7

Law Enforcement and Data-Driven Predictions at the National and EU Level

A *Challenge to the Presumption of Innocence and Reasonable Suspicion?*

Francesca Galli

7.1 INTRODUCTION

Technological progress could constitute a huge benefit for law enforcement and criminal justice more broadly.[1] In the security context,[2] alleged opportunities and benefits of applying big data analytics are greater efficiency, effectiveness, and speed of law enforcement operations, as well as more precise risk analyses, including the discovery of unexpected correlations,[3] which could nourish profiles.[4]

The concept of 'big data' refers to the growing ability of technology to capture, aggregate, and process an ever-greater volume and variety of data.[5] The combination of mass digitisation of information and the exponential growth of computational power allows for their increasing exploitation.[6]

[1] See, e.g., H Fenwick (ed), *Development in Counterterrorist Measures and Uses of Technology* (Routledge 2012). See also, on policing more specifically, National Institute of Justice, *Research on the Impact of Technology on Policing Strategy in the 21st Century. Final Report*, May 2016, www.ncjrs.gov/pdffiles1/nij/grants/251140.pdf, accessed 27 July 2020; J Byrne and G Marx, 'Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact' (2011) 20(3) *Cahiers Politiestudies* 17–40.

[2] B Hoogenboom, *The Governance of Policing and Security: Ironies, Myths and Paradoxes* (Palgrave Macmillan 2010).

[3] J Chan, 'The Technology Game: How Information Technology Is Transforming Police Practice' (2001) 1 *Journal of Criminal Justice* 139.

[4] D Broeders et al., 'Big Data and Security Policies: Serving Security, Protecting Freedom' (2017) *WRR-Policy Brief* 6.

[5] For instance, data acquisition is a kind of data processing architecture for big data, which has been understood as the process of gathering, filtering, and cleaning data before the data are put in a data warehouse or any other storage solution. See K Lyko, M Nitzschke, and A-C Ngonga Ngomo, 'Big Data Acquisition' in JM Cavanillas et al. (eds), *New Horizons for a Data-Driven Economy. A Roadmap for Usage and Exploitation of Big Data in Europe* (Springer 2015).

[6] S Brayne, 'The Criminal Law and Law Enforcement Implications of Big Data' (2018) 14 *Annual Review of Law and Social Science* 293.

https://doi.org/10.1017/9781108914857.008 Published online by Cambridge University Press

A number of new tools have been developed. Algorithms are merely an abstract and formal description of a computational procedure.[7] Besides, law enforcement can rely on artificial intelligence (i.e., the theory and development of computer systems capable of performing tasks which would normally require human intelligence), such as visual perception, speech recognition, decision-making, and translation between languages.[8] For the purpose of this contribution, these systems are relevant because they do not simply imitate the intelligence of human beings; they are meant to formulate and often execute decisions. The notion of an allegedly clever agent, capable of taking relatively autonomous decisions, on the basis of its perception of the environment, is in fact, pivotal to the current concept of artificial intelligence.[9] With machine learning, or 'self-teaching' algorithms, the knowledge in the system is the result of 'data-driven predictions', the automated discovery of correlations between variables in a data set, often to make estimates of some outcome.[10] Correlations are relationships or patterns, thus more closely related to the concept of 'suspicion' rather than the concept of 'evidence' in criminal law.[11] Data mining, or 'knowledge discovery from data', refers to the process of discovery of remarkable patterns from massive amounts of data.

Such tools entail new scenarios for information gathering, as well as the monitoring, profiling, and prediction of individual behaviours, thus allegedly facilitating

[7] RK Hill, 'What an Algorithm Is' (2016) 29 *Philosophy and Technology* 35–59; TH Cormen et al., *Introduction to Algorithms* (3rd ed., The MIT Press 2009).

[8] K Yeung for the Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT), *A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework*, Council of Europe study DGI(2019)05, September 2019, https://rm.coe.int/responsability-and-ai-en/168097d9c5, accessed 27 July 2020.

[9] On the role of algorithms and automated decisions in security governance, as well as numerous concerns associated with the notion of 'algorithmic regulation', see L Amoore and R Raley, 'Securing with Algorithms: Knowledge, Decision, Sovereignty' (2017) 48(1) *Security Dialogue* 3; C Aradau and T Blancke, 'Governing Others: Anomaly and the Algorithmic Subject of Security' (2018) 3(1) *European Journal of International Security* 1.

[10] See M Oswald et al., 'Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and "Experimental" Proportionality' (2018) 27(2) *Information & Communications Technology Law* 223; P MacFarlane, 'Why the Police Should Use Machine Learning – But Very Carefully', *The Conversation*, 21 August 2019, https://theconversation.com/why-the-police-should-use-machine-learning-but-very-carefully-121524, accessed 27 July 2020; D Lehr and P Ohm, 'Playing with the Data: What Legal Scholars Should Learn about Machine Learning' (2017) 51 *UCDL Rev* 653; 'Reinventing Society in the Wake of Big Data. A Conversation with Alex "Sandy" Pentland', *The Edge*, www.edge.org/conversation/reinventing-society-in-the-wake-of-big-data, accessed 27 July 2020.

