165]

> With regard to the jurisdiction to enforce, a State may not enforce its criminal law, that is, investigate crimes or arrest suspects, in the territory of another State without that other State's consent.

It is for this very reason that it has been a long-standing practice, in relation to international criminal matters, that states wanting to obtain evidence or apprehend people who are in another country must do so under (bilateral or multilateral) mutual legal assistance treaties (MLATs) or extradition treaties. The disagreement between the EU and the USA regarding the Microsoft case described above (section 2.2.2), illustrates this very clearly. There are elaborate arrangements in place for these, including important multilateral (European) treaties produced by the Council of Europe[166] and the EU Justice and Home Affairs arrangements.[167]

There are also elaborate treaty arrangements in place on international co-operation between certain states in relation to intelligence gathering and sharing. Unduly secret and seriously deficient though these are in terms of human rights protection, the point to be made here is that the very existence of such treaties shows that the

---

163. For a detailed discussion, see *Report of the International Law Commission*, 58th session (2006), Annex E – extraterritorial jurisdiction, p. 516ff, at http://legal.un.org/ilc/reports/2006/2006report.htm.
164. Ian Brownlie, *Principles of public international law*, 6th edn, 2006, p. 306. The classic expression of the principle is in the Palmas Island case award by the sole arbitrator, Max Huber: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State. The development of the national organization of States during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the State in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations." Island of Palmas Case (Netherlands/United States of America), Award of 4 April 1928, UNRIAA, vol. II (1928), pp. 829-71, at p. 838, available at http://legal.un.org/riaa/cases/vol_II/829-871.pdf. See also Lowe, "Jurisdiction" (n. 93 above).
165. *Report of the International Law Commission* (2006), Annex E (n. 163 above), para. 22, p. 526.
166. In particular, apart from the Cybercrime Convention discussed in section 4.5, the 1959 European Convention on Mutual Assistance in Criminal Matters (ETS No. 30) and its two additional protocols, and the 1957 European Convention on Extradition (ETS No. 24) and its additional protocols.
167. In particular, the 2000 EU Convention on Mutual Assistance in Criminal Matters between the member states of the European Union (which built on the Council of Europe Convention), with its Protocol (2001), which both came into effect in 2005, the 1995 EU Convention on simplified extradition procedure between member states of the European Union, and the 2004 European Arrest Warrant. Beyond these, the EU has also established elaborate institutional frameworks for police and judicial co-operation, including Europol, Eurojust, Eurodac, the Schengen Information System (SIS, now SIS-II), the Visa Information System (VIS), the Custom Information System (CIS) and the Prüm Treaty – all of which were discussed in another issue paper, "Protecting the right to privacy in the fight against terrorism", 2008, section 5.2, available at https://wcd.coe.int/ViewDoc.jsp?id=1469161.

principle of the need for consent is still clearly generally accepted and reflects *opinio juris*: the view of the states concerned that consent is not just a matter of international courtesy, but legally required.

The diplomatic row over interception of communications (in particular, the mobile phone conversations) of heads of state of Western countries by their supposed allies in the 5EYES intelligence community also reflects this view: they relate to the secret spying more as a matter of alleged violations of state sovereignty and diplomatic immunity than as a violation of the individual rights of the officials concerned.

Respect by states for the political and territorial integrity and sovereignty of other states is one of the core requirements of the rule of law in the wider sense, referred to by the UN Secretary-General:[168] it is the external (intra-state) equivalent of the internal duty of states to adhere to the principles of the rule of law in the exercise of their domestic powers.

A state that uses its legislative and enforcement powers to capture or otherwise exercise control over personal data that are not held on its physical territory but on the territory of another state – for example, by using the physical infrastructure of the Internet and global e- and m-communications systems to extract those data from servers, personal computers or mobile devices in the other state, or by requiring private entities within its jurisdiction that have access to such data abroad to extract those data from the servers or devices in another country and hand them over to the state – is exercising its jurisdiction extraterritorially. In accordance with the above principle, it is not lawful for the first state to do this without the consent of the second state. As Vaughan Lowe puts it:[169]

> It should be clear that if in any case the exercise by one State of its jurisdiction threatens to subvert the laws that another State has enacted to regulate life in its own territory, in the exercise of its sovereign right to choose how to organize life within its borders, the boundaries of lawful jurisdiction have been overstepped [by the first State].

Extracting information from databases or communication system is typically strictly regulated by state law. Indeed, under the Cybercrime Convention, actions of this kind must be made crimes ("interference with computer systems" or "interception of communications"). All states provide for exceptions, allowing their own law enforcement and national security agencies to perform such acts legally, but they rarely grant such privileges to foreign agencies, for which elaborate mutual assistance treaties are instead adopted, and these leave control of such matters in the hands of the state where the computer or communication systems are. In other words, in the absence of treaties that grant foreign agencies powers of extraterritorial enforcement jurisdiction,[170] a state that unilaterally grants its own agencies power to perform acts

168. Quoted at the beginning of section 3.1, above.

169. Lowe, "Jurisdiction", in M. Evans (ed.), *International Law*, Oxford UP 2003, pp. 354-5.

170. Lowe gives examples of "unusual, but not unknown" arrangements by which "one State [gives] permission to another [state] to exercise enforcement jurisdiction in its [the first state's] territory." Ibid., p. 352. The examples do not include the Cybercrime Convention.

in another state that are not legal under the law of the targeted state subverts the laws of the targeted state and violates international law.[171]

In section 4.7.3, below, we discuss whether the Cybercrime Convention itself constitutes a treaty giving the law-enforcement agencies of its states parties permission to exercise extraterritorial enforcement jurisdiction in the territories of the other states parties – and, if so, to what extent.

171. For further discussion of this issue in relation to the mass surveillance operations revealed by Edward Snowden, see the Expert Opinion provided by Douwe Korff to the Committee of Inquiry into this matter of the Lower House (Bundestag) of the German Parliament, available at: www.bundestag.de/blob/282874/8f5bae2c8f01cdabd37c746f98509253/mat_a_sv-4-3_korff-pdf-data.pdf.

Chapter 4

# The issues, and the balance between them

## 4.1. The issues

The rule-of-law requirements discussed above arise primarily out of the UN Charter (setting out the intra-state rule of law) and international human rights instruments, in particular the ICCPR and the ECHR (containing the rule-of-law requirements that states must comply with domestically). These requirements are relevant to freedom of expression and the extensive control exercised over the Internet and the wider digital environment by private entities, especially US ones. The rules on both of these are complex and, in some regards, under-developed.

In addition, we note here two issues that are subject to special regulation and central to the rule of law on the Internet and in the wider digital environment: data protection and cybercrime. The international (including European) regulations on these two issues in some ways complement each other.

There is one further issue, already mentioned: the until recently largely secret – and largely secretly (if at all) regulated – activities of states relating to national security, activities which have become ever more closely entwined with law enforcement (with the fight against terrorism in particular sitting uneasily between the two areas) and which have been subjected to considerable public attention by Edward Snowden.

Establishing the rule of law on the Internet and in the digital world will require:

- clarifying the rules in the first four areas – freedom of expression, human rights and private entities (in particular, corporations), data protection, cybercrime – and their interactions;
- ending the under-regulation of the fifth (national security activities); and
- addressing the question of a balance between them all in this environment.

## 4.2. Freedom of expression

In section 3.4.2 above, it was noted that national laws relating to activities on the Internet and the wider digital environment, and especially those relating to freedom of expression, often compete and conflict; and that this poses a fundamental threat to the rule of law on the Internet and the wider digital environment, a threat which has barely been addressed in the case law of the European Court of Human Rights.

It was suggested that the only way to resolve this would be if states, and national courts, were to show clear restraint in imposing their domestic legal standards on expressions and information disseminated over the Internet and in the wider digital environment from abroad, unless these are unlawful under international law or present clear links justifying the exercise of their jurisdictions.[172] This is one core issue that must be resolved if the rule of law is to be safeguarded on the Internet and in the wider – inherently transnational – digital environment.

### The Delfi case

A further issue is the liability, of individuals or companies managing a website, for content posted on their website. The European Court of Human Rights was faced with this in the recent Delfi case.[173] In that case, a chamber of the Court held that the national courts had not violated the Convention when they held an Internet company liable for negative and (according to the domestic courts, defamatory) comments made by third parties about another company under an (in itself, balanced and proper) article on its website, in spite of the fact that the company had taken quite serious measures to remove any offensive comments easily and quickly, by means of filters looking for offensive words (or even roots of such words), and an easy-to-use "notice and take-down" procedure, requiring just one click on its website (which the offended company did not use). In reaching this conclusion, the Court took particular account of the following elements:[174]

> the insulting and threatening nature of the comments, the fact that the comments were posted in reaction to an article published by the applicant company in its professionally-managed news portal run on a commercial basis, the insufficiency of the measures taken by the applicant company to avoid damage being caused to other parties' reputations and to ensure a realistic possibility that the authors of the comments will be held liable, and the moderate sanction imposed on the applicant company.

Consequently, the European Court of Human Rights considered that

> in the present case the domestic courts' finding that the applicant company was liable for the defamatory comments posted by readers on its Internet news portal was a justified and proportionate restriction on the applicant company's right to freedom of expression.[175]

---

172. See section 3.4.2, above.
173. *Delfi AS v. Estonia*, Application No. 64569/09, judgment of 10 October 2013, not final.
174. Ibid., para. 94.
175. Ibid.

The judgment has been heavily criticised, with many civil society and digital rights groups asking for the case to be fundamentally reconsidered.[176] The case was referred to the Grand Chamber of the Court on 17 February 2014.[177]

It indeed seems important to revisit some of the issues in the Delfi case, which have wide repercussions for the rule of law and freedom of expression on the Internet.

A core problem with the Delfi ruling is that it places a heavy onus on a private party to arbitrate on what speech is permitted or not – an onus that goes beyond the expeditious removal of offending comments and the keyword filtering that the defendant was already using.

### The Telekabel case

This is more worrying when assessed in the context of the Telekabel case of the European Court of Justice,[178] which placed a similar balancing obligation on Internet access providers. In that case, the Austrian courts had imposed an injunction on such a provider (Telekabel) ordering it to block access by its customers to a website that was offering copyright-protected materials for download, without the agreement of the copyright holders. The final injunction left it to the provider to choose the means to achieve the blocking. The Viennese *Oberlandesgericht* asked the CJEU if this was compatible with EU law. Telekabel argued, *inter alia*, that the various blocking measures that might be introduced could all be technically circumvented and that some of them were excessively costly.

In its ruling, the CJEU considered that:

> even though the measures taken when implementing an injunction such as that at issue in the main proceedings are not capable of leading, in some circumstances, to a complete cessation of the infringements of the intellectual property right, they cannot however be considered to be incompatible with the requirement that a fair balance be found, in accordance with Article 52(1), in fine, of the Charter, between all applicable fundamental rights, provided that (i) they do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available and (ii) that they have the effect of preventing unauthorised access to protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right. (§63)

---

176. See, "European Court strikes serious blow to free speech online", *Article 19*, 14 October 2013, at www.article19.org/resources.php/resource/37287/en/european-court-strikes-serious-blow-to-free-speech-online; "Case watch: a Strasbourg setback for freedom of expression in Europe", Open Society Foundations, 22 October 2013, at www.opensocietyfoundations.org/voices/case-watch-strasbourg-setback-freedom-expression-europe; and "Civil society calls on the ECHR's Grand Chamber to overturn Delfi v. Estonia ruling", *La Quadrature du Net*, 15 January 2014, at https://www.laquadrature.net/en/civil-society-calls-on-the-echrs-grand-chamber-to-overturn-delfi-v-estonia-ruling.
177. At the time of writing the Grand Chamber (hearing, 9 July 2014) had not yet issued its judgment.
178. *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, C-314/12, 27 March 2014, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0314&from=EN. Note that this is in line with the Court's ruling in the Yahoo! France case discussed at 3.4.2, above.

In other words, the Court held that, though the measures that Telekabel was ordered to take would probably not fully achieve the aim of preventing access to the website, the order still struck a "fair balance" in terms of EU law, provided that those measures did not "unnecessarily deprive Internet users of the possibility of lawfully accessing the information available", yet did serve to "seriously discourage" users of the access service from accessing the content in question illegally.

The problem with this is that it leaves one crucial matter out of the equation: the possible impact of the blocking measures that Telekabel could consider on the freedom of its customers to access lawful material. The Austrian courts did not take this into account either.

