2014

Criminal Law and Technology in a Data-Driven Society

Mireille Hildebrandt, *Radboud University Nijmegen*

DRAFT 2013
PLEASE REFER TO THE FINAL VERSION IN:

MARKUS D. DUBBER AND TATJANA HÖRNLE (EDS.), *OXFORD HANDBOOK OF CRIMINAL LAW*, OXFORD: OXFORD UNIVERSITY PRESS, 174-197

CRIMINAL LAW AND TECHNOLOGY IN DATA DRIVEN SOCIETY

Mireille Hildebrandt

1 INTRODUCTION

This chapter takes leave of the idea that lawyers can remain immersed in legal text. It takes a stand for a careful reflection on what data-driven architectures do to some of the assumptions of modern law that are mistakenly taken for granted. Merely enacting the presumption of innocence by means of legal code will not do in the present future. If the defaults of Big Data analytics all point in the direction of precrime punishment or the pre-emption of inferred criminal intent, we need to reconfigure the smart decision systems that progressively mediate the perception and cognition of law enforcement and intelligence. Architecture is politics and code is law.

This chapter starts with an analysis of different conceptions of law and technology, followed by a discussion of technology and neutrality in the light of the Rule of Law. After these explorations a relational conception of the criminal law is developed, based on Radbruch's antinomian conception of law, highlighting justice, legal certainty and the instrumentality of the law. This is aligned with a pluralist understanding of technology to flesh out the implications of data-driven intelligence for the meaning of the criminal law. Special attention is given to the presumption of innocence that seems to be overruled by the affordances of data-driven law enforcement. Finally, the chapter explains the need for a 'presumption of innocence by design', thus translating some of the crucial affordances of the written law into the critical infrastructures of data-driven society.

2 THREE WAYS OF CONCEPTUALISING LAW AND TECHNOLOGY

Law has been conceptualised as a neutral instrument of regulation (instrumentalism), as a tool to control the government (critical conceptions) and as an instrument to constitute and limit state powers while creating a web of legitimate expectations amongst citizens (relational conceptions).[1] Technology has been approached as a neutral instrument to achieve specific ends (instrumentalism), as an autonomous force that is beyond human control (autonomous conception) and as an instrument that co-constitutes the outcomes it achieves (whether or not intentional), while the same technology can evoke different outcomes depending on a host of local factors

[1] Cf. R. Foqué and A.C. 't Hart, *Instrumentaliteit en Rechtsbescherming* (1990).

(relational or pluralist conception).[2] It is important to reflect on these different conceptions because they inform how we speak and think about law and technology, how we assess the legal implications of novel technologies and how we understand the regulation of and by technologies.

2.1 THREE WAYS OF CONCEPTUALISING LAW

Law can be understood in different manners, for instance, as a neutral tool to achieve policy goals or as protection against government interventions that infringe citizens' rights and freedoms. The problem with the first is that if law is a mere instrument, it can be replaced by another instrument that is more effective and/or more efficient. Law thus becomes interchangeable with administrative regulation, with nudging based on behavioural economics or with technoregulation. I will call this conception of law an *instrumentalist* view, because it reduces law to its instrumental dimensions, notably separating it from politics and morality. Positivist conceptions of law as well as regulatory paradigms in social science seem to adhere to this position.[3] In that view, if we can deter crime by means of technologies that pre-empt criminal intention, we should base our decision on a cost benefit analysis, not on the normative idea that such things should be regulated by law.

The problem with the second – critical - understanding is that it separates law from governmental intervention, suggesting that government is basically policymaking and administration whereas the law is a matter of protecting against the negative implications of governmental interventions. Government, in that view, is a matter of police in the old sense of the term,[4] whereas law is a matter of policing the police. This can be coined as a critical or autonomous understanding of law, because it attributes a kind of autonomy to the law that, however, reduces the legal framework to its critical dimensions. The critical conception thus separates law from the constitution of societal order and from the powers of government. This is problematic because the law depends on the authority of the state to enforce the protection it offers; effective remedies require competent courts whose judgments are implemented even when they challenge governmental actions or decisions. If the criminal law does not constitute but only limits the exercise of state power we can guess that its critical potential becomes part of a balancing act that easily trades liberty against security, especially in times of emergency. If the powers of the state are constituted by the law that in the same stroke restricts their scope, such a trade-off is less likely. The balancing act will have to be performed within the law, instead of pitting law against security measures.

This brings us to a third understanding of law, that aligns with the central tenets of constitutional democracy.[5] In this conception law brings together the policy-oriented dimensions of legislation and administration with their protective

[2] Cf. Peter-Paul Verbeek, 'Materializing Morality. Design Ethics and Technological Mediation', (2006) 31 *Science Technology & Human Values* 3 (2006): 361ff.

[3] The regulatory paradigm sees law as a form of regulation, defined as a way to influence people's behaviours. Cf. J. Black, 'Critical Reflections on Regulation', (2002) 27 *Australian Journal of Legal Philosophy*, 1ff.

[4] Markus Dirk Dubber, *The Police Power. Patriarchy and the Foundations of American Government* (2005).

[5] In this chapter we speak of 'constitutional democracy', highlighting both democratic government and the constraints of the Rule of Law; we avoid the use of 'liberal democracy' as this would restrict us to one particular form of constitutional democracy, cf. John Kekes, *The Morality of Pluralism* (1993).

dimensions, enabling a double instrumentality (aiming to achieve specific policy objectives while at the same time achieving the protection of human rights). The critical potential of law is thus seen as a dimension that is part and parcel of the legal system, just like its goal-oriented dimension. Moreover, this conception of law highlights that the legal system is not a system of legal rules but rather a system of legal relations determined by and determining legal norms.[6] These relations play out at the level of the powers of the state: legislation, administration and adjudication, thus creating effective means to participate in law-making and to contest the application of legal norms. Legal relations also play out on a horizontal level, between those who share jurisdiction, by establishing a reliable framework for legitimate mutual expectations. This horizontal level is, however, enabled by the vertical relationship between citizens and the state. This geometrical architecture allows to deploy the monopoly on violence to sustain legitimate expectations between citizens, as well as between citizens and the state. It protects, for instance, against fellow citizens who try to invade our privacy to steal our identity; we can call the police and trust the state to prosecute the perpetrator. Even if this does not always work, the crucial point is whether the state aims for effective protection against crime. The same geometrical architecture, moreover, also protects against the state itself when it tries to snoop our private correspondence, mobile traffic data, or online clickstream behaviours, for instance claiming that this is necessary to protect us from transnational cybercrime. Even if, time and again, subdivisions of the state will succumb to the temptations of secretive abuse of power, the crucial point is whether a system of checks and balances is in place to allow the contestation of such measures, and their abrogation if they are found to be in violation of the law. This view of law has been called a relational or a pluralist conception, marking the rule of law as the scaffolding of constitutional democracy. From this perspective the law in a constitutional democracy is a historical artefact that has normative implications and cannot be taken for granted. It requires hard work to sustain its complexity, coherence and the fragile and robust constitution of its double instrumentality. This third understanding of law is the point of departure for this chapter. A more detailed exploration will be developed below, when discussing a relational conception of the criminal law.