[11] Although crime prevention should be rational and based on the best possible evidence. See BC Welsh and DP Farrington, 'Evidence-Based Crime Prevention' in BC Welsh and DP Farrington (eds), *Preventing Crime* (Springer 2007).

crime prevention.[12] The underlying assumption is that data could change public policy, addressing biases and fostering a data-driven approach in policy-making. Clearer evidence could support both evaluations of existing policies and impact assessments of new proposals.[13]

Law enforcement authorities have already embraced the assumed benefits of big data, irrespective of criticism questioning the validity of crucial assumptions underlying criminal profiling.[14] In a range of daily operations and surveillance activities, such as patrol, investigation, as well as crime analysis, the outcomes of computational risk assessment are increasingly the underlying foundation of criminal justice policies.[15] Existing research on the implications of 'big data' has mostly focused on privacy and data protection concerns.[16] However, potential gains in security come also at the expenses of accountability[17] and could lead to the erosion of fundamental rights, emphasising coercive control.[18]

This contribution first addresses the so-called rise of the algorithmic society and the use of automated technologies in criminal justice to assess whether and how the gathering, analysis, and deployment of big data are changing law enforcement activities. It then examines the actual or potential transformation

[12] See BJ Koops, 'Technology and the Crime Society. Rethinking Legal Protection' (2009) 1(1) *Law, Innovation and Technology* 93.

[13] M Leese, 'The New Profiling' (204) 45(5) *Security Dialogue* 494.

[14] For an in-depth study, see GG Fuster, *Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights*. Study Requested by the LIBE Committee. Policy Department for Citizens' Rights and Constitutional Affairs, PE 656.295, July 2020.

[15] A Završnik, 'Criminal Justice, Artificial Intelligence Systems, and Human Rights' (2020) 20 *ERA Forum* 567; P Hayes et al., 'Algorithms and Values in Justice and Security' (2020) 35 *Artificial Intelligence and Society* 533.

[16] C Kuner, F Cate, O Lynskey, C Millard, N Ni Loideain, and D Svantesson, 'An Unstoppable Force and an Immoveable Object? EU Data Protection Law and National Security' (2018) 8 *International Data Privacy Law* 1; O Lynskey, 'Criminal Justice Profiling and EU Data Protection Law' (2019) 15 *International Journal of Law in Context* 162; R Bellanova, 'Digital, Politics and Algorithms. Governing Digital Data through the Lens of Data Protection' (2017) 20(3) *European Journal of Social Theory* 329; J Hernandez Ramos et al., 'Towards a Data-Driven Society: A Technological Perspective on the Development of Cybersecurity and Data Protection Policies' (2020) 18(1) *IEEE Security and Privacy* 28.

[17] F Doshi-Velez and M Kortz, 'Accountability of AI Under the Law: The Role of Explanation' (2017) Berkman Klein Center Working Group on Explanation and the Law, Berkman Klein Center for Internet & Society working paper, https://dash.harvard.edu/bitstream/handle/1/34372584/2017-11_aiexplainability-1.pdf, accessed 25 August 2020.

[18] A Braga et al., 'Moving the Work of Criminal Investigators Towards Crime Control' in *New Perspectives in Policing*, (Harvard Kennedy School 2011); The European Commission for the Efficiency of justice (CEPEJ, Council of Europe), *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018), https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c, accessed 20 July 2020; Council of Europe's MIS-NET, 'Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications', https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html, accessed 2 August 2020.

of core principles of criminal law and whether the substance of legal protection[19] may be weakened in a 'data-driven society'.[20]

7.2 THE RISE OF THE ALGORITHMIC SOCIETY AND THE USE OF AUTOMATED TECHNOLOGIES IN CRIMINAL JUSTICE

7.2.1 *A Shift in Tools Rather than Strategy?*

One could argue that the development of predictive policing is more a shift in tools than strategy. Prediction has always been part of policing, as law enforcement authorities attempt to predict where criminal activities could take place and the individuals involved in order to deter such patterns.[21]

Law enforcement has over time moved towards wide-ranging monitoring and even more preventative approaches. Surveillance technologies introduced in relation to serious crimes (e.g., interception of telecommunications) are increasingly used for the purpose of preventing and investigating 'minor' offences; at the same time, surveillance technologies originally used for public order purposes in relation to minor offences (e.g., CCTV cameras) are gradually employed for the prevention and investigation of serious crime.[22] On the one side, serious crime including terrorism has had a catalysing effect on the criminal justice system, prompting increased use of surveillance techniques and technologies. The subsequent introduction of exceptional provisions has been first regarded as exceptional and limited in scope first to terrorism and then to organised crime. However, through a long-lasting normalisation process at the initiative of the legislator, specific measures have become institutionalised as part of the ordinary criminal justice system and have a tendency to be applied beyond their original

[19] The fundamental right to effective judicial protection has been one of the pillars of European integration, codified by the Treaty of Lisbon in Article 47 of the EU Charter of Fundamental Rights and Article 19(1) TEU. The CJEU has been insisting on the access for individuals to the domestic judicial review of any acts that may affect the interests of these individuals. Thus the CJEU sought to ensure not only the subjective legal protection of these individuals but also the objective legality of domestic administrative action implementing EU law, as well as ensuing unity and consistency in the application of EU law across different jurisdictions. However, specific requirements stemming from the right to effective judicial protection are not always clear. Effective judicial protection is largely a judge-made concept. There has been no comprehensive legislative harmonisation of domestic procedural provisions applied to implement EU law. See M Safjan and D Dusterhaus, 'A Union of Effective Judicial Protection: Addressing a Multi-level Challenge through the Lens of Article 47 CFREU' (2014) 33 *Yearbook of European Law* 3; R Barents, 'EU Procedural Law and Effective Judicial Protection' (2014) 51 *Common Market Law Review* 1437, 1445 ff.

[20] S Lohr, 'The Promise and Peril of the "Data-Driven Society"', *New York Times*, 25 February 2013, https://bits.blogs.nytimes.com/2013/02/25/the-promise-and-peril-of-the-data-driven-society/, accessed 27 July 2020.

[21] AG Ferguson, 'Policing Predictive Policing' (2017) 94(5) *Washington University Law Review* 1115, 1128–1130.