For companies such as Telekabel this creates a dilemma that is likely to be resolved in a way that adversely affects freedom of information on the Internet. On the one hand, they are encouraged to impose blocking measures that are at least "strongly dissuasive": if they adopt measures that are subsequently deemed by a court to be too weak, they face the risk of incurring coercive financial penalties. On the other hand, if they impose very strong blocking measures, they are likely to "over-block" and deprive Internet users that use their services of access to perfectly legal material. While many providers may in theory be willing to take the latter into account, they are likely, if in doubt, to choose measures that reduce their risk of financial penalties. And they can protect themselves from suits from their customers over denied access to legal materials (which would be difficult to mount anyway), by simply giving themselves the right, under their general terms and conditions, to block material at their own discretion.

In these circumstances, it is easy to imagine that an ISP, as a private entity, could choose to impose the very kinds of blocking/filtering measures by means of its terms and conditions – that is, by contract – that, in the Scarlet/Sabam case, the CJEU held may not be imposed by the state by means of public law.[179] Imagining that Telekabel were to introduce such a measure via a change in its terms of service, where should a citizen complain? Telekabel would claim to have obtained the agreement of its customers to the new terms and conditions, so would have a strong defence in court. At the same time, since the measure was not directly imposed by public law, it would appear to also not be in breach of the Sabam ruling. Yet if a significant number of such entities between them dominate the relevant market, and they all include such terms in their terms and conditions, the effect would be very similar to a state-imposed block. Indeed, that is precisely why states such as the UK try to "encourage" private entities to take such steps.

A broadly similar logic was followed in the Google/Spain case,[180] as described above, leaving a private company with a choice between clear legal obligations on the one hand (remove search results or face punishment) and no particular obligations to avoid over-compliance, other than whatever public interest happens to coincidentally overlap with commercial interests.

---

179. *Scarlet Extended SA v. Société belge des auteurs, compositeurs et* éditeurs *SCRL (SABAM)*, case C-70/10, 24 November 2011.

180. See n. 114 above.

This problematic situation can only be overcome if companies whose activities are directly relevant to – and sometimes dominant in respect of – the activities of Internet and digital communication system users were to be under a legal obligation not to (ab)use their terms and conditions to unduly restrict the right to seek, receive and impart information on the Internet, and/or if states were to be under a clear duty to enforce such human right-protective restrictions on the use of contract law by companies. However, although such suggestions have been made, this is currently far from the actual legal situation, and the responsibilities of states in this regard are still very unclear, as further discussed in the next section.

## 4.3. Privatised law enforcement

We noted in section 3.5 that the Internet and the global digital environment are largely controlled by private entities (especially, but not only, US corporations) and this fact poses a threat to the rule of law in that context. In section 4.2 we looked at relevant case law of the Strasbourg Court and CJEU.

We have seen (in section 3.4.2 above, the Yahoo! case) how a French court's actions indirectly led to an outcome for US Internet users that would almost certainly have been ruled unconstitutional if it had been imposed directly by a judicial or legislative body in the United States. We have also seen how Internet blocking (which is unquestionably a restriction on freedom of communication, regardless of legitimacy) has been implemented in at least one state party of the Council of Europe without this being "prescribed by law".

Private entities can impose (and be "encouraged" to impose) restrictions on access to information without being subject to constitutional or international law constraints placed on state limitations of the right to freedom of expression. They can be ordered by domestic courts, acting at the request of other private entities, to perform highly intrusive analysis of their data to detect probable (or just possible) infringements of private property rights, especially intellectual property rights. They can be ordered to "pull" data, including governmental, commercial and personal data, from servers in other countries, for law enforcement or national security purposes, without obtaining the consent of the other country – nor the consent of the companies or data subjects in the other country – in violation of the sovereignty of the other country, the commercial confidentiality that companies are entitled to and the human rights of the data subjects.

The Ruggie Principles, while indicating the importance of addressing these issues, do not yet provide the answers; and new approaches and guidelines are therefore needed also in this respect.[181]

The issues involved are extraordinarily complex, but they are central to the present and future enjoyment of human rights in the digital environment, so they need some careful analysis, which is long overdue. Issues that need to be addressed include the following.

- At what stage is state responsibility reasonably triggered when "voluntary" measures taken by private companies are encouraged by a state? Does active

181. See the final paragraphs at the end of section 3.5.1, above.

coercion of Internet companies to "voluntarily" filter or block content, in the absence of a legal duty to do so, comply with the obligation in the ECHR for such restrictions to be "prescribed by law"?

- What are the obligations of the state when such restrictions are included in contracts – more specifically in general terms and conditions – "agreed" to by individuals that are signing up to Internet access services?
- If a large Internet access provider chooses to block (publicly and with non-specific consent of its users, other than its usually vague general terms and conditions) specific content, should the provider of that content be able to rely on the obligations of the state to ensure his/her freedom to impart information to the users of that service? How should that be achieved? Through what kind of remedy?

The scale of private enforcement and policing appears to be greatly underestimated. Virtually every type of online service provider is involved in non-law-based "voluntary" enforcement measures in relation to almost every conceivable online activity in the absence of a due process framework. For example:

- US online advertisers and US payment providers have agreements with the US President to "voluntarily" take punitive measures against services appearing to be breaching US IP and counterfeiting law;[182]
- the European Commission has proposed giving Internet access providers similar rights to "voluntarily" "manage" online traffic in order to "prevent or impede" unspecified "serious crime";[183]
- Google voluntarily imposes, on a global basis, the non-judicial US DMCA[184] procedure for take-down of content accused of breaching US law and removes search results in the UK and Germany (and possibly elsewhere) on the basis of informal arrangements with national authorities in those countries. Internet users in these European countries are thus *de facto* subjected to the cumulative enforcement, by private entities, of restrictions from two jurisdictions, outside any legal framework (and thus not subject to the limitations and remedies applicable to actions by state authorities);
- Open Rights Group, a UK NGO, calculated in July 2014 that almost one fifth of popular websites in the UK were being blocked by at least one of the UK's main Internet access companies;[185]

---

182. See www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting (2013) and www.whitehouse.gov/blog/2012/03/30/safeguarding-america-s-job-creating-innovations (2012).
183. Proposal for a Regulation "laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent", COM(2013) 627 final, 11 November 2013. As preamble 47 to this proposed Regulation says: "Reasonable traffic management encompasses prevention or impediment of serious crimes, including voluntary actions of providers to prevent access to and distribution of child pornography." See https://ec.europa.eu/digital-agenda/en/news/regulation-european-parliament-and-council-laying-down-measures-concerning-european-single (2013).
184. See section 2.3.2, above.
185. Open Rights Group, "ORG's Blocked project finds almost 1 in 5 sites blocked by filters", July 2014, available at https://www.openrightsgroup.org/blog/2014/blockedproject.

- the Internet Corporation for Assigned Names and Numbers (ICANN), the global body that manages the "root domain" of the Internet, adopted rules to make the accreditation of domain name registrars contingent on unspecified policing responsibilities – essentially to avoid "permitting illegal activity". This obligation was used by the City of London Police to attempt to coerce a domain name registrar EasyDNS into non-judicial removal of domain names of its customers. EasyDNS refused and the courts ruled that a judicial order was indeed needed.[186] However, the company, in its terms of service "reserves the right to revoke any or all services associated with a domain or user account, for policy abuses" which include "copyright infringement". As a result, the company arguably could have removed the domain in question without appealing to a court and the rule of law would never have been invoked.[187]

The report from the Council of Europe on "ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values",[188] published in June 2014, offers some valuable insights. The conflicts are clear from the document, which explains that "private organisations [such as ICANN] are not duty bearers under international law", but "business enterprises have a responsibility to respect human rights as set out in the UN Guiding Principles on Business and Human Rights" (cf. §9). The document nonetheless is unequivocal about the responsibility of states with regard to restrictions that may be imposed by this private entity, pointing out that "in the member states of the Council of Europe, any interference with these rights should meet the conditions laid down in the European Convention on Human Rights" (emphasis added) and "they [states] could also be held accountable, as a last resort before supranational courts, such as the European Court of Human Rights" – presumably, for not ensuring that private entities do not violate the human rights of their citizens (cf. §124). As noted above (section 3.5.1), the recent Council of Europe "Guide to human rights for Internet users" also suggests that states have an obligation to ensure that "general terms and conditions" of private-sector entities that are not in accordance with international human rights standards must be held null and void in the domestic legal systems of Council of Europe member states.

Overall, the Council of Europe's report on ICANN and its guide are remarkably rare (bearing in mind the scale and nature of the issues discussed) but important steps towards the development of a concept of the rule of law and state responsibility in the digital world.

## 4.4. Data protection

Data-protection laws regulate the use of personal data – primarily, data relating to living individuals or "natural persons". Such laws were introduced in many European

186. See http://blog.easydns.org/2014/01/09/domains-locked-in-london-police-takedown-ordered-to-be-transferred/.

187. In reality, the company's approach is far more nuanced and quite exemplary. See http://blog.easydns.org/2012/02/21/the-official-easydns-domain-takedown-policy/.

188. See www.coe.int/t/informationsociety/icann-and-human-rights.asp.

countries in the late 1970s and 1980s to protect the rights and interests of such persons against the perceived threat posed by unregulated processing of their information, in particular (but not only) by "automated means" – meaning computers. This was followed by the still-central Council of Europe Convention on Data Protection (hereinafter the DP Convention or Convention No. 108)[189] and then by specific EU directives and regulations.

The rights that these laws, this convention and the EU rules sought to protect include the right to privacy – or "private life" as it is called in the European Convention on Human Rights (Article 8). However, the laws and the European data-protection instruments aim at more than that. First, in the view of legislators and constitutional courts in many European countries, data protection as applied to "natural persons" has the wider purpose of protecting "human identity" (*l'identité humaine*) or the protoright to [respect for one's] "personality" (*das allgemeine Persönlichkeitsrecht*). Second, in the view of some legislators, similar rules are needed to protect interests which are not specific to living individuals. Parts of the data-protection laws of some countries and some rules in the EU data-protection rules therefore also apply to data relating to companies or organisations ("legal persons").

Data protection is therefore seen, in Europe at least, as a new fundamental right, *sui generis*, linked to (but not limited to) the protection of privacy, or the interests of natural persons only. This is most clearly expressed in the EU's Charter of Fundamental Rights, in which data protection is guaranteed as a separate right from private life (Article 8).

As well as being an important right, data protection is also a key enabler of other fundamental rights, such as freedom of communication and freedom of association. For this reason, the laws and procedures surrounding data protection and privacy rights need to be clear and well enforced. To this end, it is crucial for the modernisation of both the EU rules and the DP Convention to ensure a predictable and enforceable legal framework.

Rather than examining European data-protection laws in detail, it suffices to note four major issues (to one of which we return later).

### 4.4.1. European data-protection principles

The first issue is that European data-protection instruments (and the national data-protection laws implementing or reflecting them) are built around a common core of data-protection principles first set out in the DP Convention, the mother document of all international data-protection instruments.[190] These principles,

189. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS No. 108, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

190. For Convention No. 108, see n. 189. For an overview of the EU's and the Council of Europe's applicable standards, see the *Handbook on European data protection law*, published jointly by the European Court of Human Rights and the EU Agency for Fundamental Rights (FRA) in December 2013, at: www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

confirmed and expanded in the EU data-protection directives,[191] are to be further strengthened by an EU regulation.[192]

These core principles, common to all the European instruments (with minor variations), stipulate that all personal data must be:

- processed fairly and lawfully (Article 5(a) of the DP Convention, Article 6(1)(a) of the main DP Directive);
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Article 5(b) of the DP Convention, Article 6(1)(b) of the main DP Directive);
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Article 5(c) of the DP Convention, Article 6(1)(c) of the main DP Directive);
- accurate and, where necessary, kept up to date (Article 5(d) of the DP Convention, Article 6(1)(d) of the main DP Directive); and
- kept in identifiable form for no longer than necessary for the purposes for which the data were collected or for which they are further processed (Article 5(e) of the DP Convention, Article 6(1)(e) of the main DP Directive).

