Routledge Research in Human Rights Law

HUMAN RIGHTS, DIGITAL SOCIETY AND THE LAW

A RESEARCH COMPANION

Edited by
Mart Susi

ROUTLEDGE

17 Digital security and human rights

A plea for counter-infringement measures¹

Mireille Hildebrandt

Introduction

We are often told that we must sacrifice some of our liberties to gain security. Though this is usually explained as a matter of balancing liberty against security, it actually refers to a trade-off, not a balance. The idea of balancing would imply that whenever we increase the security measures that violate our liberties, we must also increase the safeguards, to regain a balance. In this chapter, I focus on the fundamental rights infringements generated by digital security technologies and investigate what is meant when the image of the scale is invoked. The latter raises two questions. First, whether we must necessarily trade liberty against security, including the question of whether giving up liberty necessarily results in more security. Second, what type of balancing is required whenever a trade-off is inevitable? Finally, I will argue that the balancing act requires checking for an adequate implementation of counter-infringement measures.

In the next section, I discuss the difference between security and safety and its relevance for digital security technologies (DSTs). After that, three types of DSTs will be discussed: those safeguarding access and confidentiality, those involved in monitoring, filtering and blocking of data and systems. I then discuss how privacy and other fundamental rights are impacted by the employment of DSTs, arguing that they require an assessment of the need for counter-infringement measures. This is followed by an analysis of the image of the scale in terms of the trade-off that may be required between DSTs and fundamental rights, and the subsequent balancing act required by human rights law, notably the European Convention of Human Rights (ECHR). Finally, the conclusion sums up the findings regarding counter-infringement measures.

Digital security and human rights

Common sense easily confuses safety and security. In specialist discourse, safety is usually understood to refer to protection against physical or other harm, whereas security is taken to denote the prevention of or the resilience against deliberate attacks.² The concepts overlap. Safety can be increased if attacks can be prevented or withstood, but safety is also at stake beyond deliberate attacks, as in the case of natural disaster, harmful side-effects of human action and unintentional negligent causing of harm. Meanwhile, the concept of

¹ This chapter is an abbreviated and revised version of Mireille Hildebrandt (2013a) Balance or Trade-off? Online Security Technologies and Fundamental Rights.

² B. Schneier (2006) *Beyond Fear Thinking Sensibly about Security in an Uncertain World*. Berlin: Springer, 12.

security is often used to refer to the reduction of foreseeable harm (thus hopefully increasing safety) and related to resilience against crime.³

Digital security concerns the confidentiality, integrity or availability (CIA) of data, computing systems or service provision – it does not necessarily involve safety.⁴ Digital security is also a subdiscipline of computer science (focused on cryptography). Safety is thus both more and less than security and vice versa, and both safety and security overlap in part with digital security. Increased digital security does not imply increased safety, both because safety hazards exist beyond intentionally caused harm and because technical security also concerns issues that have no direct link with harm.

This chapter investigates how the legal framework of fundamental rights relates to issues of digital security. The focus is not an analysis of positive law but on the purposiveness, justice and legal certainty of legal protection in a constitutional democracy. With Radbruch,⁵ these three dimensions of the law can be seen as antinomies; they direct the operations of the law even though they do not always work in concert.⁶ This implies a balancing act. For instance, if the *purpose* of the law is to increase the safety of citizens or the availability of online services, while *justice* requires equal respect and concern for all, this implies that safety and security are distributed in a fair way and that infringements of rights and freedoms are complemented by adequate safeguards. Legal certainty means that citizens can base their own actions on the expectation that legal norms will be effective, creating trust that justice will be done while purposes are pursued. In relation to digital security, the construction of the legal framework determines the incentive structure for public and private investment in security measures that incorporate counter-infringement measures.⁷

Digital security: threats and vulnerabilities

The discipline of digital security thinks in terms of an “attacker model”. Researchers develop so-called use-cases to foresee what types of attacks could compromise which types of digital systems, resulting in requirements to prevent such compromise at the level of hardware, operating systems, firmware, software, applications and organisation (social engineering) and in tools (both technical and social) to counter attacks and/or reduce the damage. Digital security can thus be defined in terms of threats from the side of attackers (e.g. attack toolkits) and in terms of vulnerabilities on the side of the systems, networks, services and infrastructure that may be under attack (e.g. buffer overflow and

3 L. Zedner (2009) *Security*. London: Routledge.

4 If a webshop, e.g. selling shoes, suffers an attack that causes a disruption of its services, this impacts its availability and may even cause financial damages; it does not impair anybody's safety. Also see K. M. M. de Leeuw and J. Bergstra (Eds.) (2007) *The History of Information Security: A Comprehensive Handbook*. Amsterdam: Elsevier.