[22] C Cocq and F Galli, 'The Catalysing Effect of Serious Crime on the Use of Surveillance Technologies for Prevention and Investigation Purposes' (2013) 4(3) *NJECL* 256.

https://doi.org/10.1017/9781108914857.008 Published online by Cambridge University Press

scope.[23] On the other side, a parallel shift has occurred in the opposite direction. Video surveillance technologies, which are one of the most obvious and widespread signs of the development of surveillance, were originally conceived by the private sector for security purposes. They have been subsequently employed for public order purposes and finally in the prevention of minor offences and/or petty crimes (such as street crimes or small drug dealers), without any significant change in the level of judicial scrutiny and on the basis of a simple administrative authorisation. In such contexts, they were rather a tool to deter would-be criminals than an investigative means.[24] The terrorist threat has become an argument to justify an even more extensive deployment and use of video surveillance, as well as a broader use of the information gathered for the purposes of investigation.

Anticipative criminal investigations have a primary preventive function, combined with evidence gathering for the purpose of eventual prosecution.[25] The extensive gathering, processing, and storage of data for criminal law purposes imply a significant departure from existing law enforcement strategies. The relentless storage combined with an amplified memory capacity make a quantitative and qualitative jump as compared to traditional law enforcement activities. The growth of available data over the last two centuries has been substantial, but the present explosion in data size and variety is unprecedented.[26]

First, the amount of data that are generated, processed, and stored has increased enormously (e.g., internet data) because of the direct and intentional seizure of information on people or objects; the automated collection of data by devices or systems; and the volunteered collection of data via the voluntary use of systems, devices, and platforms. Automated and volunteered collection have exponentially increased due to the widespread use of smart devices, social media, and digital transactions.[27] The 'datafication'[28] of everyday activities, which is furthered driven by the 'Internet of Things',[29] leads to the virtually

[23] O Gross, 'Chaos and Rules' (2003) 112 *Yale Law Journal* 1011, 1090; D Dyzenhaus, 'The Permanence of the Temporary' in RJ Daniels et al. (eds), *The Security of Freedom* (University of Toronto Press 2001).

[24] For example, A Bauer and F Freynet, *Vidéosurveillance et vidéoprotection* (PUF 2008); EFUS, *Citizens, Cities and Video Surveillance, towards a Democratic and Responsible Use of CCTV* (EFUS 2010), 183–184; *Vidéo-surveillance Infos*, *'Dispositif de sécurité au stade de France: ergonomie et évolutivité'* (14 October 2011).

[25] See, e.g., MFH Hirsch Ballin, *Anticipative Criminal Investigations. Theory and Counter-terrorism Practice in the Netherlands and the United States* (TMC Asser Press 2012).

[26] R Van Brakel and P De Hert, 'Policing, Surveillance and Law in a Pre-crime Society: Understanding the Consequences of Technology-Based Strategies' (2011) 3(20) *Cahiers Politiestudies Jaargang* 163.

[27] G González Fuster and A Scherrer, 'Big Data and Smart Devices and Their Impact on Privacy', Study for the European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, PE 536.455, Sept 2015.

[28] 'Datafication' indicates the increasing on data-driven technologies.

[29] The Internet of Things is the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data. See J Davies and C Fortuna (eds), *The Internet of Things: From Data to Insight* (Wiley 2020).

unnoticed gathering of data, often without the consent or even the awareness of the individual.

Second, new types of data have become available (e.g., location data). Irrespective of whether law enforcement authorities will eventually use these forms of data, much of the electronically available data reveal information about individuals which were not available in the past. Plus, there is a vast amount of data available nowadays on people's behaviour.[30] Moreover, because of the combination of digitisation and automated recognition, data has become increasingly accessible, and persons can be easily monitored at distance.

Third, the growing availability of real-time data fosters real-time analyses. Thus the increased use of predictive data analytics is a major development. Their underlying rationale is the idea of predicting a possible future with a certain degree of probability.

7.2.2 *Interoperable Databases: A New Challenge to Legal Protection?*

Although police have always gathered information about suspects, now data can be stored in interoperable databases,[31] furthering the surveillance potential.[32] The possibility to link data systems and networks fosters the systematic analysis of computer processors as well as increased data storage capacity.

Interoperability challenges existing modes of cooperation and integration in the EU AFSJ and also the existing distribution of competences between the EU and Member States, between law enforcement authorities and intelligence services, and between public and private actors, which are increasingly involved in information-management activities. Moreover, large-scale information exchanges via interoperable information systems have progressively eroded the boundaries between law enforcement and intelligence services. Besides, they have facilitated a reshuffling of responsibilities and tasks within the law enforcement community, such as security and migration actors. Furthermore, competent authorities have access to huge amounts of data in all types of public and private databases. Interoperable information systems function not only across national boundaries but also across the traditional public-private divide.

[30] S Lohr (n 20).

[31] See J Ballaschk, *Interoperability of Intelligence Networks in the European Union: An Analysis of the Policy of Interoperability in the EU's Area of Freedom, Security and Justice and Its Compatibility with the Right to Data Protection*, PhD thesis, University of Copenhagen 2015 (still unpublished); F Galli, 'Interoperable Databases: New Cooperation Dynamics in the EU AFSJ?' in Special Issue a cura di D Curtin e FB Bastos (eds) (2020) 26(1) *European Public Law* 109–130.

[32] KF Aas et al. (eds), *Technologies of Insecurity. The Surveillance of Everyday Life* (Routledge 2009); see P De Hert and S Gutwirth, 'Interoperability of Police Databases within the EU: An Accountable Political Choice' (2006) 20 (1–2) *International Review of Law, Computers and Technology* 21–35; V Mitsilegas, 'The Borders Paradox' in H Lindahl (ed), *A Right to Inclusion and Exclusion?* (Hart 2009), at 56.