2.2 THREE WAYS OF CONCEPTUALISING TECHNOLOGY

Like the law, technology can be understood in different ways. If we understand technology as a tool with a material component,[7] it is clear that some will believe that the tool is neutral while others will hold that the tool co-constitutes what it makes or achieves.[8] Still others may claim that our tools reconfigure us as human beings, enabling new ways of being in the world and ruling out others.[9] It seems obvious that the use of tools is an important if not defining characteristic of the *homo sapiens*, a visit to any archaeological museum will show how closely our humanity and the use

[6] Norbert Achterberg, *Die Rechtsordnung als Rechtsverhältnisordnung: Grundlegung der Rechtsverhältnistheorie* (1982).

[7] Don Ihde, *Philosophy of Technology : an Introduction* (1993): 47-48 ff. Ihde understands technique as a style or method. In French and German the terms are often used in reverse: *Technik* or *technique* as a tool, *Technologie* or *technology* as a method.

[8] On means and ends notably John Dewey, 'The Logic of Judgments of Practice', in idem, *Essays in Experimental Logic* (1916), 335ff.

[9] Don Ihde, *Technology and the Lifeworld : from Garden to Earth* (1990).

of tools are entwined. Some authors suggest that language developed together with the use of tools, highlighting that both our material tools and language allow to manipulate the environment, relating this to our understanding of causation.[10] The type of tools co-determine the kind of society they enable. For instance, a hunting and gathering society will depend on stones and spears; an agricultural society on tools for sowing, harvesting and storing; a larger society that extends beyond face-to-face relationships will depend on some form of written text to hold together; and a state with far-reaching competences to rule in detail over the lives of its subjects in a shared territory may depend on the printing press to enable the kind of bureaucracy that is needed. Such societies make possible different types of human engagement, with different skills and different moral, political and social expectations. Technologies, societies and individuals are thus co-constitutive. Closer to home, technologies like a mobile phone may reconfigure – or rather extend – the mind of its users, changing their experience of time and space, distance and location.[11] Mobile online devices (smart phones, laptops, smart glasses) disrupt the traditional identification of spatial with contextual boundaries, as they allow a person to participate in different contexts from the same location, while bringing together people and infrastructure from different locations within the same context. This seems to transform or even negate the import of territorial jurisdiction, raising difficult questions on extraterritorial jurisdiction in the era of cybercrime. Technologies are part of our sensory and cognitive resources, shaping the extent and the workings of our mind, reconfiguring the morphology and behaviours of our brains.[12]

Meanwhile, many people still believe that technologies are neutral tools or mere instruments to achieve a goal. I will call this the neutral or instrumentalist conception of technology, which for instance informed the philosophy of science insofar as it understands technology as the result of applied science and pays little or no attention to its enabling and constitutive force for the evolution of science.[13] The opponents of this position take technologies to have a deterministic influence on human society, attributing an autonomous force to Technology (with capital T). Here the idea is that humans have little control over the technologies they invent, usually ending up in so-called doom scenarios that spell redemption or catastrophe due to technologies run amok, or in boom scenarios that assume that any problem will eventually be solved by inventing new technologies. I will call this the autonomous conception of technology, since it tends to view Technology as something that has an inherent tendency toward destruction or progress, as if it has a mind of its own. Continental philosophy has somehow given rise to a number of techno-pessimists, warning against the end of civilization as we know it.[14] Silicon Valley seems to nurture the opposite, generating what has been called Technological Solutionism.[15]

A third conception, which can be termed pluralist and relational, refutes the idea of an independent autonomous Technology while also ruling out the neutrality of toolmaking and –usage. The focus here is on concrete technologies and their actual affordances, seeking to investigate how their integration in the web of human

[10] S.H. Ambrose, 'Paeleolithic Technology and Human Evolution', (2001) 291 *Science*, 1748ff. Krist Vaesen, 'The Cognitive Bases of Human Tool Use', (2012) 35 *The Behavioral and Brain Sciences* 4, 203ff.

[11] Andy Clark, *Natural-Born Cyborgs. Minds, Technologies, and the Future of Human Intelligence* (2003).

[12] Maryanne Wolf, *Proust and the Squid: The Story and Science of the Reading Brain* (2008).

[13] Cp. Ihde (n 7).

[14] E.g. Martin Heidegger, *The Question Concerning Technology, and Other Essays* (1977). Jacques Ellul and Patrick Chastenet, *Jacques Ellul on Religion, Technology, and Politics*, (1998).

[15] Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (2013).

interaction will enable new types of actions, new types of society and how this may reconfigure the mind of individual persons. This follows up on Kreutzberg's famous dictum that 'technology is neither good nor bad, but never neutral'.[16] It is not neutral because it always impacts on the scope of our interactions, inducing or inhibiting specific patterns of behaviour or even enforcing or prohibiting them.[17] This means that whether, and if so to what extent a technology is determinative of human action is an empirical question, depending on the actual affordances of the technologies. And an affordance always depends on both sides of the equation: on the technology under scrutiny and on those who are constraint and enabled by it. So all depends on what the technology makes possible and impossible for those who engage with it. In this contribution I will follow the pluralist and relational conception of technology.

3 TECHNOLOGY AND NEUTRALITY UNDER THE RULE OF LAW

In the previous section I have rejected the instrumentalist, neutral conception of technology. This has implications for the relationship between law and technology. I will investigate this relationship at two levels of analysis. First, I will explain how law-as-we-know-it is contingent upon the technological infrastructure of the printing press. This concerns the technological articulation of modern law, its mode of existence; the way is has been technologically mediated for the past five or six centuries. Second, I will engage with the question of how modern law should deal with the normative implications of a changing technological landscape. Can law remain neutral if novel technologies affect its normative impact? Or does neutrality, on the contrary, require appropriate changes in the law to compensate for a loss of protection due to transformative aspects of new technologies? These questions concern the technology neutrality of law and the – counterintuitive - fact that such neutrality may warrant technology specific law.