5 G. Radbruch (1950) Legal Philosophy. In: E. Lask and C. Wilk (Eds.), *The Legal Philosophies of Lask, Radbruch and Dabin*. Cambridge: Harvard University Press.

6 M. Hildebrandt (2015a) Radbruch's Rechtsstaat and Schmitt's Legal Order: Legalism, Legality, and the Institution of Law. *Critical Analysis of Law*, Vol. 2, No. 1, <http://cal.library.utoronto.ca/index.php/cal/article/view/22514> (accessed 17.07.2018).

7 For instance, product liability for security vulnerabilities in software would create an entirely different incentive structure than the current one. At a more basic level, tort law and criminal liability – including the applicable law of evidence and burden of proof – determine who will invest up to what level in security measures. As counter-infringement measures become a legal requirement, the market for security technologies will adapt, ensuring their economic feasibility.

SQL protocols). Vulnerabilities can be exploited by what is called malicious code (e.g. a virus, worm and Trojan horse) that is capable of destroying data or running destructive or intrusive programmes, for instance stealing sensitive information (of a person or a business). Other digital security issues concern spam that may be sent by remotely controlled spam zombies and fraud that may be conducted by phishing hosts or bot-infected computers.

As indicated previously, security in the technical sense is usually defined in terms of confidentiality, integrity and availability, and builds on the assumption of attackers trying to violate either one. Confidentiality concerns data (including databases and software) and nourishes the numerous narratives of Alice who want to send a confidential message to Bob, while Eve tries to figure out the content of the message. Eve is clearly the attacker here; she may be a person, a computer system, or a web bot. Integrity concerns either data or computer systems and here the attack aims to manipulate data or systems, which renders them incorrect or incomplete, and/or rewrites code thus compromising the programme (e.g. hacking the operating system of a smart car). Availability concerns a computing system or service whose resilience is broken, resulting in a loss of functionality. In addition, digital security also concerns the identification and authentication mechanisms that enable access or other control; attackers will for instance try to gain access to online services by spoofing (false identification) or phishing (collecting credentials for authentication). It is important to discriminate between the digital security of, first, individual transactions or communications, second, of public or private service providers and, third, that of critical infrastructure. The seriousness of a threat or vulnerability will depend on the probability that confidentiality, integrity and/or availability is compromised and the severity of its impact. Ranking the impact will depend on the number of individuals who will be affected, on the distribution of the impact, the invasiveness, duration and on potential secondary effects. Evidently, attacks on the availability of critical infrastructure, such as telecom providers, banks, the Smart Grid, the Internet, or public transport will impact a large number of individuals as well as the resilience of societies, compromising their safety and security in the broader sense.

Threats to digital security are not equivalent with the threats of cybercrime. In a broader sense, however, digital security may also refer to resilience against cybercrime, which entails criminal offences committed with or against interconnected computing systems.⁸ The Cybercrime Convention⁹ obligates states to criminalise threats to CIA (illegal access, illegal interception, unlawful data interference, system interference, misuse of devices (including passwords)), to criminalise computer-related offences (computer-related forgery and fraud), and to criminalise content-related offences (online child pornography and online copyright infringements). Cybercrime thus partly concerns existing criminal offences that are grouped under cybercrime insofar as cyberspace has transformed the nature of these offences due to the change in the scope, speed, distribution and distance of both the relevant conduct and its effects. As will be discussed in the next section, measures to fight cybercrime may paradoxically threaten online security.

8 S.W. Brenner (2007a) History of Computer Crime. In K. De Leeuw and J. Bergstra (Eds.), *The History of Information Security*. Amsterdam: Elsevier, 705–721.

9 M. Watney (2012) Cybercrime Regulation at a Cross-road: State and Transnational Laws versus Global Laws. In: *2012 International Conference on Information Society (i-Society)*, 71–75.

Digital security is also implicated in the notion of cyberwar. Though not the subject of this chapter, due to the issue of extraterritorial jurisdiction-to-enforce and the blurring of internal and external sovereignty, this topic looms in the background.¹⁰

Digital security technologies

To evaluate the balance or trade-off between digital security and human rights, we can think in terms of benefits generated by digital security measures on the one hand, and the costs of human rights on the other. Note that the measures themselves are not a benefit; whether they are depends on their effectiveness, which obviously cannot be presumed. Also, both costs and benefits involve distribution issues: who share the costs and who share the benefits?