If, on the one hand, the so-called big data policing partially constitutes a restatement of existing police practices, then on the other hand, big data analytics bring along fundamental transformations in police activities. There has been also an evolution of the share of roles, competences, and technological capabilities of intelligence services and law enforcement authorities. The means at the disposal of each actor for the prevention and investigation of serious crime are evolving so that the share of tasks and competences have become blurred. Nowadays the distinction is not always clear, and this leads to problematic coordination and overlap.[33] Intelligence has also been given operational tasks. Law enforcement authorities have resorted to ever more sophisticated surveillance technologies and have been granted much more intrusive investigative powers to use them. Faith in technological solutions and the inherent expansionary tendency of surveillance tools partially explains this phenomenon. Surveillance technologies, in fact, are used in areas or for purposes for which they were not originally intended.[34]

Information sharing and exchange do not in itself blur the institutional barriers between different law enforcement authorities, but the nature of large-scale information-sharing activities does provide a new standing to intelligence activities in the law enforcement domain. The resources spent on and the knowledge developed by such large-scale information gathering and analysis are de facto changing police officers into intelligence actors or intelligence material users.

In addition, EU initiatives enhancing access to information by law enforcement authorities have a direct impact on the functional borders in the security domain. With the much-debated interoperability regulations,[35] the intention of the Commission has been to improve information exchanges not only between police authorities but also between customs authorities and financial intelligence units and in interactions with the judiciary, public prosecution services, and all other public bodies that participate in a process that ranges from the early detection of security threats and criminal offences to the conviction and punishment of suspects. The Commission has portrayed obstacles to the functional sharing of tasks as follows: 'Compartmentalization of information and lack of a clear policy on information channels hinder information exchange',[36] whereas there is, allegedly, a need to

[33] See J Vervaele, 'Terrorism and Information Sharing between the Intelligence and Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law?' (2005) 1(1) *Utrecht Law Review* 1.

[34] C Cocq and F Galli (n 22).

[35] *Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa*, OJ L 135/27, 22.5.2019; *Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration*, OJ L 135/85, 22.5.2019.

[36] In May 2004, the European Commission issued a Communication to the Council of Europe and the European Parliament aiming at enhancing law enforcement access to information by law enforcement agencies.

facilitate the free movement of information between competent authorities within Member States and across borders.

In this context, a controversial aspect of interoperability is that systems and processes are linked with information systems that do not serve law enforcement purposes, including other state-held databases and ones held by private actors. With reference to the first category, the issue to address concerns the blurring of tasks between different law enforcement actors. In fact, a key aspect of the EU strategy on databases and their interoperability is an aim to maximise access to personal data, including access by police authorities to immigration databases, and to personal data related to identification. This blurring has an impact on the applicable legal regime (in terms of jurisdiction) and also in terms of legal procedure (e.g., administrative/criminal). In fact, the purpose for which data are gathered, processed, and accessed is crucial, not only because of data protection rules but because it links the information/data with a different stage of a procedure (either administrative or criminal) to which a set of guarantees are (or are not) attached, and thus has serious consequences for the rights of individuals (including access, appeal, and correction rights). Neither legal systems nor legal provisions are fully compatible either because they belong to administrative or criminal law or because of a lack of approximation between Member State systems. Such differences also have an impact on the potential use of information: information used for identification purposes (the focus of customs officers at Frontex), or only for investigation purposes with no need to reach trial (the focus of intelligence actors), or for prosecution purposes (the focus of police authorities). Eventually, of course, the actors involved in the process have different impacts on the potential secret use of data, with consequent transparency concerns.[37]

7.2.3 A *'Public-Private Partnership'*

The information society has substantially changed the ways in which law enforcement authorities can obtain information and evidence. Beyond their own specialised databases, competent authorities have access to huge amounts of data in all types of public and private databases.[38]

Nowadays the legal systems in most Western countries thus face relevant changes in the politics of information control. The rise of advanced technologies has magnified the capability of new players to control both the means of communication and data flows. To an increasing extent, public authorities are sharing their regulatory competences with an indefinite number of actors by imposing preventive duties on the private sector, such as information-gathering and sharing (e.g., on telecommunication

[37] M Ananny and K Crawford, 'Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability' (2018) 20 *New Media and Society* 973; Eleni Kosta and Magda Brewczyńska, 'Government Access to User Data' in RM Ballardini, P Kuoppamäki, and O Pitkänen (eds), *Regulating Industrial Internet through IPR, Data Protection and Competition Law* (Kluwer Law Intl 2019), ch 13.

[38] See FH Cate and JX Dempsey (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data* (Oxford University Press 2017).

companies for data retention purposes).[39] This trend is leading to a growing privatisation of surveillance practises. In this move, key players in private information society (producers, service providers, key consumers) are given law enforcement obligations.

Private actors are not just in charge of the operational enforcement of public authority decisions in security matters. They are often the only ones with the necessary expertise, and therefore they profoundly shape decision-making and policy implementation. Their choices are nevertheless guided by reasons such as commercial interest, and they are often unaccountable.

In the context of information sharing, and particularly in the area of interoperable information systems, technical platform integration (information hubs) functions across national boundaries and across the traditional public–private divide. Most of the web giants are established overseas, so that often private actors – voluntarily or compulsorily – transfer data to third countries. Companies do not just cooperate with public authorities but effectively and actively come to play a part in bulk collection and security practices. They identify, select, search, and interpret suspicious elements by means of 'data selectors'. Private actors, in this sense, have become 'security professionals' in their own right.

Systematic government access to private sector data is carried out not only directly via access to private sector databases and networks but also through the cooperation of third parties, such as financial institutions, mobile phone operators, communication providers, and the companies that maintain the available databases or networks.