3.1 THE TECHNOLOGICAL ARTICULATION OF MODERN LAW

Those adhering to instrumentalist conceptions of law and technology will not be impressed by media theory or philosophy of technology and will hold that such disciplines are irrelevant for the study of law. However, if we acknowledge the implications of technological infrastructures such as the script and the printing press as enablers of different types of societies with different types of law, there may be much to learn from such disciplines. The rise of specific types of leadership and the beginnings of statehood correlate with the development of the script. The script allows for common standards that are fixed on matter (stone, clay, papyrus, paper) and capable of extending their reach beyond the face-to-face interaction of speech, thus stretching their scope in time and space. This relates to what Stiegler has called tertiary retention.[18] Our understanding of the flow of time is first of all at stake in the

[16] Melvin Kranzberg, 'Technology and History: 'Kranzberg's Laws", (1986) 27 *Technology and Culture*, 544ff.
[17] Verbeek (n. 2). M. Hildebrandt, 'Legal and Technological Normativity: More (and Less) Than Twin Sisters', (2008) 12 *Techné: Journal of the Society for Philosophy and Technology* 3, 169ff.
[18] Bernard Stiegler, 'Die Aufklaerung in the Age of Philosophical Engineering', (2013) in Mireille Hildebrandt, Kieron O'Hara, and Michael Waidner (eds.) *The Value of Personal Data. Digital Enlightenment Forum Yearbook 2013*, 29ff.

'primary retention' that is required for the continuity of our livid experience of the present. This continuity depends on the retention of what has been experienced moments ago. Eventually, such primary retentions are reconstituted as a memory by means of a secondary retention. Both take place within the confines of an individual mind, hinging on the curious interdependence of action and perception that allows us to navigate the world. Secondary retention implies that a person can reactivate earlier perceptions, re-inscribing them into the evolving web of neuronal interconnections. With tertiary retention this inscription is externalized on a 'technical support', requiring what Stiegler calls 'introjection' to bring it back into the cerebral or psychic support of living human beings.[19] Tertiary retention revolutionized human society, reconfiguring mutual expectations beyond the extended here and now of primary and secondary retention. Though this obviously affected the consolidated social norms that we might call the legal dimension of pre-state societies, it is hard to underestimate the radical implications of the uptake of the printing press. Once identical copies of original text proliferated, legal codes could be enacted and taken as guiding standards for a growing bureaucracy. The same proliferation generated a need for systemisation and interpretation. The sheer quantity of text required indexing and other forms of categorisation to enable access to relevant content, while the fact that text could be read outside its local and temporal context evoked new understandings of the same text. The combined need for systemisation and interpretation of legal text finally led to various types of consolidation in the form of doctrinal treatises, adages such as *res judicata est* and a new type of law that is valid because enacted. This means that modern, positive law is not a free-floating invention of legal minds, but an affordance of the technological infrastructure of the printing press. Though we might take the positivity of law for granted, we should be aware that the idea of positive law itself is a recent historical artefact, that is closely connected to the pervasive operations of the printed text. After the written manuscript, the printing press was the second revolution in information and communication technologies (ICTs).

To understand the implications of novel technological infrastructures that inform how we perceive and cognize our world, we need to urgently reflect on the fact that modern law is articulated in and contingent upon a particular technology. Though it is more than obvious that legal science is steeped in text and has flourished due to the continuous process of textual interpretation, the implications are not often explored. It may be that many of the characteristics of modern law, such as its relative autonomy in relation to politics and morality, derive from its association with the characteristics of the printing press era: notably the need for a class of scribes that studies, interprets and stabilizes the meaning of the persistent flow of authoritative legal texts.[20] Legal procedure, in particular the idea of procedural fairness, entails the idea that the court will suspend its judgement and hesitate before arriving at its verdict; the facts must be established in the light of the relevant legal code and the meaning of the applicable code must be reiterated in the light of the case at hand. Such characteristics have been detected by scholars writing on the impact of the script and the printing press, that both induce a distance between the meaning of the author and the meaning of the reader,[21] and a delay between reading and deciding the

[19] Stiegler builds on Husserl, who developed the notions of primary and secundary retention, as well as the idea of introjection. Cf. E. Husserl, *Phenomenology of Internal Time Consciousness* (1964). The idea of tertiary retention is Stiegler's.

[20] Paul Koschaker, *Europa Und Das Römische Recht* (1966).

[21] Paul Ricoeur, 'The Model of the Text: Meaningful Action Considered as a Text', (1973) 5 *New Literary History* 1, 91ff.

meaning of text.[22] Though a notion like the presumption of innocence is a moral notion, it is also connected with this distance, with the delay between the criminal charge and the conviction or the acquittal. In a society without a script and or one beyond the printing press our current understanding of the presumption of innocence may not work, because there is no *res judicata*, no imposed jurisdiction, no monopoly of violence; no need to interpret a text that is fixed on matter.[23] We cannot, then, take for granted that the novel ICT infrastructure will have similar affordances as that of the printing press, and as lawyers we need to consider what this means for the foundations of modern law.

In other work I have briefly summed up some of the challenges of the transition from printing press to hyperconnected networked environments that thrive on Big Data analytics.[24] The changing environment of the law challenges the linear sense of time inherent in modern law, as it is confronted with the segments and points which define the digitized interface of the Internet and the web (compare reading a book to zapping around television programs or surfing the internet); it challenges the slow accumulation of legal texts like statutes, treaties, case law and doctrine that need to be studied and interconnected, as lawyers are confronted with instant online access to of all the sources of the law (compare handbooks with selected cases to direct access to all verdicts given; compare a printed book with a hypertext); it challenges the delay inherent in procedural safeguards embodying protection against hasty judgements, as lawyers are confronted with series of real time decisions taken by automated decision systems based on machine learning techniques; it challenges modern law's ambition to achieve equal application of general legal norms to equal cases (exemplifying law's tendency to universalization and systemisation), since that ambition is confronted with refined personalisation and contextualisation made possible by advanced data mining technologies; it challenges the care with which legal theory has constructed and sustained the theoretical legitimisation and critical assessment of the positive law, since scholarly reflection is confronted with a world in which models replace theory (demanding effectiveness instead of correspondence to reality); it challenges the hermeneutical practice of law (always involved in interpreting both the facts of the case and the legal norms that should apply), since legal practice is confronted with a world in which simulation rather than interpretation turns out to be the best way to anticipate future events; it challenges the emphasis on meaning as a reference to the world outside law (semantics), since professional and scholarly interpretation are confronted with an emphasis on links and networks (syntaxis) and the actual consequences of doing things one way or another (pragmatics); and, finally, it challenges the emphasis on legal certainty, intrasystematic coherence, continuity and stability (legal doctrine and jurisprudence), that are all confronted with a rapidly changing liquid world that seems to require permanent real time monitoring (pattern recognition) instead of the slow construction of robust knowledge that survives the ravages of time.

This level of analysis raises an important question, reiterated by Stiegler, namely the issue of what it is that we need to preserve to constitute ‘a new state of law, a new rule of law, founded on digital writing, [which] in fact presupposes a new age of Enlightenment(s)’. Following the work of Maryanne Wolf, who researched the

[22] Pierre Lévy, *Les Technologies de L'intelligence. L'avenir de La Pensée à L'ère Informatique* (1990).

[23] Cf. H. Patrick Glenn, *Legal Traditions of the World* (2007), chapters 1-5.