DSTs can be divided in three types. First, technologies to ensure confidentiality of communication in digital environments (e.g. online, but also Internet of Things, connected cars, etc.). Second, technologies to detect and counter threats and vulnerabilities against availability or integrity of digital environments. Third, technologies to detect and counter cybercrime such as forgery, fraud, child pornography and copyright violations committed in digital environments.

The first type of DSTs means to ensure confidentiality. This involves encryption for identification (enabling to single out an individual user) and/or authentication (verifying access rights). Encryption is often seen as a guarantee of what some call data privacy or data confidentiality, while it may also protect against profiling based on content or metadata. The fundamental rights to privacy and data protection are often defined in terms of secrecy or data minimisation; though this covers only part of these rights it seems that encryption will not, in principle, violate fundamental rights.¹¹ However, encryption often depends on trusted third parties for key management and certification. To the extent that trust is intransitive and does not scale, this implies that encryption generates new vulnerabilities that require further DSTs to detect fraudulent third parties or attacks against trusted platforms. Similarly, DSTs which ensure authentication may seem neutral as to human rights, but this conclusion is again premature. Authentication allows access control and though this may be a benefit for individual citizens (to the extent that it prevents unauthorised access to personal data by others) it all depends on who is in control, how much transparency is built-in and what remedies individuals have against illegitimate access to their data. Authentication technologies allow to exclude people, they afford walled gardens on the web and within a secured environment these techniques may also afford the monitoring of individuals by means of re-recognition.¹²

10 M. Hildebrandt (2013b) Extraterritorial Jurisdiction to Enforce in Cyberspace. *Toronto Law Journal*, Vol. 63, No. 2, 196–224 (Focus Feature: Criminal Jurisdiction: Comparison, History, Theory) and M. Hildebrandt (2017) The Virtuality of Territorial Borders. *Utrecht Law Review*, Vol. 13, No. 2 (12 May), <https://doi.org/10.18352/ulr.380> (accessed 17.07.2018).

11 S. Gürses, B. Berendt and T. Santen (2006) Multilateral Security Requirements Analysis for Preserving Privacy in Ubiquitous Environments. In *Proceedings of the UKDU Workshop*, 51–64.

12 C. J. Bennett and D. Lyon (2008) *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. London: Routledge and O.H. Gandy, Jr. (2000) Exploring Identity and Identification in Cyberspace. *Notre Dame Journal of Law, Ethics & Public Policy*, Vol. 114, 1085.

The second type of DSTs mean to detect and counter threats and vulnerabilities in digital environments. They can be divided in monitoring, filtering and blocking technologies.¹³ Monitoring may require analysing internet traffic (attack monitoring, detection of adversarial machine learning),¹⁴ which means that volume, address, routing or even content of the packets that co-constitute the internet are inspected to detect various types of malware or illegal content. Filtering removes or diverts internet traffic, e.g. viruses, malicious users, child pornography, advertisements, or hate speech. Filtering is automated and based on code that may be either over-inclusive or under-inclusive (filtering more or less than intended). Note that child pornography, advertisements or hate speech do not threaten digital security, and advertisements are not necessarily illegal, but filtering that type of content is performed by using the same technology that protects against malware. Blocking entails preventing a specific IP address or set of IP addresses from uploading and/or downloading content to or from the Internet, for instance to prevent illegal file-sharing, to prevent malicious attacks or to prevent a computing system from controlling other computers by means of a botnet. Monitoring is connected with surveillance, and filtering and blocking is often considered to be a violation of so-called Net Neutrality. It should be clear that the eruption of the “fake news” scandals, the use of microtargeting to influence elections and more generally attempts to confuse constituencies as to the reliability of information has resulted in tech platforms running automated software to detect (monitor) and remove (filter) potentially unreliable content and/or to block websites that supposedly make it their business to spread misinformation. Even if human moderators are involved, content will first be flagged by algorithms as the volume of information that must be scrutinised is too big. Monitoring, filtering and blocking of content based on DSTs raises a number of human rights issues, especially due to the fact that they involve censorship by private companies.