The most important of these core principles are "purpose specification and limitation", "data minimisation" and "fairness." Essentially, private entities are not allowed to collect more data on individuals (typically, their customers or visitors to their websites) than they need in order to provide the goods or services in question and bill for them; they may only use those data to provide those goods and services (and for closely related "not incompatible" purposes); and they must destroy the data when the data are no longer needed. If they want to collect more data, or keep them for longer or use them for other purposes – or disclose them to other entities, in particular public-sector bodies – they need either the express, free and informed consent of the data subjects, or a special statutory authorisation. Public bodies must more generally have a statutory basis for their processing of personal data. The laws or legal rules in question must, moreover, conform to the rule-of-law requirements relating to "law", discussed earlier: the legal authorisation must be clear, accessible, specific and foreseeable in its application.[193]

---

191. 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, 23 November 1995, OJ L.281, p. 31ff. (the main EC directive on data protection, hereinafter the main DP Directive); Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, usually known as the e-Privacy Directive, and subsidiary to the main Data Protection Directive), 31 July 2002, OJ L 201, p. 37ff, as amended.
192. 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, 25 January 2012, COM(2012) 11 final (Commission's original proposal). An informal version of the latest text, containing the amendments proposed by the European Parliament, is available at www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf.
193. See section 3.2.1, above.

Because of their roots in European human rights law (especially the ECHR), European data-protection rules do not allow for discrimination in protection between nationals and non-nationals, residents and non-residents: if personal data on anyone (whatever their nationality and whatever their place of residence) are processed by a European controller, those data enjoy the full protection of the European rules – and, to the extent that there are exceptions to the rules, as discussed below, those exceptions must also be applied equally and without discrimination of any kind.

Also crucial are the concepts of "personal data" and "processing": the former is defined and interpreted strictly, the latter very widely.[194] Consequently, all data that are related to, or can in a realistic scenario be linked to, an individual are covered by the rules, whenever they are created, stored, collected, disseminated or used.

In order to prevent circumvention of the rules or their non-application in circumstances affecting individuals, the instruments also contain extensive rules on the transfer of personal data from European countries that implement the European rules to countries that do not provide similar ("adequate") levels of data protection.

Moreover, compliance with the data-protection rules and principles must be closely monitored and supervised by an independent authority (generally referred to as the data-protection authority or DPA, though it has different names in different countries).[195] And crucially, the convention provides for extensive, compulsory mutual assistance between the DPAs, subject to limited exceptions which, the explanatory report explains, "correspond generally with those provided for by other international treaties in the field of mutual assistance".[196]

This briefly described framework of European data-protection rules provides the backbone to the rule of law on the Internet and in the global digital world for European and non-European citizens, at least insofar as their data are being processed by controllers in states parties to the DP Convention (see below).

### 4.4.2. Moving beyond Europe

The second major issue to note is that the Data Protection Convention (like the Cybercrime Convention)[197] is open to non-Council of Europe member states. Indeed, both are intended to set global standards, and the Council of Europe actively encourages non-European states to join them. In addition, the EU encourages non-EU states, including those outside Europe, to adopt laws modelled on the EC directives, by offering freedom to transfer personal data only to countries with "adequate" protection of personal data.

---

194. This contrasts with the much more lax application of US privacy principles relating to "personally identifiable information" (PII): the definition of PII is much less inclusive than the European definition of "personal data" and the "third party doctrine" exempts much processing from US privacy protection.
195. The requirement of a truly independent authority was only added to the DP Convention by means of its 2001 Additional Protocol, Convention ETS No. 181, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm (see Article 1).
196. Explanatory Report to the DP Convention, para. 80.
197. Also discussed in section 4.5, below.

The Council of Europe and the European Union have had limited success in this. In 2013, Uruguay became the first non-Council of Europe state to become a party to the Data Protection Convention, and discussions are under way with several other non-European states, including Morocco. The EU's European Commission has so far recognised six non-EU states as providing privacy rules that are "adequate" from a European perspective, as well as four islands linked to the UK (technically, subject to the British Crown) and a further group of islands linked to Denmark.[198] It has also ruled that the USA provides "adequate" protection for the transfer of air passenger name records (PNRs) to the United States Bureau of Customs and Border Protection, and in relation to the transfer of data to companies that have voluntarily signed up to the so-called Safe Harbor arrangement – but both these latter findings have been put in serious doubt as a result of the Snowden (and other) revelations.[199] Even so, European data-protection law is clearly influencing privacy laws in many parts of the world, from Hong Kong and Indonesia to Mexico and South Africa.[200]

As a result, it will be crucial to ensure that the review ("modernisation") of Convention No. 108, currently under way, does not lead to any lowering of the standards. On the contrary, the aim should be to re-affirm the basic principles that have withstood the test of time and ensure that they will be fully applied to the Internet and the wider, global digital world, and also to special (so far under-regulated) areas, such as state and commercial surveillance. To this end, accession by the USA to Convention No. 108 would be particularly valuable, not just for US citizens but as a move towards a more comprehensive, global approach to respect for the fundamental right to data protection and the rights that it enables. This is why the European Commission encouraged the USA to take this step, arguing that "safeguards and guarantees agreed in international fora should result in a high level of protection compatible with what is required under EU law".[201]

Efforts by the Council of Europe and the EU to have data-protection laws or privacy laws similar to the European ones adopted globally should be supported, as a major means towards establishing the rule of law on the Internet. The Council of Europe Data Protection Convention should be strongly promoted as the "gold standard" in this respect globally.

### 4.4.3. The US position

The third issue to note here is the lack of any sign that the USA, the country with the greatest influence and power over the Internet, is willing to move in this

198. Andorra, Argentina, Australia, Canada, Switzerland and Israel, the Isle of Man, Guernsey, Jersey and Alderney, and the Faeroe Islands.

199. On PNR data transfer, see nn. 20-21 above. On Safe Harbor, see "EU calls for suspension of multi-billion 'Safe Harbor' deal over NSA spying" and "Data protection: Claude Moraes calls for suspension of EU-US 'safe companies list'" (both reporting calls to that effect from individual, high-ranking members of the European Parliament civil liberties committee) at http://rt.com/business/eu-threaten-suspend-harbor-006/ and www.socialistsanddemocrats.eu/newsroom/data-protection-claude-moraes-calls-suspension-eu-us-safe-companies-list.

200. See the "global data-protection map", produced by Privacy International in 2011, at https://www.privacyinternational.org/global-data-protection-map.

201. Communication of the European Commission, "Rebuilding trust in EU-US data flows", 27 November 2014, http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

direction. Even domestically, it does not subscribe to the "constitutional" approach to data protection adopted in Europe (as described at the beginning of this section 4.4). Indeed, as a result of the "third party doctrine", it provides very limited protection to personal data, even of its own citizens, under its own Constitution (although some state laws go further towards the European approach, in some specific contexts).[202] In addition, under US law, the US Government can rely on secret interpretations by a court (the FISA Court) sitting in camera in relation to its actions affecting both US citizens and residents and "non-U.S. persons".[203] As explained in section 3.2.1, by international human rights standards such secret interpretations of laws do not constitute "law" and cannot be relied on to impose restrictions on fundamental rights.

Moreover, US laws expressly discriminate against non-US citizens and non-US residents.[204] As already noted, the USA takes the view that its obligations under the ICCPR, including its privacy provision (Article 17), do not apply extraterritorially. In other words, the privacy of non-US citizens and non-US residents (generally referred to by the USA as "non-U.S. persons") is given almost no protection under the US Constitution, and the USA believes that it also has no duty under the ICCPR to protect the privacy of such persons.

In view of the USA's predominant power over the Internet, the denial by that country of any international legal duty to protect the privacy of non-US persons is one of the most egregious threats to the rule of law on the Internet and in the wider digital environment. It should be a high priority of all European institutions, including the Council of Europe, to urge the USA:

- to acknowledge the universality of all human rights, including privacy;
- to accept that, in all activities that affect the rights of US- and non-US persons anywhere, it is bound by its international human rights obligations (including, specifically, the ICCPR);
- to regulate all such activities through clear, specific, accessible law (that is, to end secret interpretations of the law by courts sitting in camera without making their rulings public); and
- to end all discrimination in these regards against "non-US persons".

### 4.4.4. Gaps in data protection

Finally, it should be noted that both the Council of Europe Data Protection Convention and the EU Data Protection Directives contain exceptions relating to crime prevention and law enforcement, and national security. With regard to crime prevention and

202. See the EDRi/FREE submission on the surveillance activities of the United States and certain European states' national security and intelligence agencies, sent to various European and US bodies in August 2013, in particular Section III (paras. 10-11) and Attachment 3: Summary of United States standards on national security surveillance (with further references), at www.edri.org/files/submission_free_edri130801.pdf.

203. See note 82 above.

204. See the EDRi/FREE submission (cited in n. 202), Attachment 3, paras. 5-7, with further references.

law enforcement, this is to some limited extent counterbalanced by a provision in the Cybercrime Convention requiring (a measure of) compliance with human rights standards in these fields, as discussed in the next section. But the situation in relation to national security is more seriously deficient, as we shall see.[205]

## 4.5. Cybercrime

### 4.5.1. Introduction

As noted in section 1.2 above, the Internet and the wider digital world of e-communications, apart from providing a positive space for social and cultural activities, also provide new opportunities for criminal activities, and indeed for new types of crime. The Council of Europe has taken the lead in promoting international co-operation in this field too, in particular through its Cybercrime Convention.[206] Once again, this is a convention that is open to non-European states (and non-member states Canada, Japan, South Africa and the USA were involved in drafting it). In fact, it has been ratified by 36 Council of Europe member states and five non-European states, including the USA; a further nine Council of Europe member states and two non-European states have signed but not yet ratified the convention.[207]

The Cybercrime Convention requires states parties to make certain acts – such as illegal access to computer systems (hacking), illegal interception of electronic communications, the sending of malware, copyright violations and the production or dissemination of child pornography – criminal under their national law (see Chapter II, Section 1, Articles 2-10); its Additional Protocol requires states parties to criminalise the dissemination of racist and xenophobic material (hate speech).[208] In addition, it makes extensive provision for international co-operation in fighting the crimes in question, including mutual legal assistance in investigation and preservation of evidence, extradition and similar matters (Chapter III).

There is no doubt that there is a serious need for a major international instrument in the area of cybercrime, particularly in relation to the specific crimes just mentioned. The European Court of Human Rights has expressly referred to the convention in its case law.[209] The Council of Europe is to be commended for having initiated such an instrument. However, given that this is a crucial instrument for the rule of law in the digital environment, it is of concern that some aspects of the convention are weak in three such matters: the limitation of the main human rights clause to procedural law only; the problem of concurrent and conflicting application of different national laws implementing the convention; and the contentious provision on cross-border "pulling" of data by law-enforcement agencies.

---

205. Section 4.6. We revisit the delicate and largely unresolved issues of balance in section 4.7.
206. ETS No. 185, also known as the "Budapest Convention".
207. For details of the countries concerned, see www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=05/01/2014&CL=ENG.
208. The Additional Protocol has not been signed or ratified by several parties to the main treaty, including the UK and the USA.
209. See *K.U. v. Finland*, Application No. 2872/02, judgment of 2 December 2008, paras. 24-27.

### 4.5.2. Lack of a general human rights clause in the Cybercrime Convention[210]

Article 15 of the convention requires states parties to the convention to act in accordance with international human rights law – but only in relation to procedural matters: "the establishment, implementation and application of the powers provided for in this section" (emphasis added). The requirement is not extended to the substantive legal provisions, nor to international co-operation, nor indeed to the transnational data access envisaged in Article 32, further discussed below.

The first of these omissions – the failure to require the states parties' substantive law to be in conformity with human rights law – is problematic because, under the case law of the European Court of Human Rights, while states have a positive obligation inherent in Article 8 of the convention to criminalise (actual or attempted) offences against the person and to reinforce the deterrent effect of criminalisation by applying criminal-law provisions in practice through effective investigation and prosecution, the very existence of criminal legislation can also constitute an "interference" with a fundamental right.[211] Furthermore, the imposition of criminal sanctions in relation to any matter covered by any substantive article in the ECHR will of course always constitute such an interference. This means that the very specification of the criminal offences that must be created to implement the relevant articles of the Cybercrime Convention in national law must conform to the "typical" ECHR/ICCPR standards: they must be accessible and set out in sufficiently clear and precise terms to be reasonably foreseeable; they must serve a "legitimate aim"; and they must be "necessary" and "proportionate" to that aim. The latter may mean that there is a *de minimis* exception or a public interest defence. Although it is clearly the case that the state's obligations flowing from the main human rights treaties just mentioned remain in place, the adoption of a limited (rather than all-encompassing) human rights clause clearly limits the potential of the Cybercrime Convention to ensure the prevalence rule of law in the digital environment.[212]

Yet while the Cybercrime Convention does require proportionality in implementation of the substantive articles (Article 13), it does not clarify such matters in any more specific way, and many of the substantive articles in the Cybercrime Convention can be read very extensively to criminalise trivial matters that cause no actual harm or activities that are actually in the public interest.[213] Moreover, there is nothing about exceptions or defences to the crimes covered.