[24] Slightly adapted from Mireille Hildebrandt, ‘A Vision of Ambient Law’, (2008) in Roger Brownsword and Karen Yeung (eds.) *Regulating Technologies,* 186-7ff, applying Lévy’s findings to the operations of the law.

development of both the morphology and the behaviour of the reading brain, Stiegler has proposed:[25]

> It is a question of knowing what must be preserved, within the digital brain, of that which characterised the reading brain, given that writing new circuits in the brain can erase or make illegible the old circuits.

The habits of the mind that underlie modern law were mediated by the printing press and the reading brain. Criminal law may turn into something unrecognizable under the mediation of predictive analytics and the hyperconnectivity of social media, reconfiguring the brain as it anticipates their operations.[26] This has far reaching consequences for the mode of existence of current law. Indeed, it suggests the need for a reconfiguration and a novel mediation of the law, in order to sustain both its instrumental and its protective dimensions within the novel technological landscape. Legal scholars exploring the possibility of novel mediations of law, beyond those of the printing press, should take into account how other disciplines have researched the embodiment or inscription of norms and values into the design of technologies, notably 'value sensitive design' and – closer to the law – 'privacy by design'.[27] From the legal perspective this has given rise to the notion of 'legal protection by design', that aims to incorporate both democratic participation and fundamental legal protection into the design of automated decision.[28] Especially where data mining is used to flag behaviours in the context of law enforcement and intelligence, default settings of the computational technologies should prevent the reversal of the presumption of innocence by the automation of suspicion. At the end of this chapter, in section 4.4, we will investigate the need for a 'presumption of innocence by design', following the example of privacy and data protection by design. Before taking that path, however, we need to look into the notion of technology neutral law that has played a major role in debates on cybercrime, copyright and data protection.

3.2 THE OBJECTIVES OF TECHNOLOGY NEUTRAL LAW

To investigate the notion of technology neutral law, as used in current debates,[29] we must return to the operations of written law. This section will explain how the idea of

---

[25] Stiegler (n. 18), cf. Wolf (n. 12).

[26] Mireille Hildebrandt, 'Proactive Forensic Profiling: Proactive Criminalization?', (2011) in R. A. Duff et al. (eds.) *The Boundaries of the Criminal Law*, 113ff.

[27] Batya Friedman, Peter H. Jr. Kahn, and Alan Borning, 'Value Sensitive Desing and Information Systems,' in Kenneth Einar Himma and Herman T. Tavani (eds.), *The Handbook of Information and Computer Ethics* (2008), ff. M. Flanagan, D. Howe, and Helen Nissenbaum, 'Values in Design: Theory and Practice,' in Jeroen Van den Hoven and John Weckert (eds.) *Information Technology and Moral Philosophy* (2007). Ann Cavoukian, *Privacy by Design .... Take the Challenge* (2009), available at https://ozone.scholarsportal.info/bitstream/1873/14203/1/291359.pdf, 2009).

[28] Mireille Hildebrandt, 'Legal Protection by Design', (2011) *Legisprudence*, 223ff.

[29] E.g. B.J. Koops, 'Should ICT Regulation Be Technology-Neutral', in B.J. Koops et al. (eds.) *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners* (2006), 77ff; Chris Reed, 'Taking Sides on Technology Neutrality', (2007) 4 *SCRIPT-ed* 3, 263ff; Mireille Hildebrandt and Laura Tielemans, 'Data Protection by Design and Technology Neutral Law', (2013) *Computer Law & Security Review*, ff. In most of the literature the notion of *technologically* neutral law is used interchangeable with *technology* neutral law. This chapter reserves the terms for two levels of analysis; the first for an analysis of technology as co-

technology neutral law can be understood within a relational conception of law, if we agree that neither law nor technology are neutral.

As discussed above, both law and technology generate specific normativities, whether or not this is intentional. The basic intuition that informs the notion of technology neutral law is that the law should apply equally to all, thus also having the same type of legal effect irrespective of the involvement of whatever technology. Whether a person commits murder with the help of a knife or by means of a computer virus, the idea is that the legal norm 'thou shalt not kill' can best be formulated without reference to the instrument used.[30]

Having studied the arguments that have been provided for technology neutral law, we have detected three types of objectives which inform the idea that legislation should aim to be neutral with regard to whatever technologies it encounters.[31] For our purposes the most relevant is the compensation objective. This requires that new technologies which alter the effectiveness or the substance of legal protection warrant reconfigurations in the legal framework to reinstitute what got lost. For instance, loss of protection may be due to the intrusive and invisible nature of criminal profiling informed by artificial intelligence, which may turn the presumption of innocence inside out, creating a de facto presumption of guilt. This requires additional legislation or a reconfiguration of the legal framework to compensate for the loss of effective protection. Thus *technology neutral law* sometimes requires *technology specific law* to redress undesirable disruptions of existing human rights law.

4 CRIMINAL LAW IN A DATA-DRIVEN SOCIETY

Though neither law nor technology are neutral instruments in the descriptive sense. However, in view of the compensation objective, constitutional democracy introduces a *normative neutrality,* that requires compensation in the case of adverse effects of novel technologies on the substance of legal protection. This section investigates what this means for the criminal law and how the advent of data driven environments challenges the mode of existence of the criminal law. To what extent do predictive analytics and other forms of artificial intelligence erode or enhance the preconditions of criminal law in a constitutional democracy? How does the preemption of intent enabled by machine learning combined with hyperconnectivity across national borders affect the aims of justice, legal certainty and purposiveness of the criminal law? Finally, how can we provide compensation for adverse effects of data driven architectures on the substance of the presumption of innocence; to what extent do we need a legal obligation on private and public data controllers to ensure a 'presumption of innocence by design', similar to privacy or data protection by design?

---

determinate of the mode of existence of law, the second for an analysis of how modern law aims to regulate the design, availability and usage of specific technologies.

[30] Such a virus can e.g. cause lethal harm in a patient using a medical implant.

[31] The innovation objective, the sustainability objective and the compensation objective, cf. Hildebrandt and Tielemans (n. 29).

4.1 A RELATIONAL CONCEPTION OF THE CRIMINAL LAW

A relational conception of law and a pluralist conception of technology entail a normative theory of the criminal law, aligned with the normative foundations of constitutional democracy. One of the most interesting and convincing normative theories of law is Radbruch's antinomian understanding of the law. In his famous *Legal Philosophy* Radbruch defines law as a cultural artefact that aims for justice, legal certainty and purposiveness,[32] hoping to generate fairness, trust and welfare. The choice for this particular threefold is motivated by the wish to steer clear of a moral theory of law which would reduce legal philosophy to moral philosophy, as well as a rejection of an outright positivism that would reduce law to the decisions of legislators and courts. Rejecting positivism does not, however, imply a denial of the important role played by the positiveness of the law and its complex alignment with the power to enforce. Radbruch's emphasis on legal certainty in fact celebrates the rule of law as sound protection against the arbitrary rule of men. Similarly, rejecting a moral theory of law does not mean to deny the constitutive importance of the inner morality of the law. According to Radbruch, the law's aim is to achieve justice as fairness and proportionality, not merely to achieve policy objectives in whatever way seems more effective. His rejection of political decisionism as the sole basis of law, however, does not deny the instrumentality of the law. The purposiveness of the law highlights its constitutive role in creating order and achieving welfare for its subjects. Instrumentality should not be confused with instrumentalism.