The third type of DSTs mean to detect and counter cybercrime. This concerns the powers of law-enforcement agencies, such as those imposed on states in the Cybercrime Convention: expedited preservation of stored computer data, production orders, search and seizure of stored computer data, real-time collection of computer data, and interception of content data. The most relevant technologies in relation to digital security are those that enable remote access to and remote control of computing systems (hacking), which includes disabling, disconnecting, or even destroying data and software running on a remote computing system (server). This includes decryption technologies to gain access to content, operating systems, cloud servers and social media profiles. Obviously, these technologies are precisely those that threaten the CIA of data, software, hardware and related services – thus compromising the digital security of the environment we

13 On monitoring based on deep packet inspection, see, e.g. R. Bendorath (2009) Global Technology Trends and National Regulation. Explaining Variation in the Governance of Deep Packet Inspection. Conference Paper at International Studies Annual Convention New York City, 15–18 February 2009, http://userpage.fu-berlin.de/bendorath/Paper_Ralf-Bendorath_DPI_v1-5.pdf (accessed 17.07.2018).

More generally on monitoring, filtering and blocking, see L. DeNardis (2007) A History of Internet Security. In: K. De Leeuw and J. Bergstra (Eds.), *The History of Information Security*. Amsterdam: Elsevier, 681–704.

14 Adversarial machine learning is a technique to disrupt the output of machine learning, for instance reducing the accuracy of image recognition techniques to prevent detection of child pornography or copyright infringements. Also see L. Chen, Y. Ye and T. Bourlai. (2017) Adversarial Machine Learning in Malware Detection: Arms Race between Evasion Attack and Defense. In 2017 European Intelligence and Security Informatics Conference (EISIC), 99–106, <https://doi.org/10.1109/EISIC.2017.21> (accessed 17.07.2018).

increasingly depend on. Employment of these technologies will often fall within the scope of criminal offences, requiring specifically circumscribed and purpose-bound legal competences as a justification. In the case of law enforcement this is in the first place required by the criminal law legality principle that constrains the investigation and prosecution of criminal offences. The wave of so-called crypto wars highlights that decryption technologies, while potentially enabling a breakthrough in an individual case, may cause havoc at some of the deeper levels of our critical infrastructure, basically increasing the vulnerability of the system as a whole, potentially also endangering a series of human rights in the process.

Unsurprisingly, DSTs generate new digital security risks as well as violations of fundamental rights: encryption requires trusted third parties (certification authorities, key management) that can violate their duties; authentication allows monitoring and exclusion; monitoring is connected with surveillance which threatens confidentiality and privacy; surveillance also links with social sorting which threatens equal treatment; and finally filtering and blocking is often considered a violation of net neutrality that should guarantee equal access for all users, while filtering and blocking often grants unprecedented powers of censure to private companies with private interests that may not align with the human rights such filtering ultimately aims to protect.

DSTs and human rights

Security technologies have always generated new security risks. Guns can be used to defend against attacks or to enforce compliance with the law, providing trust and security between citizens. However, they can also be used to intimidate a population into submission. The monopoly of violence that grounds internal and external sovereignty has been tamed by the legal framework of the Rule of Law that binds those in power to the law, limiting their capability to bend the law to their own purposes. This is a historical artefact that cannot be taken for granted, necessitating a vigilant civil society and an independent judiciary to keep the system of checks and balances in operation. DSTs have a disruptive potential, like guns, and require reinstatement of the Rule of Law on the nexus of national and international jurisdiction, taking into account the new affordances of data- and code-driven infrastructures, compared to the previously prevalent text-driven ICTs (written regulations). This section discusses the affordances of DSTs with regard to fundamental rights, arguing their radical difference from traditional security technologies (guns, search and seizure, incarceration, interception of traditional communications such as letters and telephone).

Cybercrime differs from “ordinary” crime in terms of distance (e.g. remote hacking), scale (e.g. DDOS attack, spam), speed (e.g. dissemination of malware), automation (e.g. Web bots tracing and tracking vulnerabilities, DDOS attack), interconnectivity (e.g. peer-to-peer file-sharing of malicious software, remote hacking¹⁵) and invisibility (the backend systems are often intransparent due to their computational complexity, incomprehensibility and intellectual property rights). This provides the reasons for treating cybercrime differently from “ordinary” crime, resulting in the need for new types of investigative methods. These new methods (e.g. DSTs) in turn differ from previous technologies in terms of distance (e.g. remote search, notably extraterritorial reach), scale (e.g. easy access

15 Also see S.W. Brenner (2007b) *Law in an Era of “Smart” Technology*. New York: Oxford University Press.

to data on SNSs, blogs and publicly posted personal information), speed (e.g. deleting evidence of unlawful investigative methods), automation (e.g. profiling of online content and of online behaviours), interconnectivity (once data are disclosed, difficult to put back in Pandora's box due to the network effect), and, invisibility (law-enforcement agencies may work with proprietary software they cannot explain). While both cybercrime and DSTs have novel impacts on safety and security, the same goes for their impact on fundamental rights. One may expect that the impact of DSTs in terms of distance, scale, speed, automation, interconnectivity and invisibility change the mode of existence of fundamental rights such as privacy, data protection, non-discrimination, due process, presumption of innocence and free speech. I will briefly discuss how these novel security technologies reconfigure these rights to prepare for the central argument in the next section, which concerns the image of balance that permeates discussions on liberty and security.