Personal data originally circulated in the EU for commercial purposes may be transferred by private intermediaries to public authorities, often also overseas, for other purposes, including detection, investigation, and prosecution. The significant blurring of purposes among the different layers of data-gathering – for instance, commercial profiling techniques and security – aims to exploit the 'exchange value' of individuals' fragmented identities, as consumers, suspects of certain crimes, 'good citizens', or 'others'.

In this context, some have argued that the most important shortcoming of the 2016 data protection reform is that it resulted in the adoption of two different instruments, a Regulation and a Directive.[40] This separation is a step backwards regarding the objective envisaged by Article 16 TFEU – which instead promotes a cross-sectoral approach potentially leading to a comprehensive instrument embracing different policy areas (including the AFSJ) in the same way. This is a weakness because the level of protection envisaged by the 2016 Police Data Protection Directive is de facto lower than in the Regulation, as data gathering for law enforcement and national security purposes is mostly exempted from general data protection laws or constitutes an exemption under

[39] V Mitsilegas, 'The Transformation of Privacy in an Era of Pre-emptive Surveillance' (2015) 20 *Tilburg Law Review* 35–57; HE De Busser, 'Privatisation of Information and the Data Protection Reform' in S Gutwirth et al. (eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer 2013).

[40] P Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' in M Cremona (ed), *New Technologies and EU Law* (Oxford University Press 2017).

those provisions even at the EU level.[41] Furthermore, what happens in practice mostly depends on terms and conditions in contractual clauses signed by individuals every time they subscribe as clients of service providers and media companies.

A further element of novelty is thus the linkage of separate databases, which increased their separate utility since law enforcement authorities and private companies partially aggregated their data.[42] Such a link between criminal justice data with private data potentially provides numerous insights about individuals. Law enforcement and private companies have therefore embraced the idea of networking and sharing personal information. Law enforcement thus benefits from the growth of private surveillance gathering of information.

The nature and origins of data that are available for security purposes are thus further changing. Public and private data are increasingly mixed. Private data gathering tools play a broader role in security analyses, complementing data from law enforcement authorities' sources.[43] An example is the use of social media analyses tools by the police together with intelligence (e.g., in counter-terrorism matters). It is often not merely the data itself which is valuable but the fact of linking large amounts of data.

Having examined the use of surveillance technologies for preventive and investigative purposes, it would be interesting to focus on the next phase of criminal procedure – that is, the retention and use of information gathered via surveillance technologies for the prosecution during trials for serious crimes, including terrorism. In fact, a huge amount of information is nowadays retained by private companies such as network and service providers, but also by different CCTV operators. The question is under which circumstances such information can be accessed and used by different actors of criminal procedures (police officers, intelligence services, prosecutors, and judges) for the purposes of investigating and prosecuting serious crimes. The retention of data for investigation and prosecution purposes poses the question of the collaboration between public authorities and private companies and what kind of obligations one may impose upon the latter.

7.3 THE TRANSFORMATION OF CORE PRINCIPLES OF CRIMINAL LAW

7.3.1 *Control People to Minimise Risk*

Technology is pivotal in the development of regulatory legislation that seeks to control more and more areas of life.[44]

[41] See Recital no. 19 and art. 2(d), GDPR.

[42] An interesting example are the data sets of the EU-US Passenger Name Records and Terrorism Financing Programs. See R Bellanova and M De Goede, 'The Algorithmic Regulation of Security: An Infrastructural Perspective' (2020) *Regulation and Governance*.

[43] AG Ferguson, *The Rise of Big Data Policing* (NYU Press 2017).

[44] K Brennan-Marquez, 'Big Data Policing and the Redistribution of Anxiety' (2018) 15 *Ohio State Journal of Criminal Law* 487; J Byrne and D Rebovich (2007), *The New Technology of Crime, Law and Social Control* (Criminal Justice Press 2007).

https://doi.org/10.1017/9781108914857.008 Published online by Cambridge University Press

In fact, predictive policing is grounded and further supports a social growing desire to control people to minimise risk.[45] Sociologists such as Ulrich Beck have described the emergence of a 'risk society': industrial society produces a number of serious risks and conflicts – including those connected with terrorism and organised crime – and has thus modified the means and legitimisation of state intervention, putting risks and damage control at the centre of society as a response to the erosion of trust among people.[46]

Along similar lines, Feeley and Simon have described a 'new penology' paradigm (or 'actuarial justice'[47]): a risk management strategy for the administration of criminal justice, aiming at securing at the lowest possible cost a dangerous class of individuals whose rehabilitation is deemed futile and impossible.[48] The focus is on targeting and classifying a suspect group of individuals and making assessments of their likelihood to offend in particular circumstances or when exposed to certain opportunities.

According to David Garland, the economic, technological, and social changes in our society during the past thirty years have reconfigured the response to crime and the sense of criminal justice leading to a 'culture of control' counterbalancing the expansion of personal freedom.[49] In his view, criminal justice policies thus develop from political actors' desire to 'do something' – not necessarily something effective – to assuage public fear, shaped and mobilised as an electoral strategy.

The culture of control together with risk aversion sees technological developments as key enabling factors and is intimately linked to the rise of a surveillance society and the growth of surveillance technologies and infrastructures.

Koops has built upon pre-existing concepts of the culture of control and depicts the current emergence of what he calls 'crime society', which combines risk aversion and surveillance tools, with the preventative and architectural approaches to crime prevention and investigation.[50] Technology supports and facilitates the crucial elements at the basis of a crime society, pushing a further shift towards prevention in the fight against crime.

Finally, the prediction of criminal behaviours is supposed to enable law enforcement authorities to reorganise and manage their presence more efficiently and effectively. However, there is very little evidence as to whether police have, in fact, increased efficiency and improved fairness in daily tasks, and it seems to be very much related to the type of predictive policing under evaluation.