For the criminal law *justice* entails a focus on a fair attribution of punishment, where the fairness refers to the procedural justice of the fair trail, and to distributive and proportional substantive justice. Distributive justice means that equivalent criminal offences are punished similarly (equal treatment); proportional justice means that the measure of punishment depends on the gravity of the offense (which includes the harm it causes, the wrongness it entails and the guilt that is implied). Distributive and proportional fairness interrelate, because ensuring equivalent punishment assumes a measure of punishment that should be provided by the measure of proportional fairness. There is, of course, no objective standard to determine this measure. This means that democratic legislation and adjudication should constitute and legitimize the standards that are applied. This relates substantive justice to the procedural values of participation, deliberation and the contestability of governmental interventions. The fairness of the trial hinges on a set of principles such as the presumption of innocence, the independence of the court, the immediacy of the proceedings, the equality of arms between prosecution and defence, and internal and external publicity. Procedural fairness thus incorporates substantive moral values such as the right to contest the state's decisions in a court of law whenever they have a major impact on one's life. The fair trial also asserts the simultaneity of the constitution *and* the limitation of the *ius puniendi*; lawful punishment can – in principle – only be attributed after a fair trial. The fair trial is a precondition for fair punishment.

Distributive and proportional justice as well as procedural justice is aligned with *legal certainty*, since it provides those who share jurisdiction with legitimate expectations on the consequences of their actions. Within the criminal law legal certainty is even more significant than in other fields of law, because of the impact of

[32] Gustav Radbruch, Legal Philosophy, in Emil Lask and Curt Wilk, *The Legal Philosophies of Lask, Radbruch and Dabin* (1950), 47ff. On a normative theory of criminal law see notably R.A. Duff, *Punishment, Communication, and Community* (2001).

punishment on individual lives. A relational conception of law entails that the criminal law should be as clear and as precise as possible for two reasons. First, since the law is an instrument to prevent crime it should provide clear guidance on what a society considers to be a criminal offence; otherwise no deterrent effect can be expected. Second, since the law should always be goal-oriented as well as protective (creating competences and limiting their scope), those addressed by the criminal law should be aware in advance when their actions will be interpreted as liable to punishment. The first reason is focused on deterrence and prevention, the second is focused on fairness and retribution. Within a relational conception of law these reasons are not alternative but should both inform the criminalization, the criminal investigation and the adjudication of allegedly criminal conduct.

The criminal law targets the *legitimate goal* of reducing and redressing crime, thus upholding the legal norm that has been violated. Criminalization should be restricted to a set of wrongs that warrant the censure of society, without unnecessary violations of human rights freedoms such as privacy, freedom of speech or religion. Some would invoke the harm principle here, which however raises the difficult question of what is harm. Within a relational theory of law the more important question would be who decides what is harm, how this decision is prepared and to what extent such decisions are constraint by the protection of minorities or weaker voices within the constituency. The focus is thus on democratic participation in the process of criminalization, limited by the constraints of constitutional government and by the effective respect for human rights. This assumes that democracy should not be understood outside the bounds of a substantive conception of the Rule of Law, as it may otherwise generate populism and criminalize conduct disliked by a majority or an influential minority that manages to control popular opinion.

4.2 FROM AN INFORMATION SOCIETY TO A DATA-DRIVEN SOCIETY

The time that 'Information Law' and 'Law and Informatics' were niches in legal research will soon be over. The datafication and the hyperconnectivity generated by interconnected computing systems are in the process of transforming the concept of law as an autonomous discipline that reigns within the confines of the nation state to a notion of law as a more responsive discipline that must find new ways of relating to computer science, information theory, artificial intelligence and cybernetics. The challenge for law will be to engage with these other disciplines without either sacrificing or petrifying its identity. In this section we shall discuss the upheaval caused by the increased automation of decision-making, notably when based on machine learning. This relates to the shift from an information society, where more information is a good thing that enables better judgment, to a data-driven society that is flooded by data, where more information risks a loss of meaning. Due to the volume, speed and immediacy of the availability of ever more data, Big Data turns into noise until computational techniques enable the retrieval of 'valid, novel, potentially useful, and ultimately understandable patterns in data'.[33] Note that this entails the creation of new types of knowledge, often depicted as the holy grail of Big

[33] This is the definition of 'knowledge discovery in databases' (KDD), one of the most prominent techniques to select and indeed *construct* new knowledge and information. Usama M. Fayyad et al., *Advances in Knowledge Discovery and Data Mining* (1996), 41ff.

Data,[34] with the promise of added value for commerce, healthcare, tax fraud detection and other forms of crime control. The bottom line is that these techniques are thought to enable the prediction of future behaviours. In this section we briefly explain the workings of 'predictive analytics' and the kind of decisions it generates.

In their *Artificial Intelligence. A Modern Approach*,[35] Russell and Norvig explain the development of artificial intelligence (AI) as an interdisciplinary research domain, building on mathematics, economics, neuroscience, psychology, linguistics, computer engineering and cybernetics. Instead of looking for ways to merely imitate the intelligence of human beings, intelligent systems are now constructed to prepare and often execute decisions. Core to the current concept of AI is the notion of an intelligent agent that is capable of taking relatively autonomous decisions, depending on its perception and cognition of its environment. The emphasis on agency implies that we are not dealing with a rigid execution of rules but with systems capable of learning how to improve their performance on the basis of feedback. As these systems get to be more complex it becomes next to impossible for a single person to foresee the repercussions of alternative architectural choices. Though humans determine the goals, artificial agents will necessarily reconfigure these goals while seeking the smartest way to achieve them. Therefor architecture, the design of the computational decision systems that run an increasing part of our life world, is politics;[36] it impacts the kind of outcomes that are enabled and these are never neutral. For similar reasons Lawrence Lessig claimed that 'architecture (or computer code) is law', referring to the regulatory potential of computational architectures.[37]

The most transformative AI technology is machine learning, based on knowledge discovery in databases (KDD). The idea is that the use of computerized algorithms allows for patterns-detection in very large data sets. These patterns have not necessarily been hypothesized before their 'discovery'. They may have been 'mined' from the data by means of advanced statistical techniques. For instance, nodal policing is increasingly based on the use of Big Data to infer what types of crime will be committed where, when, and how. By running algorithms on a massive amount of data it is possible to predict the occurrence of criminal behaviours in specific neighbourhoods, at specific times. This supposedly enables the police to reconfigure and manage its presence more efficiently and effectively.[38] The inferences on which all this is based do not merely confirm or falsify existing beliefs about where disturbances are most likely to occur. They may also point in new, unexpected directions. This has even led some protagonists of Big Data analytics to claim that

[34] Cf. Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (2013).