The first type of DSTs may infringe privacy in the sense of control over one's personal data when key management or certification go awry, and data breaches occur. Attempts to prevent this may involve monitoring that could involve profiling with far more invasive privacy effects. Also, online authentication may – depending on whether this involves full identification or the management of credentials – allow for full-scale monitoring behind the access-point. This will, again, allow for invasive types of profiling with more complex and invasive impacts on privacy. The second type of DSTs requires monitoring of Internet traffic and thus links up with surveillance. Monitoring can consist of shallow or deep packet inspection to check on volume, routing, origin or destination, or even content. It affords eavesdropping, censorship and all kinds of statistical operations such as data mining, for instance for commercial purposes, law enforcement or intelligence. This easily results in privacy infringements and erosion of free speech, while it enables different types of discrimination and reduces rights of due process (due to the invisibility of online surveillance). The third type of DSTs provide extensive investigatory technologies for law enforcement, again infringing privacy, enabling invisible discrimination, generating a chilling effect on the freedom of expression, while also reducing the protection of the presumption of innocence as criminal investigation shifts to the pre-trial phase.

The notion of the scale: trade-off and balance?

Immediately after 9/11 the metaphor of the scale gained traction. It gives the impression of balance and reasonableness in times of emergency. The core idea seems to be that between security and liberty, we cannot have our cake and eat it too; choices will have to be made and if so, they had better be well balanced. The idea that some of our liberty must be given up to achieve security has a rhetorical ring that fits the political agenda of extended law-enforcement competences, as well as that of the security technologies' industry in the broad sense, including arms production for military purposes. That agenda also includes DSTs and we can imagine that companies developing and selling them have two strategies to enlarge their turnover: they can increase their market share or expand the market. This usage of the metaphor of the scale can be used to sell security technologies which may infringe fundamental rights: if we want online security, we must accept that privacy, data protection, non-discrimination, due process and free speech will have to be limited. Giving up a measure of privacy to gain a measure of security sounds reasonable to many people.

Preliminary observations

Before embarking on the intricacies of the image of the scale several caveats apply. First, the discourse of balance evokes the notion of weighing. On a scale, one can weigh different ingredients, assuming that all that matters is their weight. In the case of security technologies that infringe fundamental rights this raises the question of the nature of the ingredients, noting they are weighted in terms of a trade-off rather than a balance. Is the public good of security traded against the private good of privacy, or must we consider both to be public goods? Must these goods be qualified as rights or as interests?¹⁶ Is the right to safety or that to security traded against the right to privacy or to non-discrimination? Is an individual right such as privacy traded against collective interests such as security? Or do we trade a private interest in privacy against a public interest in security? Obviously, such questions are related to traditional distinctions in moral philosophy. Kantian deontologists may vouch for a rights approach, whereby rights are trump cards that overrule interests. Benthamite utilitarians may vouch for an approach based on aggregate interests, though Millian liberals could restrict the utilitarian calculation by claiming a fundamental right to liberty that can only be overruled by security interests that serve to protect individual liberty. Pitting individual rights or interests in fundamental rights against a public good or a collective interest in online security is highly problematic. It assumes that fundamental rights and security are at the same level, whereas their relationship is more complicated as one may be conditional for the other. It also, wrongly, assumes that privacy is not a public good or a collective interest and security not a private good or individual right. For their realisation, private interests in privacy and security both depend on a legal framework that provides a minimum of legal certainty with regard to these interests, which explains that *individual privacy and individual security are also public goods*.