---

210. This sub-section draws on Douwe Korff, "Note on some main issues", submitted to the Council of Europe CyberCrime@IPA Conference, Baku, Azerbaijan, 5 November 2012.

211. See *K.U. v. Finland* (see n. 209), para. 46; Klass (see n. 66) on surveillance, and *Dudgeon v. the UK*, Application no. 7525/76, judgment of 22 October 1981, on criminalisation of homosexual acts.

212. It becomes even more difficult to understand the Cybercrime Convention's approach in this regard, if we compare it with the 2014 Convention on preventing and combating violence against women and domestic violence which takes a more comprehensive approach (cf. Article 71.1: "this Convention shall not affect obligations arising from other international instruments").

213. The Convention leaves states parties considerable discretion in relation to the substance of such crimes and important elements of these crimes (intent, damage, seriousness) and many states have entered declarations when signing the Convention that create further, explicit divergences, for example, by limiting certain crimes to cases of "malicious intent" or where there is "[real] damage", or not defining what constitutes child pornography (see Example 2). The crimes created under the same provisions by different states parties may therefore be quite different in detail. Thus, national laws differ in many respects in defining infringement of copyright, and the exceptions and exemptions (see Example 3).

It may be useful to illustrate this point with some examples close to real situations.

### Example 1

It would appear that Edward Snowden, when he downloaded highly classified information for purposes unrelated to his job, accessed the computer system from which he obtained the information "without right". Prima facie, his activities appear to constitute a criminal act in terms of Article 2 of the Cybercrime Convention[214] (even if, in reality, he has been charged with the more serious offence of spying). If he or someone like him were to be convicted of the offence in the Cybercrime Convention, it seems entirely plausible that the European Court of Human Rights would rule that such an activity deserved a "public interest" defence and that the Human Rights Committee would concur. If the Cybercrime Convention contained a general human rights clause, a national law that wrongly criminalised whistle-blowing of this nature by not providing a public interest defence to "accessing a computer system without right" would be incompatible with the Cybercrime Convention.

### Example 2

As noted above, under UK law (and the law of other countries), an 18-year-old man in possession of a sexually explicit photograph of his 16-year-old girlfriend is technically guilty of possession of child pornography if she looks like a 15-year-old, even though the girl was not under 16 and consented to the picture being taken. Although it is unlikely that the young man would be prosecuted in most countries, that is certainly a possibility. Yet a conviction on this charge might well be in violation of the young couple's rights to privacy and "family life" (a right that is very widely interpreted by the European Court of Human Rights). Article 13(1) requires any sanctions to be proportionate, but a situation where the very criminalisation of an act (the substantive scope of the offence) violates human rights law is not addressed.

### Example 3

It is explicitly recognised in Article 4 that a state party to the Cybercrime Convention may make, *inter alia*, "alteration or suppression of computer data without right" a criminal offence, even if no "serious harm" resulted from this. This provision can clearly be used by states to criminalise non-malicious "hacking" that causes no harm and may even have positive effects, for instance by exposing security weaknesses in systems (so-called "white hacking"). The second paragraph, which allows states

214. Article 2: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

to apply the provision only to activities that do cause serious harm, clearly shows that some states at least are concerned about excessively wide application of the offence. Again, it is arguable that criminalising such non-malicious, non-harmful activity could contravene human rights law.

These deficiencies are aggravated by the vague and broad terms used in Article 6 that require criminalisation of a wide range of activities connected to the offence in Article 4 (and other offences), including "making available" "a computer program, designed or adapted *primarily* for the purpose of" committing the offence, or of a password to a computer system "with the intent that it be used" for the offence in question. Again, there is no mention of any required limitation or defence.

### Example 4

In spite of the fact that – as noted in Article 10(1) – there are extensive international agreements on intellectual property law, national laws on the matter still differ in many respects, in particular in the exceptions and exemptions from rules that restrict the use of IP-protected material. For instance, some countries have clear and strong exceptions relating to the use of such material for educational purposes or in making material accessible to people with certain disabilities. Others provide for special exemptions for quotation and criticism, or for parody or satire. The international treaties allow for such divergence. Some exceptions and exemptions are arguably required under international human rights law, for example to protect freedom of political or artistic expression. Yet once again, the Cybercrime Convention does not acknowledge this and – because there is no general human rights clause – it does not require such exceptions and exemptions to be read into the relevant provisions.

### Example 5

Finally we return to the role of the private sector in this context, more specifically the use by private companies of their general terms and conditions to impose restrictions on the actions of individual users of their products or services. Specifically, any individual who accesses an online service in a manner that does not fully respect the terms of service (using any incorrect information when signing up to Facebook, for example) is arguably intentionally accessing the whole or part of a computer system "without right".[215] Bearing in mind the very broad, often long and unclear terms of service that some operators use, this essentially places the power to decide what is criminal or not in the hands of the company in question. As the issues and wording are broadly similar, the submission of the Electronic Frontier Foundation to the European Parliament on the draft Directive on Attacks against Computer Systems provides useful analysis.[216]

---

215. See Article 2 of the Cybercrime Convention, see n. 214.
216. See https://www.eff.org/files/filenode/Submission-Parliament-Hacking-Tools-vf.pdf.

### 4.5.3. Concurrent and conflicting criminal laws: lack of a *ne bis in idem* rule[217]

In section 3.4.2, above, we noted the problems caused to the rule of law on the Internet and in the digital environment by different, concurrent and conflicting national laws simultaneously applying to activities of individuals in that environment.

Unfortunately, the Cybercrime Convention does not address these problems – indeed, it clearly itself allows for (and partly provides for) concurrent criminal jurisdiction. Article 22(1) in principle requires states to exercise jurisdiction over the cybercrimes listed, both on the basis of territory and on the principle of active nationality – exercising jurisdiction over one's own nationals, although states can limit this under Article 22(2) – but Article 22(4) in effect permits states to also claim jurisdiction on any other ground in their domestic law, for instance, that the effect of the crime was felt in their state or by one of their nationals or by a company established in their territory. This clearly creates a serious risk of concurrent and conflicting laws applying to the same (transnational) acts. Moreover, the Cybercrime Convention does not contain a transnational *ne bis in idem* rule such as is included in the EU Charter on Fundamental Rights (see below).

In mitigation, one could point to Article 22(5), which places an obligation on states to "consult", "where appropriate", in cases of concurrent jurisdiction, although only in the context of "determining the most appropriate jurisdiction for prosecution". In this, one could perhaps draw parallels with safeguards in extradition and mutual legal assistance treaties with regard to *ne bis in idem*. However, there is no clear stipulation, either in the convention itself or in the Explanatory Memorandum, that this consultation should aim at avoiding double jeopardy. On the contrary, the only aims of the "consultations" mentioned in the Explanatory Memorandum are "to avoid duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the States concerned, or to otherwise facilitate the efficiency or fairness of the proceedings." At most, one can read into this that individuals should not be prosecuted more than once, in different jurisdictions, for the same acts, if to do so would be "unfair" in the specific circumstances.

However, it is to be noted in this respect that, in the ECHR, *ne bis in idem* is not listed as an essential part of the right to a fair trial per se in the article on fair trials, Article 6 ECHR. Rather, the guarantee against double jeopardy in the ECHR is set out as an additional right in an optional protocol only (Article 4, 7th Protocol) – and what is more, even there, it is limited to repeated proceedings over the same acts in the same country, and even then of course only with regard to states that have ratified that protocol. In other words, the ECHR does not protect against double prosecution of a person in different countries: it does not stipulate (and is not interpreted as

217. For more detail and in-depth discussion, see H. W. K. Kaspersen, "Cybercrime and jurisdiction", draft discussion paper prepared for the Economic Crime Division of the Council of Europe, March 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/t-cy/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf. This report in turn draws on a 1990 Council of Europe European Committee on Crime Problems study and recommendation on extraterritorial jurisdiction and jurisdictional conflicts. Professor Kaspersen was closely personally involved in the drafting of the Cybercrime Convention. His comments on the intentions of the drafters are therefore of great importance, and we refer to them in this section and especially in section 4.5.3, below.

providing) that it would *ipso facto* be "unfair" to prosecute the same person twice for the same acts in different countries, even after a final acquittal or conviction in one of those countries.[218] The point to note here is that the Cybercrime Convention also does not seek to provide protection against such double jeopardy, even between states parties to that convention. By contrast, the EU member states have decided to apply the principle of *ne bis in idem* to any case in which a person has been finally acquitted or convicted (only) within the Union (Article 50 CFR).

In other words, Article 22(5) does not appear to be aimed at avoiding double jeopardy, and the reference to "fairness" as an aim for the (non-mandatory) consultations can therefore not be seen as a guarantee against double jeopardy.[219] The reference to "the most appropriate" country to exercise jurisdiction in transnational cases could therefore refer to the question of what would be the "best" country to exercise jurisdiction. Law-enforcement agencies may feel that the "most appropriate" country to exercise jurisdiction is the country that provides for the widest law and the heaviest penalties; while others might argue to the contrary and/or, as in the case of Gary McKinnon, that a person should preferably be tried in his home country, under the laws of that country, rather than be extradited to another country (in McKinnon's case, the USA) that has much harsher laws on the relevant crime.[220]

Of course we must also acknowledge that, to the extent that the activities in question would have been criminalised anyway by individual states, the concurrent jurisdiction problem that was not solved by the convention was not created by it either. Even so, to summarise in the light of the above, there are three problems in this regard.

- First, states can investigate and take intrusive measures in relation to activities by individuals in another state, even if the activities might not be criminal under the law of that other state (even if the laws in both states claim to give effect to the same provision in the convention). This is increasingly done, in ways that bypass established MLAT arrangements (including the mutual assistance arrangements in the Cybercrime Convention itself).[221] See section 4.5.3 below.

---

218. The Explanatory Report of Protocol 7 notes: "The words 'under the jurisdiction of the same State' limit the application of [Article 4] to the national level. Several other Council of Europe conventions, including the European Convention on Extradition (1957), the European Convention on the International Validity of Criminal Judgments (1970) and the European Convention on the Transfer of Proceedings in Criminal Matters (1972), govern the application of the principle at international level." The European Convention on Extradition (ETS No. 24) provides some protection against double jeopardy, in that it prohibits extradition of a person who has been finally acquitted or convicted of the same act in the requested country (Article 9), but this does not shield such a person from prosecution in another state if he or she ends up in that other state (or in a third state party to the Convention that might extradite him) other than as a result of extradition.
219. Cf. Kaspersen (see n. 217), para. 11.
220. The case of Gary McKinnon was already noted in section 1.2 and note 6, above.
221. As Brown and Korff noted in their report for the GNI (see n. 116), governments in countries with widely varying regimes have threatened legal action and (at least as serious) commercial sanctions like the withdrawal of contracts or licences, against companies that they feel facilitate dissemination of materials that contravene the states' domestic standards, even if the companies are based in another country where the relevant content is not illegal. Sometimes a "word in the ear" of a senior executive can be most effective, even in Western democracies. Cf. M. Anderson, "A sneak peek at a fractured web", *Wired News*, 13 November 2006, at: www.wired.com/news/technology/0,72104-0.html.

- Second, individuals are exposed to a risk of prosecution by states of which they are not nationals, in relation to acts not committed on the territory of those states but in their home country, even if there is comparable legislation in their home country or the country where they committed the relevant acts. The case of McKinnon, just mentioned, is an example.
- Third, as a result, individuals are at risk of being prosecuted more than once for the same offence, in different countries that can claim jurisdiction on the basis of these rules.

From the perspective of the rule of law, there should be limits on the extraterritorial exercise of national jurisdiction in relation to transnational cybercrimes. Issues of "appropriate jurisdiction" and "appropriate forum" should be urgently discussed, with consideration of the effect of substantive limitations to the crime, and of exceptions or defences, in the individual's home country (or the country where the acts were committed) in relation to jurisdiction claimed by other states that do not acknowledge such limitations, exceptions or defences. These issues are especially crucial in relation to free speech, but also arise elsewhere.