[35] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3rd ed. (2009).

[36] Jeanette Hofmann, 'Et in Arcadia Ego. From Techno-Utopia to Cybercrime,' in Helen Margetts and Christopher Hood (eds.) *Paradoxes of Modernization:Unintended Consequences of Public Policy Reform* (2010), referring at 90 to Mitchell Kapor (1991), see http://cyber.law.harvard.edu/archived_content/people/reagle/inet-quotations-19990709.html.

[37] Lawrence Lessig, *Code Version 2.0* (2006).

[38] Arie van Sluis, Peter Marks, and Victor Bekkers, 'Nodal Policing in the Netherlands: Strategic and Normative Considerations on an Evolving Practice', (2011) 5 *Policing* 4, 365ff. Somini Sengupta, 'In Hot Pursuit of Numbers to Ward Off Crime,' Big Data 2013, *The New York Times. Technology. Bits Blog*, June 19, 2013, http://bits.blogs.nytimes.com/2013/06/19/in-hot-pursuit-of-numbers-to-ward-off-crime/.

they will diminish unjustified racial profiling or redlining. From now on, discrimination will be based on objective calculations, or so they say.[39]

Machine learning goes one step further than KDD. It integrates machine-wise pattern recognition with machine-wise responses, enabling automated decision systems to gain a measure of autonomy:

> A machine learns with respect to a particular task T, performance metric P, and type of experience E, if the system reliably performs its performance P at task T following experience E.[40]

This implies that machines have ways to perceive their environment and to anticipate – statistically – how their own subsequent behaviours will influence their ability to achieve certain goals. Depending on the architecture machine learning may leave more or less room for independent machine interventions. Computing systems will thus develop something akin to what we call agency, while taking care of our physical and institutional surroundings, surreptitiously adapting them to our inferred preferences (or to the strategic objectives of whoever is paying for these systems). Some have compared the proactive accommodation of smart environments to the subliminal adaptations of the autonomic nervous system that sustains the homeostasis of individual persons. IBM termed one of its recent computing research projects 'autonomic computing',[41] highlighting the resemblance with the autonomic nervous system of biological agents. This raises the question of the difference between autonomous action and autonomic computing. Whereas the latter produces a form of mindless agency, human autonomy stands for mindful agency, including the ability to give reasons for one's actions.

To the extent that decisions informed by predictive analytics and adaptive computing cause harm, they raise a number of questions for the criminal law. What if a doctor based her decision to perform surgery on her knowledge management system that calculated the best treatment?[42] If the patient suffers brain damage because the analytics were mistaken, should we blame the doctor, the software designer, the vendor or the patient who decided to hide part of her health records? This type of questions becomes more urgent where the software actually decides what action to undertake. This is where the notion of agency becomes pivotal: is the computer executing a set of rules that lead to foreseeable results or is the computer capable of reconfiguring its operations to achieve results that resolve problems in unforeseen ways? Within the sciences of AI, the latter would be a sign of agency and intelligence. The smarter the system, the less predictable it will be, and the more added value it will create for its human masters. As long as everything works out fine this seems

---

[39] Cp. Bernard E. Harcourt, *Against Prediction : Profiling, Policing, and Punishing in an Actuarial Age* (2007). Though they may not claim objectivity Mayer Schonberger and Cukier seem to overrate the objectivity achieved by the mere amount of data, see Mayer-Schonberger and Cukier (n. 34). Critical about this danah boyd and Kate Crawford, 'Critical Questions for Big Data', (2012) 15 *Information, Communication & Society* 5, 662ff.

[40] Tom M. Mitchell, *The Discipline of Machine Learning* (2006), available at http://www-cgi.cs.cmu.edu/~tom/pubs/MachineLearningTR.pdf, 2006).

[41] Jeffrey O. Kephart and David M. Chess, 'The Vision of Autonomic Computing', (2003) *Computer* (January), 41ff.

[42] Katie Hafner, 'Software Programs Help Doctors Diagnose, but Can't Replace Them', *The New York Times*, December 3, 2012, http://www.nytimes.com/2012/12/04/health/quest-to-eliminate-diagnostic-lapses.html.

entirely beneficial, but once artificial agents take decisions that cause harm their mindless agency challenges conventional notions of agency in the criminal law.

4.3 THE ANTINOMIES OF THE CRIMINAL LAW IN A DATA-DRIVEN SOCIETY

Data driven societies challenge the criminal law's antinomian aims for justice, legal certainty and purposiveness. This is partly due to the new types of crime that emerge with the advent of interconnected computing networks which constitute a hidden, computational layer of decision systems. In an earlier phase of digitalisation, legal scholars spoke of computer crime, usually differentiated as crimes where the computer is the tool, as those where computers are the target and as those where the computer plays an incidental role.[43] Tool-crimes are, for example, ID theft and online fraud, while examples of target-crimes are the use of malware and hacking. Next to these many existing crimes can be committed while using a computer, though other tools might have been used to commit the same crime. We can think of extorting or blackmailing a person via email or, even more mundane, hitting a person on the head with an iMac.

Data driven societies, however, thrive on interconnected computational decision systems that change the scope, the (often invisible) intrusiveness, the coerciveness and the distribution of human action. Rather than speaking of computer crime, scholars now refer to the criminal behaviours enabled by these systems as cybercrime, highlighting the hyperconnectivity and the artificial intelligence that nourish these offences. Cybercrime differs from ordinary crime in terms of distance (remote hacking), scale (DDOS attack, spam), speed (real-time dissemination of malware), automation (Webbots tracing and tracking vulnerabilities, DDOS attack) and interconnectivity (peer-to-peer file sharing of malicious software, remote hacking).[44] All this impacts the aim for justice, legal certainty and the purposiveness of the criminal law.

First, the aims of *distributive and proportional justice* are faced with disruptions in the attribution of punishment as well as the procedural safeguards that constitute the fair trial. The distance between a human action and its consequences increases exponentially if criminal offences are committed via online applications. This has implications for the jurisdiction that determines whether an action is criminalized and decides the measure of punishment. Since the person or organisation committing the offence may reside in another jurisdiction than the one in which the criminalized effects materialize, different standards of criminalization and punishment may apply. Equivalent distribution and proportional retribution may both be violated. The same goes for the procedural safeguards that may differ between jurisdictions, creating problems in the case of extradition or judicial cooperation. Different conceptions of fairness, incompatible investigative techniques and contradictory standards of evidence may disturb the legitimate expectations of criminal justice that reign within a particular jurisdiction, thus also challenging the *legal certainty* that sustains positive law. The scale or reach of computerized decision and operations increases the impact of criminal offences on all accounts. Together with the speed, the automation and the interconnectivity this raises the issue of distributed responsibility.