This brings to the fore the question whether legal certainty can be achieved without security in the broad sense of being safe against violent attacks. This relates to the question of whether security is, like privacy, a human right or rather a precondition for the legal framework on which effective human rights depend, which, in turn, raises the issue of power and authority.¹⁷ These are hefty terms, often mistakenly used interchangeably. Authority is based on the power to command obedience, power is based on the economic or military ability to enforce submission. Under the Westphalian system of sovereign states, state authority depends on the monopoly on violence and implies the power to protect citizens against violence from other citizens (internal sovereignty depends on this) and from other states (external sovereignty). Social contract theory from Hobbes to Rousseau somehow assumes that the state is capable of providing the fundamental security required to go about one's daily business.¹⁸ Once such security can no longer be provided, the social contract crumbles and states dissolve in civil war. Security in that broad sense,

16 On different theories concerning the difference between rights and interests. Also see W.A. Edmundson (2004) *An Introduction to Rights*. Cambridge: Cambridge University Press.

17 M. Hildebrandt (2010) The Indeterminacy of an Emergency: Challenges to Criminal Jurisdiction in Constitutional Democracy. *Criminal Law and Philosophy* Vol. 4, No. 2, 161–181 and M. Hildebrandt (2013b) Extraterritorial Jurisdiction to Enforce in Cyberspace. *Toronto Law Journal*, Vol. 63, No. 2, 196–224 (Focus Feature: Criminal Jurisdiction: Comparison, History, Theory).

18 This is related to the fact that contract theory concerns the institution of the monopoly of violence, that is only acceptable insofar as the state actually manages to protect its subjects from violent attack. On the complexities of, e.g. the right of resistance in Hobbes, Locke and Rousseau Also see J. C. Johari (1987) *Contemporary Political Theory: New Dimensions, Basic Concepts and Major Trends*. New York: Sterling, 388.

combining safety against attack and legal certainty, seems conditional for state authority. This means that authority works within the state but hardly between competing states and transnational corporations, where power is at stake rather than authority. This raises a number of questions as to how security technologies function across national borders, playing out across various jurisdictions, where the user may be unaware of the actual location of the data servers that are being accessed to wipe out botnets or other threats to cybersecurity. It is worthwhile to note here that the protection of human rights ultimately depends on a court of law and an administration that grants and executes the substance of the right, whereas at the level of extraterritorial jurisdiction such protection is not guaranteed. In that case, security may be provided without being complemented with the safeguards of fundamental rights.

Six caveats from Jeremy Waldron

Not long after 9/11, when criticising security measures in the USA was easily interpreted as unpatriotic behaviour, legal philosopher Jeremy Waldron spoke at a workshop on “Terrorism and the Liberal Conscience” at All Souls College, Oxford on the subject of “Security and Liberty: The Image of Balance”.¹⁹ In his topical paper, he develops six concerns regarding the idea that international terrorism requires states to strike a new balance between security and liberty. These concerns are relevant for similar calls to strike a new balance with regard to online security, based on the plethora of threats and vulnerabilities that endanger critical infrastructure, service providers and individual citizens.

First, the image suggests that by diminishing liberties we will achieve security. This, however, cannot be taken for granted, as it will depend on a number of empirical facts, many of which are simply not known when taking the measures. In other words, their effectiveness cannot be assumed but should be assessed. Whether DSTs achieve effective protection against threats and vulnerabilities of the ICT infrastructure and against various types of cybercrime does not depend on whether they infringe fundamental rights. In many instances alternative technologies that cause less or even no infringement could be equally or even more effective.

Second, the image suggests a measure of precision that is inherent in cost-benefit analyses; to increase security (benefit) we must decrease liberty (cost). Such precision is an illusion, due to various types of incertitude, for instance those discussed by Waldron, who discriminates between risk, uncertainty, ambiguity and ignorance.²⁰ The precision suggested reinforces a bias to quantifiable, machine readable criteria whose weighing depends on a tertium comparationis that may not be available: how does one weigh rights’ infringements against security interests?

Third, the image suggests that liberties can be traded at will, though from the perspective of the Rule of Law these liberties are exclusionary reasons,²¹ side constraints,²²

19 J. Waldron (2003) Security and Liberty: The Image of Balance. *Journal of Political Philosophy*, Vol. 11, No. 2, 191–210. doi:10.1111/1467-9760.00174.

20 Andy Stirling (2008) Science, Precaution, and the Politics of Technological Risk. *Annals of the New York Academy of Sciences*, Vol. 1128 (Strategies for Risk Communication Evolution, Evidence, Experience), 95–110.

21 Joseph Raz (1999) *Practical Reason and Norms*. Oxford: Oxford University Press.

22 Robert Nozick (1988) Side Constraints. In Samuel Scheffler (Ed.), *Consequentialism and Its Critics*. Oxford: Oxford University Press.

or trump cards²³ that cannot simply be overruled by assumed security gains. The image thereby seems to privilege a utilitarian rather than a Kantian ethics.