[45] S Leman-Langlois, *Technocrime: Technology, Crime, and Social Control* (Willan Publishing 2008).
[46] U Beck, *Risk Society: Towards a New Modernity* (Sage 1992), 21.
[47] O Gandy, *Race and Cumulative Disadvantage: Engaging the Actuarial Assumption*, The B. Aubrey Fisher Memorial Lecture, University of Utah, 18 October 2007.
[48] MM Feeley and J Simon, 'The New Penology' (1992) 30(4) *Criminology* 449.
[49] D Garland, *The Culture of Control* (Oxford University Press 2001).
[50] Koops (n 12).

7.3.2 *Would Crime-Related Patterns Question Reasonable Suspicion and the Presumption of Innocence?*

The emergence of the 'data-driven society'[51] allows for the mining of both content and metadata, allegedly inferring crime-related patterns and thus enable pre-emption, prevention, or investigation of offences. In the view of law enforcement authorities and policymakers, by running algorithms on a massive amount of data, it is allegedly possible to predict the occurrence of criminal behaviours.[52] In fact, data-driven analysis is different from the traditional statistical method because its aim is not merely testing hypotheses but also to find relevant and unexpected correlations and patterns, which may be relevant for public order and security purposes.[53]

For instance, a computer algorithm can be applied to data from past crimes, including crime types and locations, to forecast in which city areas criminal activities are most likely to develop.

The underlying assumption of predictive policing is that certain aspects of the physical and social environment would encourage acts of wrongdoing. Patters emerging from the data could allow individuals to be identified predictively as suspects because past actions create suspicions about future criminal involvement. Moreover, there seems to be the belief that automated measured could provide better insight than traditional police practices, because of a general faith in predictive accuracy.

Yet a number of limits are inherent in predictive policing. It could be hard to obtain usable and accurate data to integrate into predictive systems of policing.[54] As a consequence, notwithstanding big data perceived objectivity, there is a risk of increased bias in the sampling process. Law enforcement authorities' focus on a certain ethnic group or neighbourhood could instead take to the systematic overrepresentation of those groups and neighbourhoods in data sets, so that the use of a biased sample to train an artificial intelligence system could be misleading. The predictive model could reproduce the same bias which poisoned the original data set.[55] Artificial intelligence predictions could even amplify biases, thus fostering profiling and discrimination patterns. The same could happen with reference to the linkage between law enforcement databases and private companies' data, which could increase errors exponentially, as the gathering of data for commercial purposes is surrounded by less procedural safeguards, thus leading to a diminished

[51] A Pentland, 'The Data-Driven Society', ScientificAmerican.com, October 2013, 79, https://connection.mit.edu/sites/default/files/publication-pdfs/data%20driven%20society%20sci%20amer_0.pdf, accessed 27 July 2020.

[52] H-B Kang, 'Prediction of Crime Occurrence from Multi-modal Data Using Deep Learning' (2017) 12 (4) *PLoS ONE*.

[53] M Hildebrandt, 'Criminal Law and Technology in a Data-Driven Society' in *Oxford Handbook of Criminal Law* (Oxford University Press 2018).

[54] AG Ferguson, *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement* (NYU Press 2017).

[55] K Lum and W Isaac, 'To Predict and Serve?' (2016) 13(5) *Significance* 14.

quality of such data.[56] Existing data could be of limited value for predictive policing, possibly resulting in a sort of technology-led version of racial profiling.

Could big data analyses strengthen social stratifications, reproducing and reinforcing the bias that is already present in data sets? Data are often extracted through observations, computations, experiments, and record-keeping. Thus the criteria used for gathering purposes could distort the results of data analyses because of their inherent partiality and selectivity. The bias may over time translate into discrimination and unfair treatment of particular ethnic or societal groups. The link between different data sets and the combined result of big data analyses may then well feed on each other.

Datafication and the interconnection of computing systems which grounds hyperconnectivity is transforming the concept of law, further interlinking it with other disciplines.[57] Moreover, the regulatory framework surrounding the use of big data analytics is underdeveloped if compared with criminal law. Under extreme circumstances, big data analysis could unfortunately lead to judging individuals on the basis of correlations and inferences of what they might do, rather than what they actually have done.[58] The gathering, analysis, and deployment of big data are transforming not only law enforcement activities but also core principles of criminal law, such as reasonable suspicion and the presumption of innocence.

A reasonable suspicion of guilt is a precondition for processing information, which would eventually be used as evidence in court. Reasonable suspicion is, however, not relevant in big data analytics. Instead, in a 'data-driven surveillance society', criminal intent is somehow pre-empted, and this could, at least to a certain extent, erode the preconditions of criminal law in a constitutional democracy – especially when there is little transparency with reference to profiles inferred and matched with subjects' data.[59]

Such major change goes even beyond the notorious 'shift towards prevention' in the fight against crime witnessed during the last decades.[60] First, the boundaries of what is a dangerous behaviour are highly contentious, and problems arise with the assessment of future harm.[61] Second, 'suspicion' has replaced an objective 'reasonable belief' in most cases in order to justify police intervention at an early stage

[56] AG Ferguson, 'Big Data and Predictive Reasonable Suspicion' (2015) 163(2) *University of Pennsylvania Law Review* 327.

[57] M Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Elgar 2015).

[58] Yet individuals also make discriminatory choices, and there is no evidence that artificial intelligence systems would necessarily do worse.

[59] P Nemitz, 'Constitutional Democracy and Technology in the Age of AI' (2018) 376 *Philosophical Transactions of the Royal Society*.

[60] See F Galli, *The Law on Terrorism. The United Kingdom, France and Italy Compared* (Bruylant 2015).