---

[43] Susan W. Brenner, *Cybercrime Criminal Threats from Cyberspace* (2010).

[44] Mireille Hildebrandt, 'Balance or Trade-off? Online Security Technologies and Fundamental Rights', *Philosophy & Technology*: 1ff.

Is it still possible to attribute causality to the action of an individual person if her actions are induced and mediated by a host of interacting computing systems that transform the implications of her actions in ways that are difficult to foresee?[45] To what extent will distributed artificial intelligence interfere with the casting of blame to a single human node in the network of human-machine interventions? The combination of scale, speed, automation and hyperconnectivity also impacts the distribution and proportionality of law enforcement and punishment. For some it may become very easy to escape the reach of justice authorities, whereas others can easily be traced and tracked across various contexts and jurisdictional borders.[46]

Second, the aim of *legal certainty* is disrupted by the distance between an action and its consequences. This causes problems because of the lack of extraterritorial jurisdiction to enforce and because of differential criminalizations, that refer to cultural diversity as to what is considered a criminal offence. Simultaneously, cybercrime law enforcement may transform into cyber war. If states decide to enforce their criminal law on the territory of another state, without its permission, this may be qualified as an act of war, triggering retaliation and generating interstate conflicts that transform the logic of the criminal law into that of the law of war. This will further the blurring of the border between intelligence and policing, and fit the agenda of those seeking to attribute far reaching emergency competences for law enforcement. For a citizen it will become less clear what a police officer is allowed to do, what kind of knowledge is gained between justice authorities and intelligence services and which of her behaviours will trigger intensified tracing and tracking. The combination of speed, automation and interconnectivity may require faster - even real-time – responses to cybercrime. It may be more difficult to ensure the foreseeability of the measures needed to counter real-time automated remote attacks, for instance on critical infrastructure. The difficulties of coping with novel technologies capable of causing large-scale disruptions of the monopoly of violence may elicit more surreptitious surveillance. For instance, the advent of 3D printing will enable the online sharing of software to build weapons and/or drones, calling for more pervasive monitoring of the content of online communications. The call for broader competences and more pervasive surveillance will erode legal certainty as it will be more difficult to define the legal boundaries of criminal law enforcement. Certainty as to what law enforcement *will do* and what *knowledge it may have obtained and inferred* will become illusionary at some point.[47]

Third, the *purposiveness* of law is increasingly lost due to the emergent behaviours of socio-technical infrastructures. The criminal law's instrumentality in achieving the policy goal of reducing and redressing crime, is eroded by the mediation of computational layers that are nested between intended objectives and actual outcomes. The instrumental character of the law as a means to prevent and deter criminal offences assumes a measure of linearity between legal conditions (framed in legislation and case law) and legal effect. Due the distance between the criminalization of specific behaviours and its consequences in other parts of the world, it becomes difficult if not impossible to foresee the legal effect of criminalization. Similarly, due to the scale of interacting computing systems on which

[45] C.E.A. Karnow, 'Liability for Distributed Artificial Intelligences', (1996) 11 *Berkely Technology Law Journal*, 148ff.

[46] Jack Goldschmidt, 'The Internet and the Legitimacy of Remote Cross-Border Searches', (2001) *The University of Chicago Legal Forum* 1, 103ff.

[47] Matt Buchanan, 'How the N.S.A. Cracked the Web', *The New Yorker Blogs*, September 7, 2013, http://www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html.

critical infrastructure depends, the legal effects of law meant for one context easily leak into other contexts that are connected via the computational in-between. The network effects generated by the combination of speed, automation and interconnectivity effectively turn the environment of the law into one better described by complexity theory than systems theory, meaning that it becomes ever more difficult to guess how legal interventions reconstitute the future. Democratic participation in the process of criminalization limited by constitutional constraints and effective respect for human rights thus becomes a challenge wherever the legal effect of such criminalization is easily overruled by the transformative affordances of a changing technological landscape, or by the limited scope of national jurisdiction.

The following section will highlight some of the more salient implications for substantive criminal law and law enforcement, notably the emerging architecture of a surveillance society and, for instance, its correlation with precrime punishment. Instead of succumbing to techno-determinism, however, the chapter will end with an argument for 'legal protection by design', to retain and reinvent the criminal law as an instrument for fairness (justice), trust and foreseeability (legal certainty), and public benefit (purposiveness).

4.4 PRESUMPTION OF INNOCENCE BY DESIGN?

Though the NSA's infiltration of private enterprise and independent standard-setting fora may not have surprised experts working in the domain of computer security or international relations, the extent of its access to content and metadata has evoked outcry even amongst the most cynical advocates of human rights, Rule of Law and democracy. This is obviously connected with the rise of data-driven society which enables to mine both content and metadata, inferring a plethora of crime-related patterns that may enable to preempt, prevent or resolve crimes. At the same time the fact that a high level systems administrator requires access to a mass of highly confidential classified information to keep the systems running, indicates the dependence of intelligence and law enforcement on technical experts who may have entirely unpredictable loyalties as far as data-driven intelligence goes.[48] We now have to admit that we live in the midst of surveillance societies,[49] that urgently require new checks and balances to survive as constitutional democracies sustaining fairness, trust and welfare.

A data-driven surveillance society threatens many of the core principles of the criminal law, especially when there is no transparency about the profiles that are inferred and matched with a person's data points. In this final section we single out the presumption of innocence and its relation to the predictive analytics that progressively drive law enforcement, because it connects with many of the requirements of procedural, distributive and proportional justice. The presumption incorporates the fact that the burden of proof in criminal proceedings rests on the prosecutor and demands strong evidence (beyond reasonable doubt). It entails that a person is considered innocent until proven guilty, whereas data-drive surveillance deftly lures law enforcement into the opposite direction. Notably, the presumption is

[48] Joe Davidson, 'NSA to Cut 90 Percent of Systems Administrators', Washington Post, *Federal Eye*, August 13, 2013, http://www.washingtonpost.com/blogs/federal-eye/wp/2013/08/13/nsa-to-cut-90-percent-of-systems-administrators/.

[49] David Lyon, *Surveillance Studies: an Overview* (2007).

also associated with the notion of equality of arms in criminal proceedings, with the right to privacy as a firewall against unwarrented investigative techniques and with the right to non-discrimination as a way to protect against prejudice and unfair bias. Surveillance society easily crosses the border that should protect individual persons who wish to reinvent themselves in spite of all the statistics that pin them to their past behaviours.