Fourth, the image also suggests that one's liberty must be traded against one's security, whereas in practice there is a problem of distribution. Usually the liberties of specific groups (illegal immigrants, unemployed, convicted criminals, suspects, outliers in the case of profiling technologies) are traded against the security of other groups (those assumed to be law abiding citizens, those who remain "under the radar" in the case of profiling technologies). This raises the issue of distribution of costs and benefits.

Fifth, the image is not transparent about the fact that by diminishing liberties the powers of the state are increased and that this simple fact will entail security threats. Montesquieu's warning about the need to introduce countervailing powers regards precisely this point. DSTs may reduce citizens' security against state powers.

Sixth, the image may condone symbolic measures that have no real effect in terms of security, hoping to achieve a largely illusionary public sense of security. This has been coined "fact-free policies" and we should note that much of what is presented as evidence-based policies in fact engages a rhetoric that is entirely fact free.²⁴

Limitation of fundamental rights

Constitutional and international human rights law employ various strategies to limit the scope of fundamental rights, while ensuring they do not lose their substance. Limitation is inevitable, either because they clash with public goods that are conditional for the effectiveness of fundamental rights or because various rights or liberties clash and must be aligned one way or another. Within the context of the European Convention of Human Rights which determines the human rights framework within the Council of Europe (52 states), the limitation of the rights to privacy, freedom of thought, conscience and religion, freedom of expression and freedom of assembly and association require a triple test to determine whether a security technology measure that violates one of these rights can be legally justified. This triple test can be used to exemplify how the trade-off and the balance that define the image of the scale can be related to the impact of DSTs on fundamental rights.

After attributing a right to privacy in the first paragraph of Art. 8 of the Convention, the second paragraph articulates three cumulative conditions to justify the infringement:²⁵ the infringing measures must be in accordance with the law, necessary in a democratic society and have a legitimate aim. The "legitimate aim" and the requirement that the measure is "necessary in a democratic society" imply that a trade-off *can be* justified, but only if the infringing measure is necessary and proportional to achieve public goods such as the protection of public order, health or morals or the protection of the rights and freedom of others. DSTs that cannot be expected to achieve one of the public goods enumerated in

23 Ronald Dworkin (1991) *Law's Empire*. Glasgow: Fontana.

24 In the context of anti-terrorism measures such as anti-money laundering. Also see N. Passas (2006) Fighting Terror with Error: The Counter-productive Regulation of Informal Value Transfers. *Crime, Law and Social Change*, 45(4–5), 315–336.

25 S. Sottiaux (2008) *Terrorism and the Limitation of Rights. The ECHR and the US Constitution*. Oxford: Oxford University Press and P. De Hert and S. Gutwirth (2009) Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action. In: S. Gutwirth, Y. Poullet, P. De Hert, S. Nouwt, and C. de Terwangne (Eds.), *Reinventing Data Protection?* Dordrecht: Springer, 3–44.

Art. 8.2, cannot be justified. This implies at least a marginal test of the effectiveness of the infringing measure. The trade-off is a necessary – but not sufficient – condition. Justification is also conditional on the assessment that the infringing measures are “in accordance with the law”. In the case law of the ECHR the requirement of lawfulness is detailed as demanding a basis in national law that is adequately accessible, sufficiently foreseeable and contains effective safeguards. Adequate accessibility and sufficient foreseeability means that citizens can anticipate what types of measures their government can take that might infringe their privacy and thus relates to their reasonable expectation of privacy. For instance, secret surveillance may be allowed, if citizens can foresee in what circumstances it might occur, even if the police will not notify them before wiretapping or requiring access to the personal data of a subscriber to an online service provider. Adequate and effective safeguards necessitate that secret surveillance is neither unlimited in scope (time and content) nor in scale (number of people, frequency of interception) and the condition of safeguards also entails that a warrant or permission from a judge is needed if the invasiveness, frequency or duration of the measure increases beyond a certain threshold. The most important safeguard has been that infringing measures are only allowed in specific cases, ruling out general monitoring of groups or individual citizens.²⁶