[61] See K Sugman Stubbs and F Galli, 'Inchoate Offences. The Sanctioning of an Act Prior to and Irrespective of the Commission of Any Harm' in F Galli and A Weyembergh (eds), *EU Counter-terrorism Offences* (Ed de l'Université Libre de Bruxelles 2011), 291. Child and Hunt concisely point out the lack of justification for the existence of the special part inchoate offences. See J Child and

without the need to envisage evidence-gathering with a view to prosecution.[62] Traditionally, 'reasonable grounds for suspicion' depend on the circumstances in each case. There must be an objective basis for that suspicion based on facts, evidence, and/or intelligence which are relevant to the likelihood of finding an article of a certain kind. Reasonable suspicion should never be supported on the basis of personal factors. It must rely on intelligence or information about an individual or his/her particular behaviour. Facts on which suspicion is based must be specific, articulated, and objective. Suspicion must be related to a criminal activity and not simply to a supposed criminal or group of criminals.[63] The mere description of a suspect, his/her physical appearance, or the fact that the person is known to have a previous conviction cannot alone, or in combination with each other, become factors for searching such individual. In its traditional conception, reasonable suspicion cannot be based on generalisations or stereotypical images of certain groups or categories of people as more likely to be involved in criminal activity. This has, at least partially, changed.

By virtue of the presumption of innocence, the burden of proof in criminal proceedings rests on the prosecutor and demands serious evidence, beyond reasonable doubt, that a criminal activity has been committed. Such presumption presupposes that a person is innocent until proven guilty. By contrast, data-driven pushes law enforcement in the opposite direction. The presumption of innocence comes along with the notion of equality of arms in criminal proceedings, as well as the safeguard of privacy against unwarranted investigative techniques, and with the right to non-discrimination as a way to protect individuals against prejudice and unfair bias.

Are algorithms in their current state amount to 'risk forecasting' rather than actual crime prediction?[64] The identification of the future location of criminal activities could be possible by studying where and why past times patterns have developed over time. However, forecasting the precise identity of future criminals is not evident.

If suspicion based on correlation, instead of evidence, could successfully lead to the identification of areas where crime is likely to be committed (on the basis of property and place-based predictive policing), it might be insufficient to point at the individual who is likely to commit such crime (on the basis of person-focused technology).[65]

A Hunt, 'Risk, Pre-emption, and the Limits of the Criminal Law' in K Doolin et al. (eds), *Whose Criminal Justice? State or Community?* (Waterside Press 2011), 51.

62 Proactive/anticipative criminal investigations have a primary preventive function, combined with evidence gathering for the purpose of an eventual prosecution. See MFH Hirsch Ballin (n 25).

63 Ferguson (n 56).

64 Walter P. Perry and others, *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations* (Rand 2013).

65 Ferguson (n 56).

https://doi.org/10.1017/9781108914857.008 Published online by Cambridge University Press

7.3.3 *Preventive Justice*

Predictive policing could be seen as a feature of preventive justice. Policy-making and crime-fighting strategies are increasingly concerned with the prediction and prevention of future risks (in order, at least, to minimise their consequences) rather than the prosecution of past offences.[66] Zedner describes a shift towards a society 'in which the possibility of forestalling risks competes with and even takes precedence over responding to wrongs done',[67] and where 'the post-crime orientation of criminal justice is increasingly overshadowed by the pre-crime logic of security'.[68] Pre-crime is characterised by 'calculation, risk and uncertainty, surveillance, precaution, prudentialism, moral hazard, prevention and, arching over all of these, there is the pursuit of security'.[69] An analogy has been drawn with the precautionary principle developed in environmental law in relation to the duties of public authorities in a context of scientific uncertainty, which cannot be accepted as an excuse for inaction where there is a threat of serious harm.[70]

Although trends certainly existed prior to September 11, the counter-terrorism legislation enacted since then has certainly expanded all previous trends towards anticipating risks. The aim of current counter-terrorism measures is mostly that of a preventive identification, isolation, and control of individuals and groups who are regarded as dangerous and purportedly represent a threat to society.[71] The risk in terms of mass casualties resulting from a terrorist attack is thought to be so high that the traditional due process safeguards are deemed unreasonable or unaffordable and prevention becomes a political imperative.[72]

Current developments, combined with preventive justice, lead to the so-called predictive reasonable suspicion. In a model of preventive justice, and specifically in the context of speculative security,[73] individuals are targets of public authorities' measures; information is gathered irrespective of whether and how it could be used

66 L Zedner, 'Fixing the Future?' in S Bronnit et al. (eds), *Regulating Deviance* (Hart Publishing 2008).
67 L Zedner, 'Pre-crime and Post-criminology?' (2007) 11 *Theoretical Criminology* 261.
68 Ibid., 262.
69 Ibid.
70 See E Fisher, 'Precaution, Precaution Everywhere' (2002) 9 *Maastricht Journal of European and Comparative Law* 7. The analogy is made by L Zedner, 'Preventive Justice or Pre-punishment?' (2007) 60 *CLP* 174, 201.
71 L Amoore and M de Goede (eds), *Risk and the War on Terror* (Routledge 2008); L Amoore, 'Risk before Justice: When the Law Contests Its Own Suspension' (2008) 21(4) *Leiden Journal of International Law* 847; C Aradau and R van Munster, 'Governing Terrorism through Risk: Taking Precautions, (Un)knowing the Future' (2007) 13(1) *European Journal of International Relations* 89; U Beck, 'The Terrorist Threat: World Risk Society Revisited' (2002) 19(4) *Theory, Culture and Society* 39.
72 A Ashworth and L Zedner, 'Prevention and Criminalization: Justifications and Limits' (2012) 15 *New Crim LR* 542. By contrast, with reference to automated decision-making, see also DK Citron and F Pasquale, 'The Scored Society: Due Process for Automated Prediction Easy' (2014) 89 *Washington Law Review* 1.
73 See M De Goede, *Speculative Security* (University of Minnesota Press 2012).

to charge the suspect of a criminal offence or use it in criminal proceedings and eventually at trial.