One pivotal example of the reach of data-driven surveillance concerns the advances made in neuroscience. On the one hand, mechanistic interpretations of the correlations between brain behaviours and proneness to criminal intent may erode our notions of human autonomy, guilt, blameworthiness and accountability. Such mechanistic interpretations have already – on the basis of mere correlations – evoked a salient discussion on the meaning of free will within the criminal law.[50] On the other hand, similar research may be used to detect liars and outliers in the context of criminal intelligence, aiming to preempt crime rather than respond after the fact. In both cases neuroscience is taken to enable new methods to manipulate people into certain types of behaviours, based on predictions of how their brain states will correlate with external stimuli and their own behaviours. Obviously, the privacy implications of such usage are gross. One might even wonder what privacy could mean in an era where nervous systems can be connected directly to computer interfaces and to the nervous system of another person.[51] The most problematic issue here is not merely the fact that interesting patterns are mined which correlate brain behaviours or morphology with human mind and society, thus enabling manipulation of human action. The real problem resides in the naïve interpretation of such pattners in terms of, for instance, evolutionary metaphors,[52] or a new type of mechanics that defies causality while displaying an unsubstantiated belief in statistical correlations.[53] Typically, an ingenuous 'belief' and a somewhat naïve misrepresentation of the findings of neuroscientific research tempts policy makers to build data-driven infrastructures supposedly capable of forecasting who will engage in criminal – or undesirable – behaviours. The lure of gaining access to thoughts, intentions and dispositions may induce vast public private surveillance networks to capture the data points that correlate with high risk behaviours. Such systems will not necessarily be restricted to criminal offences, as information-driven governments will seek to employ them for risk-based healthcare, criminal policy, social security allocation, employment programs and all types of sophisticated nudging operations. Coupled with the naïve idea that neuroscience has already proven that free will is an illusion, the borders between criminal law enforcement and the preemption of undesirable behaviours will be further destabilized, creating leeway to foster what has been called 'precrime punishment'.[54]

Since the proliferation of personal data processing systems, researchers on the cusp of law, human machine interaction and computer science have been working on

---

[50] E.g. Stephen J. Morse, 'Brain Overclaim Syndrome and Criminal Responsibility: A Diagnostic Note', (2006) 3 *Ohio State Journal of Criminal Law* 2, 397ff. Against overly sceptical accounts of human autonomy Antonio R. Damasio, *Self Comes to Mind : Constructing the Conscious Brain* (2011).

[51] K. Warwick et al., 'Thought Communication and Control: a First Step Using Radiotelegraphy', (2004) *Communications, IEE Proceedings* 3, 185ff.

[52] Bernd Carsten Stahl, 'Evolution as Metaphor: A Critical Review of the Use of Evolutionary Concepts in Information Systems and e-Commerce', in Ned Kock (ed.) *Evolutionary Psychology and Information Systems Research* (2010), 357ff.

[53] Kate Crawford, 'Think Again: Big Data,' (2013) *Foreign Policy*, May 9.

[54] Hildebrandt (n. 54).

privacy by design. Convinced of the normative impact of interconnected semi-autonomous computing systems on the substance of human rights, they have aligned with research into value-sensitive design and argued that privacy must be an affordance of the infrastructures on which we depend. Trying to regulate such systems after their consolidation will not work. According to many privacy advocates, the opacity of individual persons that is core to privacy must be built into the so-called 'backend' of these systems as they are designed. The focus on privacy is understandable, but surveillance is not only about prying into the private sphere. As argued above, data-driven surveillance challenges the foundations of the presumption of innocence by suggesting precognition of criminal intent. Even if internal critique demonstrates that crucial assumptions of criminal profiling are invalid,[55] law enforcement and criminal intelligence have already embraced the assumed benefits of Big Data and will increasingly base their criminal justice policy on the outcomes of computational risk assessments. The logic of these policies goes against the grain of the presumption of innocence. If criminal law does not reinvent itself the presumption of innocence will turn into a relic of outdated – bookish - Enlightenment thought.

True to the pluralist conception of technology and the relational conception of law, we should acknowledge that the extent to which data-driven surveillance societies will erode the presumption of innocence will depend on the design of the surveillance infrastructures. Though it may appear to be a mission impossible, the antinomian aims of the criminal law require a surveillance architecture that sustains the presumption of innocence. Next to privacy and non-discrimination by design, we will need a presumption of innocence by design. This will depend on collaboration between criminal law scholars and practitioners, requirements engineering, human machine interfacing experts, and those involved in technology impact assessment. Key features of surveillance systems that operationalize the presumption of innocence will be the transparency of the architecture (to know what type of data are observed and inferred how, where and for how long), access to the algorithms that claim to predict criminal intent (to enable peer review of the mechanics involved), software verification (to make sure that knowledge of these systems does not depend on the beneficience of the system owners willing to share their code), and, finally, ICT citizens' platforms that allow citizens to foresee how their behaviours could match with criminal profiles (to empower individuals in the face of anonymous data processing by secret services or private enterprises forced to share their data with criminal or foreign intelligence). These types of 'legal protection by design' should ensure an effective capability to contest allegations based on data-driven criminal profiling. This should reinvent procedural, distributive and proportional criminal justice, by opening the black box of data-driven applications and achieving their contestability in a court of law; it should re-incribe legal certainty into the hybrid socio-technial systems, by giving people control over the consequences of their interactions; and, it should re-enable the purposiveness and instrumentality of the criminal law in the face of shifting interactions between inferred 'present futures' and their own *future present*.[56]

[55] Harcourt (n. 39).

[56] Elena Esposito, *The Future of Futures: The Time of Money in Financing and Society* (2011). More specifically in relation to the law: Elena Esposito, 'Digital Prophecies and Web Intelligence', in Mireille Hildebrandt and Katja de Vries (eds.) *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology* (2013), 121ff.

5 CONCLUDING OBSERVATIONS

In this chapter we have looked into the relationships between law and technology, highlighting the transformations of the criminal law in the face of a data-driven society. Instead of embarking on a straightforward discussion of cybercrime and law enforcement in cyberspace, this chapter devoted considerable attention to the assumptions that inform lawyers' understanding of both law and of technology. Depending on such assumptions different types of relationships between legal norms, legal relations and legal systems and technological devices and infrastructures can be configured in different ways. In times of disruptive technological transformations it is crucial to reflect on the meaning of both law and technology in relation to notably self, mind and society. Legal systems and technological infrastructures mediate between individual minds and societal institutions, co-constituting patterns of interaction and consolidating complex mutual expectations between citizens, government agencies and other organisations. This chapter has highlighted that modern law itself has been mediated by information and communication technologies (ICTs), such as the printing press, while at the same time the hyperconnectivity and artificial intelligence of current ICT infrastructures may limit or reinvent the substance of legal protection. This has major implications for the normative force of the criminal law, notably for its aim to achieve procedural, distributive and proportional justice, legal certainty and for its aim to contribute to specific policy goals such as a reduction of cybercrime. The chapter ends with an argument for a 'presumption of innocence by design' that should inform the architecture of the data-driven surveillance state, precisely because we cannot take for granted that novel technological landscape will afford the same rights and freedoms as earlier ones.