### 4.5.4. Lack of safeguards in other respects

Although Article 15 of the Cybercrime Convention says that state procedures relating to the investigation and prosecution of the crimes listed must be in accordance with the ECHR (for Council of Europe member states), or with other international human rights treaties such as the ICCPR (for non-European states such as the USA), it provides no details or guidance on what this entails. Nor can such clarification easily be found in the case law of the European Court of Human Rights, which is by its nature ad hoc. It is particularly difficult to identify precisely, for very different criminal-legal systems, the procedural requirements that flow from the international human rights instruments and must be met to ensure that criminal proceedings (from pre-trial investigation to final acquittal or conviction) are "fair". The result is an obligation on states to criminalise certain activities, that is not counterbalanced by strong obligations and safeguards to ensure respect of human rights instruments in actually applying the criminal law to those activities.

While a complete resolution of this issue would have been difficult to achieve in the context of the convention, some rules and guidance would nonetheless have been valuable. The convention could, for example, have required prior judicial authorisation for certain intrusive investigative measures, such as the use of "special investigative measures" to gather evidence, or restrictions on certain evidence in criminal proceedings.[222] This would seem all the more necessary in view of the fact that the Cybercrime Convention is open to non-Council of Europe member states, which means that there is no firm guarantee that the non-European states that become party to the convention will always meet international fair trial (and fair investigation) standards in their domestic laws and practices – again, also and especially in relation to law-enforcement activities that take place outside the relevant state's territory, or

222. Cf. the UK Crown Prosecution Legal Guidance on *Obtaining evidence and information from abroad* (see n. 237), discussed later in this section.

that have extraterritorial effects in other states; the more so if the state in question (like the USA) does not even accept that it is bound by international human rights law in such regards.[223] Some aspects of this are further discussed in section 4.5.5.

Article 24(6) of the convention allows a state to refuse extradition if that state itself is willing to consider prosecution, but there is no rule on when a state ought to do this. This ties in with the – as we have seen, largely unanswered – question of what is the "appropriate jurisdiction for prosecution" and with the issue of *ne bis in idem*. The convention does not say that a state party should not extradite a person to another state party if this might lead to violations of the fundamental rights of that person (in particular his right to a fair trial), or if the person is a national of the requested state and could also be tried under the law of his home state. For those who have been finally convicted of the relevant offence, this is mitigated by the ban on extraditing these persons, contained in the European Extradition Treaty.[224] However, this treaty has not been signed or ratified by most non-Council of Europe states that are parties to the Cybercrime Convention, including the USA. The ban on extraditing someone who has been finally acquitted or convicted therefore does not apply to them.

On mutual assistance, Article 27(4)(b) of the convention similarly allows a state to refuse assistance if it "considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests", but there is no requirement to refuse assistance if compliance with a request could lead to violations of anyone's human rights (in particular, of course, the rights of any person to whom the requested information relates). Between member states of the Council of Europe, this is mitigated by safeguards in the European mutual legal assistance treaties (MLATs), in particular the European Convention on Mutual Assistance in Criminal Matters (ETS No. 30). However, again, although this convention is open to non-European states, it has not been ratified by the USA or other non-Council of Europe states that are parties to the Cybercrime Convention.

Again, a general human rights clause in the convention could have provided some protection against such wrongs occurring. Such a general provision could have stipulated that all states parties to the convention must fully comply with their international human rights obligations in anything they do (or fail to do) under the convention, be that in defining the relevant crimes (and the elements, exceptions and defences relating to them), in any criminal investigations or prosecutions and in relation to mutual legal assistance and extradition. If the convention is reviewed and amended, such a clause should be added.

## 4.5.5. Investigating crimes in the digital environment

Investigating crimes with a cross-border element is always complex, even without any "cyber" connection; and the national and international rules on such operations are far from comprehensive or clear. From a rule-of-law perspective, it is always preferable if such operations are carried out under an MLAT, in accordance with the rules,

223. See section 3.4.1.

224. The European Extradition Treaty is open to non-Council of Europe member states, and has been ratified by Israel, Korea and South Africa.

procedures and formalities set out in the MLAT. However, in practice more informal means of co-operation are often preferred – and indeed sometimes encouraged, for instance by the United Nations Office on Drugs and Crime (see below).

As explained in section 2.2, the Internet and the wider digital environment are by their nature global and transnational. This poses special problems for criminal investigations. In particular, digital evidence – emails, postings on social networks, files held in digital vaults in the Cloud – will often be in a different country from the country where the relevant crime is being investigated, and may be controlled by a company that has its headquarters in another state. In view of the dominance of US companies in this environment, the company that controls the data will often be in the USA, but in specific situations the investigative agencies may want to obtain data from many countries (for example, they may want data on the location and movements of mobile phones from mobile network operators in all the countries where a suspect or other "target" travelled, or even where contacts of such a suspect or target travelled, to expose criminal networks; or they may want data on payments made in different countries by bank card).

Although the Cybercrime Convention was drafted specifically to deal with crimes committed in this environment, the rules on cross-border disclosures, gathering and sharing of information fail to provide a fully adequate framework, with one core provision apparently applied in ways that were not intended by the drafters.

### Article 26 of the Cybercrime Convention

Thus, first of all, Article 26 expressly allows states parties – or rather, in practice, the police and other investigative bodies of those states – to "spontaneously" pass on information they obtain within the framework of their own investigations to similar bodies in other states parties, if they think the information will be helpful to the other agency. No safeguards, procedures or formalities are stipulated in that regard, other than that the disclosure has to be "within the limits of" the law of the disclosing country – the convention does not require that such cross-border disclosures of data be recorded. The UN Office on Drugs and Crime (UNODC), in a report issued in December 2012, praised Article 26 of the Cybercrime Convention as enabling "informal means of communication and information sharing among the parties of the Convention, even if they do not have such a provision in their national legislation".[225] In other words, at least in the view of this UN agency, law-enforcement bodies can disclose information to similar agencies in other countries as long as this is not expressly forbidden under their national law: Article 26, in this view, itself constitutes an enabling provision to that effect. Since such data disclosures will often constitute an interference in a fundamental right such as the right to privacy (UNODC specifically refers to obtaining data from Internet service providers), this reading of the Cybercrime Convention fundamentally undermines the rule-of-law requirement that such interferences be based on clear, specific domestic legal rules.

225. UNODC, "The use of the Internet for terrorist purposes", September 2012, para. 244. Available at www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

The European Commission, too, has approvingly (albeit somewhat obliquely) referred to informal arrangements for gaining access to data in situations where a formal request would have been granted.[226]

## Article 32 of the Cybercrime Convention

More contentious still is Article 32, which stipulates that relevant bodies in any state party may access data stored on a computer in another state party, without the authorisation of that other party, if the data are "publicly available" or if the party accessing the data "obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system." The latter person will not necessarily be the data subject, but can be a company such as an ISP or a MNO or, these days, a social network provider.[227]

Professor Kaspersen, who was closely involved in the drafting of the Cybercrime Convention, makes clear that Article 32(b) was intended to "allow unilateral transborder activity in a very limited number of cases" only, namely in situations where "volatile data" were at risk of being lost,[228] and where "the person concerned who enables access finds himself within the territory of the investigating party".[229] In general, apart from these limited special cases:

> [S]elf-help of national law enforcement authorities through transborder network searches was not to be made legally possible.[230]

---

226. See European Commission, "Evaluation report on the Data Retention Directive 2006/24/EC". Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF.
227. We focus on this second possibility covered by Article 32(b), where law-enforcement authorities obtain data from companies that feel they have authority to disclose data. The situation covered by Article 32(a), where law-enforcement authorities obtain "publicly available" data, is largely uncontentious. However, there could be problems if this were used by law-enforcement authorities in one country to "pull" complete public registers from another country, to use in data matching and mining for law-enforcement purposes. In Europe, such secondary uses of public register data are not unregulated: on the contrary, the EU Article 29 Working Party has expressly held that, just because data are publicly available, that does not mean they are exempt from data-protection law, and from the purpose-limitation principle in particular. See Opinion 7/2003 on the re-use of public sector information and the protection of personal data – Striking the balance, 12 December 2003 (WP83), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp83_en.pdf.
228. Kaspersen, *Cybercrime and jurisdiction* (cited in n. 217 above), para. 75.
229. Ibid., para. 80. In line with this, para. 294 of the Explanatory Memorandum also suggests that the drafters had in mind law-enforcement authorities in a country asking a person or a company in that same country, but one that happens to have stored data in another country (e.g. on a remote Cloud server), to extract those data from that other country, in circumstances (and subject to the conditions and procedures) in which the person or company in question could also be asked to provide the data if the data had not been stored abroad.
230. Ibid., para. 79. Kaspersen agrees with our view, set out in section 3.6 above, that under traditional international law, investigative acts by states on the territory of another state – including the "pulling" of data from servers in that other state – violate the sovereignty of the latter state, but adds that "Considering the nature and use of international electronic communication structures and other technical facilities a more pragmatic approach could be defended" (para. 77, with reference to the Lotus case).

> The result of the negotiations of the Cybercrime Convention was that transborder investigative activity was not accepted in principle. Instead, [a] system of expedited mutual assistance combined with preliminary measures was chosen.[231]

However, neither of the intended limitations is expressly reflected in the text of Article 32. It does not refer to, and on its face is not limited to, situations in which access is sought to "volatile" data that are in danger of being lost if they are not immediately "pulled" from another country. And the reference in Article 32(b) to cross-border access to data being allowed with "the lawful and voluntary consent of the person who has the lawful authority to disclose" also does not contain the apparently intended limitation that this only applied to "persons" (in practice, generally companies) that are based on the territory of the investigating state.

Unsurprisingly, it appears that in practice "self-help" without recourse to MLATs is increasing – and this is facilitated by a coming together of the absence of the above-mentioned limitations from Article 32(b) with the fact, discussed earlier,[232] that most of the Internet and the digital world – and most of the data in that world – are controlled by private entities, who can effectively give themselves the very "authority" referred to in the article.

Many ISP and MNO terms and conditions of service appear to have been drafted also with this possibility specifically in mind (even if the meaning of the relevant provision may not always be obvious to their customers). For example, the privacy policy of Vodafone UK (as an entirely random example) allows access by "law enforcement agencies, regulatory organisations, courts or other public authorities if we have to, or are authorised to by law" (note the last phrase).[233] O2's terms and conditions stipulate, in an even more convoluted way, that the customer, by entering into a mobile phone agreement, "authorises" O2 to disclose details of their mobile phone use, including their location data, to effectively any "government agency" for, *inter alia*, "fraud and crime detection and prevention and... as required for reasons of national security or [*sic*] under law".[234] The notable point in these terms and conditions (which are typical of most ISPs and MNOs) is that they do not simply say that the company will disclose data to their own domestic law-enforcement agencies as and when required by law, subject to the relevant procedures, conditions and formalities of the relevant domestic law. Rather, they seem to have been drafted with a view to providing the companies in question with "authorisation" to make such disclosures, whenever they (the companies) believe that such a disclosure is useful to the national police or the secret service or some other state agency, and indeed, it would appear, to foreign agencies of that kind.

Article 32 of the Cybercrime Convention can be seen as completing this arrangement in a cross-border context, by seemingly giving law-enforcement agencies the power

---

231. Ibid., para. 89.
232. See section 2.3.2.
233. See www.vodafone.co.uk/about-this-site/terms-and-conditions/automatic-topup/. The quotation is from p. 16 of this 17-page, 7,400-word text.
234. See www.o2.co.uk/termsandconditions/mobile/our-latest-pay-monthly-mobile-agreement. The "authorisation" is provided in section 21.3 on p. 16 of a 19-page, almost 10 000-word text.

to rely on such "authorisations created by terms and conditions" to obtain the data from companies (ISPs, MNOs, but also others such as airlines or banks, though they often have stricter rules in place in this regard, and/or are subject to stricter legal duties of confidentiality) that are outside their own country and thus, normally, outside their jurisdiction.