In line with new approaches to “protection by design”, the General Data Protection Regulation (GDPR) has articulated a legal obligation to implement “data protection by default and by design” (DPbD, Art. 25 GDPR), requiring that those responsible for respecting the fundamental right to data protection (Art. 8 Charter Fundamental Rights of the European Union) implement state of the art technical and organisational protection at the level of the sociotechnical architecture that may infringe various fundamental rights. I have argued elsewhere that this right to DPbD should be understood as an instance of a broader concept of legal protection by design that is meant to ensure that the protection of human rights in the era of data-driven environments remains effective. The point is that data- and code-driven human rights infringements require data- and code-driven protection, entailing a translation of text-driven legal protection into the architecture of data- and code-driven systems.²⁷

DSTs that aim to detect and counter online security threats, vulnerabilities and various types of cybercrime may infringe privacy. Building on the triple test of European human rights law, such infringements should be justifiable in terms of a proportional trade-off that instigates a threshold before the employment of such technologies is allowed. If, however, that threshold is reached, the requirement of proportionality demands the implementation of *counter-infringement measures* that reduce potential infringements to what is reasonable in relation to expected benefits. In that case, the notion of proportionality becomes contingent upon the technical and economic state of the art in counter-infringement technologies. Next to that the employment of DSTs should be conditioned by the implementation

26 See e.g. on mass interception in the context of national security ECtHR, 19 June 2018, Application no. 35252/08, Case of *Centrum för Rättvisa v. Sweden*, finding that the abstract test requested by the applicant (who did not provide evidence of being a victim of an infringing measure) was not required, as the applicant was considered to have enough alternative legal remedies. For minimum safeguards see consideration 95 of ECtHR, 29 June 2006 Application No. 54934/00, Case of *Weber Saravia v. Germany*.

Seminal judgements can be found in the fact sheet on mass interception of the ECHR at www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

27 Mireille Hildebrandt and Laura Tielemans (2013) Data Protection by Design and Technology Neutral Law. *Computer Law & Security Review* and M. Hildebrandt (2017) The Virtuality of Territorial Borders. *Utrecht Law Review*, Vol. 13, No. 2 (12 May), <https://doi.org/10.18352/ulr.380> (accessed 17.07.2018).

of a set of safeguards that are proportional in relation to the expected scope of potential infringements (the more substantial the infringement, the more substantial the safeguards). These safeguards will require human intervention, for instance to judge whether the threshold for a justifiable trade-off is reached – while in an automated environment some of the safeguards should be automated,²⁸ for instance by flagging potential abuse of DSTs based on certain indicators.

In short, the issue of the trade-off means that if an DST is not effective in reaching a legitimate aim, it cannot be proportionate and must be prohibited in as far as it infringes privacy or other fundamental rights. To assess this, we need *freedom infringement impact assessments for DSTs*, resulting in evidence-based DSTs instead of fact free security policies. The issue of balance requires that the more serious the infringement may be, the more substantial the required counter-infringement technologies should be. This can be achieved, for instance, by developing smart security and data protection by design – as imposed by the proposed General Data Protection Regulation.

Concluding remarks: counter-infringement measures as necessary safeguard under human rights law

The reach, scope, speed, automation, interconnectivity and invisibility of threats and vulnerabilities of data- and code-driven systems have offset a growing demand for DSTs, both in the private and the public sector. Various types of DSTs can be distinguished, based on encryption technologies and key management, on monitoring, filtering and blocking and on (remote) hacking of computing systems. DSTs are meant to increase online security in the broad sense of safety from attacks against confidentiality, integrity and availability of personal data and critical infrastructure; resilience against fraud and forgery; and detection and prevention of child pornography and violations of copyright. At the same time, they afford violations of human rights, notably privacy. This chapter inquired into the nature of the metaphor of the scale, fleshing out the difference between a trade-off and a balance. A trade-off suggests that more digital security means less privacy. This cannot be assumed. A more effective level of digital security is a necessary but not a sufficient condition for giving up some privacy, also taking into account that the more privacy invasive a DST the higher the threshold should be for allowing it. If security threats and proportionate DSTs meet the threshold of a sufficient condition, a balance must be struck: the higher the infringement of human rights, the more effective safeguards must be implemented. In line with data protection by design and default, human rights law must develop the notion of counter-infringement measures as part of the necessary safeguards under human rights law. Like data protection by design this would be another instance of legal protection by design.

28 This involves Legal Protection by Design and/or Privacy by Design. Also see M. Hildebrandt (2011) Legal Protection by Design. *Legisprudence*, Vol. 5, No. 2, 223–248 and M. Langheinrich (2001) Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In *Proceeding of 3rd International Conference Ubiquitous Computing*. Berlin: Springer, 273–291.