Law enforcement authorities can thus act not only in the absence of harm but even in the absence of suspicion. Thus there is a grey area for the safeguard of rights of individuals who do not yet fall into an existing criminal law category but are already subject to a measure which could lead to criminal law-alike consequences. At the same time, individual rights (e.g., within the realm of private or administrative law) are not fully actionable/enforceable unless a breach has been committed. However, in order for information to become evidence in court, gathering, sharing, and processing should respect criminal procedure standards. This is often at odds with the use of technologies in predictive policing.

7.4 CONCLUDING REMARKS

Law enforcement authorities and intelligence services have already embraced the assumed benefits of big data analyses. It is yet difficult to assess how and to what extent big data are applied to the field of security, irrespective of exploring whether or not their use fosters efficiency or effectiveness. This is also because of secrecy often surrounding law enforcement operations, the experimental nature of new means, and authorities' understandable reluctance to disclose their functioning to public opinion. 'Algorithms are increasingly used in criminal proceedings for evidentiary purposes and for supporting decision-making. In a worrying trend, these tools are still concealed in secrecy and opacity preventing the possibility to understand how their specific output has been generated',[74] argues Palmiotto, addressing the Exodus case,[75] while questioning whether opacity represents a threat to fair trial rights.

However, there is still a great need for an in-depth debate about the appropriateness of using algorithms in machine-learning techniques in law enforcement, and more broadly in criminal justice. In particular, there is a need to assess how the substance of legal protection may be weakened by the use of tools such as algorithms and artificial intelligence.[76]

Moreover, given that big data, automation, and artificial intelligence remain largely under-regulated, the extent to which data-driven surveillance societies could erode core criminal law principles such as reasonable suspicion and the presumption of innocence ultimately depends on the design of the surveillance

[74] F Palmiotto, 'Algorithmic Opacity as a Challenge to the Rights of the Defense', Robotic & AI Law Society, blog post, 6 September 2019 https://ai-laws.org/en/2019/09/algorithmic-opacity-challenge-to-rights-of-the-defense/.

[75] C Anesi et al., 'Exodus, gli affari dietro il malware di stato che spiava gli italiani', Wired, 18 November 2019, www.wired.it/attualita/tech/2019/11/18/exodus-malware-affari-italia/, accessed 27 July 2020.

[76] A Sachoulidou, 'The Transformation of Criminal Law in the Big Data Era: Rethinking Suspects' and Defendants' Rights using the Example of the Right to Be Presumed Innocent', EUI Working Paper, MWP, RSN 2019/35.

infrastructures. There is thus a need to develop a regulatory framework adding new layers of protection to fundamental rights and safeguards against their erroneous use.

There are some improvements which could be made to increase the procedural fairness of these tools. First, more transparent algorithms could increase their trustworthiness. Second, if designed to remove pre-existing biases in the original data sets, algorithms could also improve their neutrality. Third, when algorithms are in use profiling and (semi-)automated decision-making should be regulated more tightly.[77]

Most importantly, the ultimate decision should always be human. The careful implementations by humans involved in the process could certainly mitigate the vulnerabilities of automated systems. It must remain for a human decision maker or law enforcement authority to decide how to act on any computationally suggested result.

For instance, correlation must not be erroneously interpreted as a causality link, so that 'suspicion' is not confused with 'evidence'. Predictions made by big data analysis must never be sufficient for the purpose of initiating a criminal investigation.

Trust in algorithms both in fully and partially automated decision processes is grounded on their supposed infallibility. There is a tendency (as has been the case in the use of experts in criminal cases[78]) among law enforcement authorities to blindly follow them. Rubberstamping algorithms' advice could also become a trick to minimise the responsibility of decision maker.

Algorithm-based decisions require time, context, and skills to be adequate in each individual case. Yet, given the complexity of algorithms, judges and law enforcement authorities can at times hardly understand the underlying calculus, and it is thus difficult to question their accuracy, effectiveness, or fairness. This is linked with the transparency paradox surrounding the use of big data:[79] citizens become increasingly transparent to government, while the profiles, algorithms, and methods used by government organisations are hardly transparent or comprehensible to citizens.[80] This results in a shift in the balance of power between state and citizen, in favour of the state.[81]

[77] D Spiegelhalter, 'Should We Trust Algorithms?', *Harvard Data Science Review*, https://hdsr.mitpress.mit.edu/pub/56lnenzj/release/1, accessed 27 July 2020.

[78] PW Grimm, 'Challenges Facing Judges Regarding Expert Evidence in Criminal Cases' (2018) 86(4) *Fordham Law Review* 1601.

[79] N Richards and H King, 'Three Paradoxes of Big Data' (2013) 66 *Stanford Law Review Online* 41, http://ssrn.com/abstract=2325537.

[80] According to Palmiotto, there is a risk to transform the criminal justice system in a 'system of machinery' where individuals only what machines are yet uncapable of pursuing. See F Palmiotto, 'The Blackbox on Trial. The Impact of Algorithmic Opacity on Fair Trial Right in Criminal Proceedings' in M Ebers and M Cantero-Gamito (eds), *Algorithmic Governance and Governance of Algorithms* (Springer 2020).

[81] See F Pasquale, *The Black Box Society* (Harvard University Press 2015); S Zuboff, *The Age of Surveillance Capitalism* (Public Affairs 2019).