Such procedures may explain the European Commission's analysis that the reason for the very low proportion of (formal) cross-border requests for retained communications data is that law-enforcement authorities

> prefer to request data from domestic [read: foreign] operators, who may have stored the relevant data, rather than launching mutual legal assistance procedure which may be time consuming without any guarantee that access to data will be granted.[235]

This strongly suggests that many police forces, including European ones (and probably also US ones), do indeed act in accordance with this interpretation of Article 32 and seek access to communications data "informally", across borders, directly from communications services providers in other countries; and that the ISPs and MNOs in question indeed feel that they have "lawful authority" to "consent" to such requests – even in situations where access under an MLAT might well be refused (or would at least be closely scrutinised). Perhaps not coincidentally, such practices also echo the New York judge's ruling in the Microsoft case mentioned earlier, which was rightly criticised by Commission Vice-President Viviane Reding.[236]

This appears to create a situation where cross-border access to personal data by national law-enforcement agencies is becoming effectively unregulated and close to arbitrary.

Some countries attempt to at least lay down some restrictions on such practices. The UK Crown Prosecution Service, for instance, provides the following "Legal Guidance" on "International Enquiries" and "Mutual Legal Assistance".[237] This guidance first acknowledges that

> it is not always necessary for a prosecutor to issue a [formal] MLA request in order to obtain evidence and information in the prosecution phase. Evidence can often be obtained via other [informal] forms of co-operation.

However, it then makes a useful distinction:

> As a general rule, requests for evidence which require a judicial oversight and/or involve a degree of coercion or invasion of privacy usually require a [formal] letter of request [issued under an MLAT], as otherwise they are likely to be refused. If a judicial order would be required to obtain evidence in the UK it is likely that it would also be required in the majority of other countries. In these circumstances a letter of request to a judicial authority with the power to order the coercive measure would be appropriate.

---

235. European Commission, "Evaluation report on the Data Retention Directive 2006/24/EC". Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF.
236. See section 2.2.2 and note 25 above.
237. CPS: *Obtaining evidence and information from abroad*, available at: www.cps.gov.uk/legal/l_to_o/obtaining_evidence_and_information_from_abroad/.

As can be seen, the guidance makes this difference for pragmatic reasons ("as otherwise [requests] are likely to be refused"). However, underneath this is a serious principle: that in many if not most states under the rule of law, collecting of information in criminal cases is subject to important procedures and formalities that constitute fundamental protections in such a state under the rule of law. The above guidance therefore also reflects the consideration that cross-border enquiries in criminal proceedings should not bypass the formal conditions imposed on domestic law-enforcement agencies.

The bypassing of such formal conditions and protections is said to be the main reason why certain states have not signed up to the convention.[238] At the Octopus Conference on Co-operation against Cybercrime (Strasbourg, 4-6 December 2013), there was broad support for further policy development with regard to the best ways of dealing with this issue.[239] At that event, Markko Künnapu, chair of the Cybercrime Convention Committee (T-CY) explained that discussions have been under way on cross-border access since 2010, followed by a questionnaire and analysis of different approaches to Article 32b. Subsequently, a sub-group on access to data and jurisdiction was established in November 2011. A year later, the T-CY adopted the sub-group's report and asked it to prepare a draft guidance note on transborder access to data and draft elements of "the" additional protocol to the convention. Finally, in June 2013, it was agreed to commence drafting a second additional protocol to the Cybercrime Convention on transborder access.[240] The details of this protocol will be of crucial importance to ensuring the rule of law in the digital world in relation to law-enforcement investigations. It will therefore be essential that human rights and civil society groups and experts be closely involved in the drafting.

In this context, it should also be reaffirmed that if any state party takes actions that affect individuals outside its territory, this does not exempt that party from those obligations but rather, on the contrary, those obligations equally apply to such extraterritorial acts.[241] The protocol could perhaps also clarify, in binding legal terms, how the difficult issues of "applicable law", "appropriate jurisdiction" and "appropriate forum" should be resolved in relation to cybercrime.

Finally, it should be noted that the Cybercrime Convention deals with criminal-legal matters and criminal policy matters (only).[242] While its provisions would appear to

238. But note that the very inclusion of this article in the treaty confirms that direct cross-border access to data held in another country, without the consent of the targeted country, is contrary to international law: for the parties to the Convention, this article arguably constitutes such consent; but states that are not a party cannot be deemed to have consented. See section 3.4.1, above.

239. On the conference, see www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2013/Octopus2013_en.asp.

240. See www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/Presentations/Plenaryl/Kunnapu_Octopus_2013_TCY_update.pdf.

241. See section 3.4.1, above.

242. Cf. the third preamble to the Cybercrime Convention: "Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation". Cf. also the terms of reference of the committee charged with drafting the Cybercrime Convention, set out in para. 11 of the Explanatory Memorandum.

be inapplicable to other matters like intelligence operations aimed at countering threats to national security, as noted in section 1.2 above and section 4.7 below, in practice it is increasingly difficult to keep these matters separate and balance them appropriately against each other, and states are increasingly inclined to merge or at least closely link the two.[243]

### 4.5.6. Conclusion

The overall assessment of the Cybercrime Convention from the point of view of the rule of law in the digital environment is mixed. On the one hand, an instrument of this kind is needed to counter crime in the global digital environment – cybercrime. On the other hand, as it stands, the convention does not fully ensure compliance with the rule of law in its implementation by states parties.

The main reason for this is the absence of a comprehensive human rights clause. As a result of this omission, the convention does not provide protection against states imposing unduly wide criminal offences, or failing to include exceptions or defences in their substantive law (such as a public interest defence for whistle-blowers); it does not protect against double jeopardy, or the provision of (formal or informal) assistance to states parties when this could violate human rights; and it fails to provide clear, human rights-compatible guidance on "applicable law", "appropriate jurisdiction" and "appropriate forum".

Another reason why the convention does not fully ensure compliance with the rule of law is the absence of any linkage to other major instruments developed by the Council of Europe supporting the rule of law in digital and/or transnational contexts. Such linkage is necessary because the Cybercrime Convention is open to states that are not party to the European Convention on Human Rights (ECHR) or that have not fully accepted the comparable requirements of the International Covenant on Civil and Political Rights (such as the USA in respect of its extraterritorial activities or the rights of "non-US persons"). From the perspective of the rule of law in Europe, states should only have been allowed to join the Cybercrime Convention if they had fully accepted their obligations under the ECHR and/or ICCPR, and if they were already (or became) party to the Data Protection Convention, the European Extradition Convention and the European Convention on Mutual Assistance in Criminal Matters.

Finally, Articles 26 and 32 of the convention have been interpreted in such a way as to support the tendency of law-enforcement agencies to resort to "informal" means of information-gathering for law-enforcement purposes, even across borders, without laying down clear safeguards in that respect (e.g. that such informal measures should not be used for intrusive information gathering that would normally, within a state under the rule of law, require a judicial warrant); and the tendency of such authorities to increasingly "pull" data directly from servers in other countries, or to demand that companies within their jurisdiction – in particular the main "Internet giants" – do this for them, without recourse to formal, inter-state

243. On the example of the FBI, see note 9.

mutual legal assistance arrangements, arguably in violation of the sovereignty of the state where the data are found.[244] This too undermines the rule of law on the Internet and in the wider digital environment.

It is to be hoped that the drafting of the proposed new additional protocol to the Cybercrime Convention will provide an opportunity to resolve at least some of these issues.

## 4.6. National security

The ECHR and the Council of Europe Data Protection Convention apply to all activities of the states that are party to them; although there are some special rules and exceptions in both of them, as noted below, issues of national security are not simply excluded. In this, the mandate of the Council of Europe and the scope of these instruments differ from EU law, which expressly excludes national security from the competence and jurisdiction of the Union.[245]

This means that, when it comes to the international legal regulation of the activities of national security and intelligence agencies, the Council of Europe must take the lead role, if not globally then at least in Europe.

### The "rule of law" tests

The basic parameters are clear: whenever a state acts in a way that affects ("interferes with") the human rights of individuals who come within its jurisdiction or power, that interference has to be based on "law"; the law in question has to meet the relevant "quality" requirements (clear, specific, accessible, etc.); the interference must serve a "legitimate aim" (and national security is such an aim in most, but not all cases); the interference must be "necessary" and "proportionate" to the aim in question (within a "margin of appreciation"); and the individuals affected must have an "effective [preferably judicial] remedy" available to them. The state in question may also not discriminate in this, for instance, against non-nationals or non-residents (unless there is an "objective reason" to make a distinction).[246]

The crucial point here is that, in terms of international human rights law, apart from times of war or public emergencies threatening the life of the nation, these basic "rule of law" tests apply not only to actions by a state's law-enforcement agencies (as is generally recognised) but also to any actions by a state's national security and

244. See section 3.6, above.

245. As Article 4(2) of the Treaty on European Union puts it: "[N]ational security remains the sole responsibility of each Member State." For discussion of this exclusion and its limits, see Douwe Korff, "Surveillance and the EU general data protection regulation: possibilities, limits and obstacles", *Datenschutz Nachrichten* 4/2013 (December 2013), pp. 150-4 (not available online), and the author's Expert opinion provided to the German Bundestag Committee of Inquiry into this matter (see n. 171).

246. See the various sub-sections on these issues in section 3, above.

intelligence agencies.[247] Of course, in specific contexts, limitations of or restrictions on basic rights may sometimes be justified as "necessary" and "proportionate" to protect national security even if they go beyond what may be "necessary" and "proportionate" for appropriate law-enforcement activities. However, this is always a matter for legal judgment: "national security" is, in European and international human rights law, not a card that trumps all other considerations. Indeed, the very question of what legitimately can be said to be covered by the concept of "national security" is justiciable.

On the latter point – what can legitimately be said to be covered by the concept of national security – the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, drafted by the NGO Article 19 but endorsed by various international forums including the UN Special Rapporteur on Freedom of Opinion and Expression, provide useful guidance.[248] These principles make clear that states can only invoke national security as a reason to interfere with human rights in relation to matters that threaten the very fabric and basic institutions of the nation.[249] Sometimes, terrorism can reach this level, but in most cases it is a phenomenon that should be dealt with within a law-enforcement paradigm rather than a national security paradigm. States that want to interfere with fundamental rights on the basis of an alleged threat to national security must demonstrate that the threat cannot be met by means of ordinary criminal law, including special anti-terrorist laws that still fit within the accepted parameters of criminal law and procedure and that meet international standards for criminal law and procedure. This also applies to state actions that affect the Internet or e-communications. Failure to abide by this requirement violates the international rule of law.

The need to secure the rule of law in relation to the activities of national security and intelligence agencies has become obvious in the light of the revelations of Edward Snowden, in particular about the global surveillance operations of the USA's National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ) and their partners in the 5EYES group (Australia, Canada and New Zealand). Those revelations have shown that these agencies routinely tap into the high-capacity fibre-optic cables that form the backbones of the Internet, and also intercept mobile

---

247. We do not discuss in this Issue Paper the rules that might apply to actions by a state in times of war or national emergency, though some US politicians have used terminology that appears to invoke an "armed conflict" paradigm to justify the USA's global surveillance operations. Here it must suffice to note that, for European states and the USA, except in the immediate aftermath of "9/11", this is not an appropriate paradigm for current actions, particularly for surveillance in Europe. See Anne Peters, *Surveillance without borders? The unlawfulness of the NSA-Panopticon, Part I,* available at www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/. More specifically, no state has formally declared such an emergency (as required under Article 4(3) ICCPR) or formally derogated from its human rights obligations (under Article 15 ECHR); and none can therefore at present invoke the special exemptions or derogations. See also again Douwe Korff's *Expert opinion* for the German Bundestag Committee of Inquiry (see n. 171).

248. Available at: www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf. See also Sandra Coliver, "Commentary on the Johannesburg Principles on National Security, Freedom of Expression and Access to Information", in *Secrecy and liberty: national security, freedom of expression and access to information*, The Hague: Martinus Nijhoff 1999, available at www.right2info.org/exceptions-to-access/resources/publications/CommentaryontheJohannesburgPrinciples.pdf.

249. See Coliver, "Commentary" (n. 248), particularly the section on "Components of a legitimate national security interest".

and other communications worldwide on a massive scale by, *inter alia,* intercepting radio communications, using "backdoors" they have installed in major communications systems or exploiting security weaknesses in such systems.

The Political Declaration adopted at the Council of Europe Conference of Ministers in Belgrade in 2013 explained what is at stake very clearly, stating that,

> given the growing technological capabilities for electronic mass surveillance and the resulting concerns, we emphasise that there must be adequate and effective guarantees against abuse which may undermine or even destroy democracy.[250]

The same meeting adopted Resolution No. 1, which called on the Council of Europe to "examine closely" the "deliberate building of flaws and 'backdoors' in the security system of the Internet or otherwise deliberately weakening encryption systems."[251]

## The legal basis of actions of security and intelligence agencies

One particular concern in this regard is the lack of clear legal rules governing the actions of national security and intelligence agencies in many countries, and especially the treaty rules that are the basis of their operations and exchange of data. In many countries, there are few clear, published laws regulating the work of these agencies. In some, there are no published rules at all (in the UK, the very existence of the secret services was unacknowledged until the late 1980s); in many more, there is at most a broad, vague legal basis that does not allow citizens – let alone foreigners – to foresee, with reasonable accuracy, how and when the secret services might use their powers against an individual. In the USA, as we have seen, agencies often operate on the basis of rules, or interpretations of rules, that are kept secret. Another serious concern is the ineffectiveness of many supervisory systems.

In addition, international co-operation between the national security and intelligence agencies of certain countries – under which extensive data collection and data-sharing appears to be taking place, especially in relation to the Internet and electronic communications – has been largely based on secret treaties such as the UK–USA treaty of 1946, since amended and extended to Australia, Canada and New Zealand (now jointly known as 5EYES) and only made public a few years ago.[252] The

---

250. See www.coe.int/t/dghl/standardsetting/media/belgrade2013/Belgrade%20Ministerial%20Conference%20Texts%20Adopted_en.pdf.

251. Ibid.

252. For the original text, see www.nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf. For background and extensive documentation, see www.nsa.gov/public_info/declass/ukusa.shtml but note that this is still incomplete; some (many?) documents relating to 5EYES arrangements, including subsidiary agreements or guidelines, remain secret. The principle that 5EYES countries (initially, the USA and UK) would not spy on each other may be derived from the clarification in footnote 3 to the 5 March 1946 text, which says that "the U.S., the British Commonwealth of Nations, and the British Empire" shall not be regarded as "foreign countries" and that their communications therefore do not constitute "foreign communications". Note that one word was deleted from the declassified text: the word may well be "diplomatic". If so, that suggests that diplomatic communications in countries outside the 5EYES were (still are?) specifically targeted under the treaty – contrary to international law and thus also in breach of the rule of law.

Western Allies similarly imposed detailed secret treaties on the Federal Republic of Germany at the end of the Second World War occupation period.[253] Little is known of other treaties, let alone of additional or subsidiary agreements or annexes to them, but they appear to be widespread among Western states.

In fact, the activities of these agencies were largely excluded from public discourse throughout the Cold War. While perhaps politically understandable, this flouted the principle of "law" in European and international human rights law. In view of the fact that (as discussed in section 1.2 above) the activities of law-enforcement agencies and secret services are becoming increasingly intertwined, particularly (but not only) in relation to terrorism, this legal vacuum can no longer be ignored.

It is axiomatic in terms of modern human rights law that all activities of national security and intelligence agencies of nation states must be brought within the rule of law, just as it is accepted that all activities of law-enforcement agencies must be within the rule of law. As a first step, the Council of Europe could seek full disclosure of all laws, subsidiary rules and treaties that cover the activities of these agencies and services in all member states, and it should support efforts by broader international organisations such as the UN to do the same beyond Europe, in particular in relation to the USA.

Under Article 52 of the ECHR, the Secretary General of the Council of Europe has the right to initiate an "inquiry", under which all states parties (that is, all member states of the Council of Europe) can be required to provide such information. This would appear to be an appropriate way to collect the texts of the relevant laws, rules, rulings and treaties.

Until we know the rules under which the national security and intelligence agencies operate – in detail, domestically, extraterritorially and/or in co-operation with each other – their activities cannot be said to be in accordance with the rule of law.

Given the increased partnerships between law-enforcement and national security agencies, this negation of the rule of law threatens to spread from the latter to the policemen and prosecutors. This trend is most (although not only) apparent in Internet surveillance, interception and analysis of electronic communications, and the use of malware by these agencies to access personal computers and mobile devices. Co-operation between law-enforcement agencies and national security agencies can only happen under the rule of law if both agencies act in accordance with rule-of-law principles. The absence of clear legal frameworks in this regard, domestically and internationally, is a further threat to the rule of law on the Internet and in the global digital environment.

---

253. Joseph Foschepoth, *Überwachtes Deutschland*, 3rd edn, 2013, chapter 2. The German text of the Memorandum of Understanding between the Western allies and the young FRG (full English title: "Agreements affecting the Intelligence Situation in Germany after the Termination of the Occupation", 11 May 1955, ref. NACP, RG 84) can be found on pp. 291-2. It was only declassified in recent years.

## 4.7. The delicate (and unresolved) balances

### 4.7.1. Tensions between data protection, law enforcement and national security

It is clear from the analyses in the previous sections that there are tensions between data protection, law enforcement and national security.[254] This is reflected in the general tensions between the Council of Europe Data Protection Convention and its Cybercrime Convention, and also in the special context of suspicionless compulsory retention of communications data.

#### Data protection, law enforcement and national security generally

In Article 9(2), the Council of Europe Data Protection Convention reflects the limitation paragraphs in the main, general human rights treaties, by allowing for exceptions to, *inter alia*, the core data-protection principles (including purpose limitation, data minimisation and data-retention limitations), when this is

> provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:
> a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; [or]
> b. protecting the data subject or the rights and freedoms of others.

This of course begs the question of what limitations or interference can be said to be "necessary" and "proportionate". The Data Protection Convention gives little guidance on this, except in the important Article 16, which deals with "refusal of requests for assistance" and makes clear that data-protection authorities may refuse to collect or pass on personal information to other DPAs, at the request of such other DPAs, if:

> a. the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;
> b. the request does not comply with the provisions of this convention; [or]
> c. compliance with the request would be incompatible with the sovereignty, security or public policy (*ordre public*) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

The Explanatory Report adds that:

> The term "compliance" which is used in littera c should be understood in the broader sense as covering not only the reply to the request, but also the action preceding it. For example, a requested authority might refuse action not only if transmission to the requesting authority of the information asked for might be harmful for the fundamental rights of the individual, but also if the very fact of seeking the information might prejudice his fundamental rights.

These arrangements underline the problem with Article 32 of the Cybercrime Convention. In the broader context of general data-protection rules, Article 16 of the

254. See sections 1.2 and 4.6, above.

Data Protection Convention shows that the obtaining, by a public authority in one country, of personal data on an individual in another country can be highly sensitive, and will affect both the sovereignty of that other country and the fundamental rights of the data subjects in that other country. Article 16 of the Data Protection Convention therefore quite rightly allows for the latter country to refuse to allow such data to be collected and/or passed on to the first country, if that would be incompatible with its (the latter country's) sovereignty or *ordre public* (which of course includes its constitutional order), or if the collecting or disclosure would prejudice the data subject's fundamental rights. In this context, it is worth pointing out that the Data Protection Convention does foresee derogations to Articles 5 (quality of data), 6 (special categories of data) and 8 (additional safeguards for the data subject) for a narrow range of purposes, including the "suppression of criminal offences".

The principle that there are clear limitations to the circumstances in which personal data may be collected and/or passed on, spontaneously or at the request of another country, should therefore also inform the Cybercrime Convention. Yet the only references to such limitations in the Cybercrime Convention are in its preambles, which state that, in drawing up or acceding to the convention, the states parties to the convention were "mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties" and "mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"; and that they "recall[ed]" various Council of Europe Committee of Ministers' recommendations. But being "mindful" of or "recalling" such recommendations is not the same as requiring full compliance with them, as illustrated by the UNODC analysis referred to earlier.[255]

In fact, Article 32 of the Cybercrime Convention appears to allow complete bypassing of the kinds of crucial safeguards envisaged in Article 16 of the Data Protection Convention in relation to mutual assistance between DPAs: in this article, the Cybercrime Convention appears to implicitly envisage the cross-border collection and extraction of personal data by law-enforcement agencies, irrespective of whether this is "compatible with the sovereignty, security or public policy (*ordre public*)" of the state where the data are held or with "the rights and fundamental freedoms of persons under the jurisdiction of [that other country]", as defined in the constitution or laws of that other country. Of course, the roles of DPAs and law-enforcement agencies such as the police are different – but the principle that in transnational activities of either kind of agency – or for that matter any state agency – the targeted country should be able to prevent actions of foreign agencies on its territory or affecting its citizens if there are reasons to believe that those actions are incompatible with its public policy should surely be applied to both.[256]

255. See section 4.5.3.

256. See the quotation from Vaughan Lowe in section 3.6.

The suggestion made at the 2013 Octopus Conference that it was time to reconsider the article and to address the matter of cross-border access to personal data between states parties in a new protocol or other binding international (Council of Europe) instrument should therefore be supported.[257] That instrument should at least contain an exception clause similar to Article 16 of the Data Protection Convention.

## Recommendations of the Committee of Ministers

The Council of Europe Committee of Ministers' recommendations referred to in the preamble to the Cybercrime Convention also deserve further attention, along with some of its later recommendations and declarations.[258] In several respects, they provide useful guidance, albeit still limited, on how to strike the balance between upholding data-protection principles and allowing or enabling appropriate law enforcement. Of particular importance is Recommendation No. R (87) 15, regulating the use of personal data in the police sector. This recommendation has become part of the "hard" law of EU police and judicial co-operation arrangements, and has become the central instrument in Europe in this field.[259] It too is currently under review.

We note also Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, and the 2013 Declaration of the Committee of Ministers on risks to fundamental rights stemming from digital tracking and other surveillance technologies. These and other relevant recommendations and declarations in effect spell out what the rule of law requires in terms of data protection in relation to law enforcement and other access to data on the Internet and the wider digital environment, and in relation to the use of the thus-obtained data.

Compliance by their law-enforcement agencies with Recommendation No. R (87) 15 (or its successor, provided this does not reduce protection), Recommendation CM/Rec(2010)13, the Committee of Ministers' Declaration on tracking and surveillance, and other relevant existing and future standards set by the Committee of Ministers, as well as ratification of the Convention No. 108, should be preconditions for states wishing to join the Cybercrime Convention. Failure of states – including states parties

257. See section 4.5.3.

258. The Cybercrime Convention's preamble mentions: Committee of Ministers Recommendation No. R (85) 10 on the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for interception of telecommunications; Committee of Ministers Recommendation No. R (88) 2 on piracy of copyright and neighbouring rights; Committee of Ministers Recommendation No. R (87) 15 regulating the use of personal data in the police sector; Committee of Ministers Recommendation No. R (95) 4 on protection of personal data in telecommunication services, with particular reference to telephone services; Committee of Ministers Recommendation No. R (89) 9 on computer-related crime, providing guidelines for national legislatures on the definition of certain computer crimes; and Committee of Ministers Recommendation No. R (95) 13 on problems of criminal procedural law connected with information technology.

259. See the discussion of the EU's police and judicial co-operation agreements in the previous issue paper on protecting the right to privacy in the fight against terrorism, 2008 (see n. 167), section 5.2. This includes the Schengen Agreement and other EU JHA agreements that expressly require compliance with Recommendation No. R (87) 15.

to the Cybercrime Convention – to adhere to these standards undermines the rule of law on the Internet and in the wider digital environment, and is likely to violate international human rights law.

The fact that the legal frameworks for law-enforcement agencies, on the one hand, and national security and intelligence agencies, on the other, are increasingly blurred also undermines some of the rules in Recommendation No. R (87) 15, in particular the principles that "personal data collected and stored by the police for police purposes should be used exclusively for those purposes" (Principle 4) and that "communication of data to foreign authorities should be restricted to police bodies" and take place on the basis of "a clear legal provision under national or international law" (Principle 5.4(a)). The exceptions to these rules are very limited and must normally also be based on "a clear legal obligation or authorisation" or on "authorisation of the supervisory authority [the country's DPA]" (Principle 5.2.i), or at least may not be "contrary to the legal obligations of the communicating body". Although the recommendation makes some provision for disclosures beyond the above, even in the absence of "clear legal provisions", this is limited to highly exceptional cases when this is "necessary so as to prevent a serious and imminent danger" (Principles 5.2.ii.*b* and 5.3.ii.*b*)

These rules are far from perfect: they leave too much scope for evasion of the restrictions on the basis of the rather broadly phrased exceptions. But they are in danger of being totally ignored in the new context of overlapping powers and activities of law-enforcement and national security agencies in relation to the Internet and global communications.

The aim should not be to extend the lawlessness of the secret services to the actions of the police agencies (as is happening), but instead to bring both national security and intelligence agencies and law-enforcement agencies under a firm framework of law, compatible with international human rights and data-protection standards.

To this end, the rules in Recommendation No. R (87) 15 and in other relevant Committee of Ministers' recommendations should be reviewed in relation to law enforcement and national security activities, and amended and improved in that regard, in the context of both the review of Recommendation No. R (87) 15 and consideration of a possible new additional protocol to the Cybercrime Convention. The Council of Europe has, in the Data Protection Convention and the recommendations adopted under it, provided the initial, basic principles on which the rule of law can be introduced on the Internet and in the wider digital environment – provided that these instruments are strengthened and much more closely integrated with and into the Cybercrime Convention, and provided that the activities of national security and intelligence agencies are brought within such an overarching, integrated legal framework.

## Data protection and suspicionless data retention

Basic data-protection principles are also undermined by compulsory suspicionless untargeted retention of communications data "just in case" those data might be

helpful later in a criminal investigation. This practice was imposed in the EU by the Data Retention Directive.[260] As noted in a Council of Europe publication:[261]

> [Compulsory suspicionless, untargeted retention of communication records] "just in case" the data might be useful in some future police or secret service enquiry … ought to be viewed as mass surveillance of citizens without due cause: a fundamental departure from a basic principle of the rule of law.

It is also fundamentally contrary to the most basic data-protection principles of purpose limitation, data minimisation and data-retention limitation.

This issue is seriously aggravated by the fact that even metadata (i.e. recording what links and communications were made in the digital environment, when, by whom, from what location, etc.) can be highly sensitive and revealing, often exposing, for instance, a person's race, gender, religious beliefs, sexual orientation or political and social affiliations.[262]

What is more, extensive research has failed to show any significant positive effect on clear-up rates for crime, and especially not for terrorism-related crime, as a result of compulsory data retention.[263]

Civil society has strongly and convincingly argued for the replacement of suspicionless data retention by data preservation (also referred to as quick-freeze of data), making it possible for law-enforcement agencies to obtain an order requiring e-communications companies and the like to retain the communications data of people when there are factual indications that it may be helpful to the prevention, investigation or prosecution of crimes, with urgent procedures allowing for the imposition of such a measure without delay in appropriate cases, subject to *ex post facto* authorisation.[264]

Not surprisingly, laws introducing compulsory suspicionless data retention have been held to be unconstitutional in several EU member states, including Germany,

---

260. 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 L.105, p. 54ff. As the title shows, technically this amends the e-Privacy Directive (Directive 2002/58/EC).
261. Korff and Brown, "Social media and human rights", chapter 6 in *Human rights and a changing media landscape* (Council of Europe 2011), p. 184.
262. See the expert witness statement of Prof. Edward Felten in the case of *ACLU vs. the NSA et al.*, at https://www.documentcloud.org/documents/781486-declaration-felten.html. The Article 29 Working Party opinion on surveillance, noted below, also refers to the Felten statement and usefully adds further references to judgments of the European courts stressing that metadata are equally protected under European human rights law as is content: Article 29 WP Opinion 04/2014 (see n. 269), pp. 4-5.
263. *Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten*, Max Planck Institute for Comparative and International Criminal Law, 2nd enlarged report, prepared for the German Federal Ministry of Justice, July 2011, at www.bmj.de/SharedDocs/Downloads/DE/pdfs/20120127_MPI_Gutachten_VDS_Langfassung.pdf?__blob=publicationFile.
264. See the Shadow evaluation report on the Data Retention Directive (2006/24/EC), produced by EDRi in April 2011, available at www.edri.org/files/shadow_drd_report_110417.pdf.

with the Constitutional Court of Romania holding the very principle to be incompatible with fundamental rights.[265]

In April 2014, the Court of Justice of the EU similarly held that the Data Retention Directive violated basic principles of the EU Charter of Fundamental Rights and was invalid *ab initio*.[266] The CJEU criticised in particular the untargeted nature of the retention measures:

> Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime....
> Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.[267]

Such untargeted compulsory data retention may therefore no longer be applied under EU law, or under national laws implementing EU law. Since most national data-retention laws explicitly do exactly that, they will all have to be fundamentally reviewed and replaced with targeted surveillance measures.

Two points are worth noting after this important ruling. First, the CJEU described the legislation as a "particularly serious interference with those fundamental rights in the legal order of the EU". Despite this and despite the court's indication in 2007[268] that

---

265. Eleni Kosta, "The way to Luxembourg: national court decisions on the compatibility of the Data Retention Directive with the rights to privacy and data protection", *Scripted*, Vol. 10 No. 3 (October 2013), p. 339ff, at http://script-ed.org/wp-content/uploads/2013/10/kosta.pdf. The Romanian Constitutional Court decision can be found at www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf and an unofficial translation at www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf (sources taken from Kosta).

266. Judgment of the Court of Justice of the European Union in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014, available at: http://curia.europa.eu/juris/documents.jsf?num=C-293/12. This follows the opinion of the Advocate-General, who had concluded that the Directive "as a whole" was invalid and in violation of the Charter: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=145562&occ=first&dir=&cid=218559.

267. Judgment in Joined Cases C-293/12 and C-594/12 (cited in n. 267), paras. 58-59. The court also criticised the lack of clarity over what constitutes "serious crime".

268. Opinion on the Promusicae/Telefónica de España case from Advocate General Kokott, who pointed out that "there is reason to doubt, whether storing of personal data of all users – quasi on stock – is compatible with fundamental rights, in particular as this is done without any concrete suspicion", *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, case C-275/06, 29 January 2008. See Juliane Kokott, "Data retention – a critical side note by the Advocate General", available at www.libertysecurity.org/article1602.html.

the legality of the legislation was questionable, it took eight years for the directive to be overturned. It is also important to consider that the case only reached the CJEU as a result of a legal action taken by small NGOs whose very existence was threatened by the possibility of costs being awarded against them.

Second, since the ruling, member states have seemed to prefer to seek justifications to retain this serious interference with fundamental rights rather than repeal their national legal instruments transposing the directive.

Two days after the CJEU judgment, the EU Article 29 Working Party that advises on the interpretation and application of EU data-protection law issued its own opinion on state surveillance over electronic communications data, in which it cross-referred to the CJEU judgment:[269]

> From its analysis, the Working Party concludes that secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security. Restrictions to the fundamental rights of all citizens could only be accepted if the measure is strictly necessary and proportionate in a democratic society.

The CJEU judgment and the Article 29 Working Party opinion came less than two weeks after the Human Rights Committee issued its concluding observations on the latest periodic report under the ICCPR by the USA, in which it took the same view and called upon the country to "refrain from imposing mandatory retention of data by third parties".[270]

In sum, compulsory retention of communications data is fundamentally contrary to the rule of law, incompatible with core data-protection principles and also ineffective. The EC Data Retention Directive and all national data-retention laws should be repealed and replaced by data-preservation laws.

### 4.7.2. Privatised law enforcement

It is an unquestioned principle of international human rights law that restrictions on fundamental rights and freedoms must be prescribed by "law" – that is, they must be in accordance with a specific and predictable legal framework. There is a significant and valuable body of European Court of Human Rights case law in this context.[271]

---

269. EU Article 29 Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes (WP215 of 10 April 2014), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf. The opinion did not deal with "cable bound interception of personal data", i.e. with the alleged diversion of "full stream" data from the major high-capacity fibre-optic cables that are part of the backbone of the Internet. Rather, it focused on access to precisely the kind of data – metadata – that are the main object of European data-retention laws, and on the CJEU judgment. The cross-reference to (and brief summary of) the CJEU judgment is on p. 5.
270. Human Rights Committee, Concluding observations on the fourth report of the United States of America (see n. 98), para. 22(d).
271. See section 3, above.

However, the private nature of most of the digital public space is putting this basic concept under threat. Many private companies choose to place restrictions on what happens on their Internet platforms, some are encouraged or coerced to place restrictions by governments that either do not want to legislate for whatever reason or cannot legislate because of constitutional or international law restrictions. Similarly, weak liability protections for intermediaries (such as the increasingly out-of-date EU E-Commerce Directive, 2001/31/EC) and injunctions imposed by courts on intermediaries that do not specify how the injunction is to be implemented (such as the Telekabel case in the European Court of Justice)[272] can provoke intermediaries to impose restrictions on freedom of communication that have not been tested for effectiveness or proportionality and which do not have the predictability of "law".

There are four key questions by which enforcement or other restrictions need to be assessed.

- To what extent have the restrictions been directly or indirectly brought about by government actions (pressure in the press, direct pressure on the company involved, legislative pressure through, for example, weak liability protections or strong contributory liability obligations)? How much state involvement is needed for the intermediary's action to be considered to entail state responsibility?
- When measures are not directly imposed by the state but, typically, through a company's general terms and conditions, how can redress be accorded to the individual(s) whose rights have been restricted? In principle, they agreed to the terms of service of the service provider (assuming that they are a customer) and the state was not directly involved. The practical barriers to redress appear to be very significant.
- Where measures fall below the threshold for state responsibility, what are the state's responsibilities to ensure that private measures respect human rights? Is there a broad obligation to ensure that terms of service are sufficiently clear? How much competition does there need to be, for there to be adequate alternative means of communication? What are the obligations of large Internet access providers in respecting fundamental rights of non-users? For example, taking the widespread blocking reported by Open Rights Group into account,[273] can it be assumed that the clients of the ISPs knew that they were signing up to such a high level of blocking, particularly of often innocuous material? Does the restriction of the freedom to impart information of the blocked websites necessitate state action to redress this problem?
- Insofar as, for whatever reason, the intermediary is imposing restrictions in order to achieve specific (and, indeed, legitimate) public policy goals, how can measures be developed that are, in fact, necessary, effective, proportionate and subject to the kind of scrutiny that a democratic process would normally produce? The "voluntary" informal child pornography blocking systems in place in some EU countries were introduced without any assessment of

272. Cf. note 178 and the discussion in section 4.2.

273. See www.openrightsgroup.org/press/releases/orgs-blocked-project-finds-almost-1-in-5-sites-are-blocked-by-filters.

effectiveness (or risk of counter-productive results) and, despite being in existence for nearly ten years in some cases, have never been subject to any serious review. This approach appears to fail on all fronts, particularly in regard to respect for the rule of law and basic diligence when dealing with activities that are serious crimes, as defined, *inter alia,* by the Cybercrime Convention.

Andrei Soldatov, a security and information technology expert, has described the restrictive effects of the measures to regulate blogging and social media sites, and to extend blocking measures, in a way that neatly illustrates many of the issues that need to be addressed, not only in Russia and but also in jurisdictions that, on the surface, appear to be far less restrictive:

> The people working for these companies become frightened of what could happen and start being cautious, they start voluntarily cooperating with the authorities.... In other words, the control of the Russian Internet is done, to a big extent, through self-censorship, which grows exponentially in the absence of well-defined rules.[274]

Urgent consideration needs to be given to the range of complex issues arising from the role of private intermediaries in the online "public" environment, in order to ensure that basic principles of human rights can be preserved in the online environment. If, as the Council of Europe has repeatedly declared, people should enjoy the same rights (of privacy, freedom of expression, etc.) online as they do offline, then actions by private-sector entities (which dominate the digital world) that affect the exercise and enjoyment of those rights should be subject to clear regulation too.

274. Committee to Protect Journalists, "Russia intensifies restrictions on blogs, social media", http://cpj.org/blog/2014/07/russia-intensifies-restrictions-on-blogs-social-me.php.

We exercise a significant part of our human rights today using the Internet and the wider digital environment. But our human rights can also be breached using these very same means.

There is general agreement that human rights should be enjoyed online as they are offline. In practice, however, the actors who can ensure that we enjoy human rights are not exactly the same in the two environments. In particular, the disproportionate influence and control that certain states and certain private companies exercise on the Internet and its physical infrastructure at the global level, are two essential elements of this difference.

This issue paper looks at how the rule of law can be maintained in an environment characterised by these specific governance issues, focusing on some policy areas of particular human rights relevance: freedom of expression, data protection and privacy, cybercrime and national security. It suggests possible ways forward to ensure that we can trust the rule of law to apply to our online activities.

**www.commissioner.coe.int**

PREMS 70114 ENG

ENG

**www.coe.int**

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, 28 of which are members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE