Algorithmic impropriety in UK policing?

Jamie Grace
Sheffield Hallam University

Abstract

There are concerns that UK policing could soon be awash with 'algorithmic impropriety'. Big(ger) data and machine learning-based algorithms combine to produce opportunities for better intelligence-led management of offenders, but also creates regulatory risks and some threats to civil liberties - even though these can be mitigated. In constitutional and administrative law terms, the use of predictive intelligence analysis software to serve up 'algorithmic justice' presents varying human rights and data protection problems based on the manner in which the output of the tool concerned is deployed. But regardless of exact context, in all uses of algorithmic justice in policing there are linked fears; of risks around potential fettering of discretion, arguable biases, possible breaches of natural justice, and troubling failures to take relevant information into account. The potential for 'data discrimination' in the growth of algorithmic justice is a real and pressing problem. This paper seeks to set out a number of arguments, using grounds of judicial review as a structuring tool, that could be deployed against algorithmically-based decision making processes that one might conceivably object to when encountered in the UK criminal justice system. Such arguments could be used to enhance and augment data protection and/or human rights grounds of review, in this emerging algorithmic era, for example, if a campaign group or an individual claimant were to seek to obtain a remedy from the courts in relation to a certain algorithmically-based decision-making process or outcome.

1. Introduction

As well as great opportunities, there are considerable *negative* dimensions and risks of using algorithmic intelligence analysis in the context of what has been categorised as 'high stakes public sector decision-making'[1]. This is a piece that seeks simply to set out a number of administrative law arguments, using grounds of judicial review as a structuring tool, that could be deployed against algorithmically-based decision making processes that one might conceivably object to when encountered in the UK criminal justice system. This means that this article is not, per se, calling for the recognition of a new ground of judicial review that could be termed 'algorithmic impropriety' as such. Instead, algorithmic impropriety, as other scholars have begun to explain[2], is something that could be seen as the combination of administrative law grounds of review as part of a bundle of accountability standards that draw on wider bodies of law. In this way, administrative law arguments could readily be used to enhance and augment data protection and/or human rights grounds of review in this emerging algorithmic era. For example, a campaigning organisation or an individual claimant could

[1] 'High stakes public sector decision-making' is part of the title of a learned paper, and frankly is also a great catch-all concept: See Michael Veale, Max Van Kleek, Reuben Binns, 'Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision Making', CHI 2018 Paper 440, April 2018.

[2] Cobbe, Jennifer, 'Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making ', (August 6, 2018). A pre-review version of a paper in *Legal Studies*, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3226913 or http://dx.doi.org/10.2139/ssrn.3226913 (accessed 17.02.2019)

seek to obtain a remedy from the UK courts in relation to a certain algorithmically-based decision-making process or outcome in the criminal justice context.

This piece is also one that is meant to be timely, if possible; because there is an increasing need to explore the manner in which 'high stakes public sector decision-making' is increasingly algorithmically informed: by machine learning technology that is by very definition relatively unaccountable to human intuition and evaluation. This piece seeks to explore the manner in which common law principles requiring avoidance of 'procedural impropriety' are challenged by the 'data inequalities', 'accuracy biases' and 'decisional opacity' of 'learners'[3] that are to be deployed by, for example, criminal justice agencies, social care organisations and health bodies[4]. In this piece there is an emphasis on examples of algorithmically-based, 'high stakes public sector decision-making' in the criminal justice arena, not least because this is where scholarship to date on 'high stakes public sector decision-making' has proliferated, but because, from a doctrinal point of view, whilst due process rights might not always sit well with algorithmic decision-making, the corollary of breaches of due process in the criminal justice system may be unwarranted harm to private and family life, or the unfair intensification of impacts upon personal liberty.

The use of algorithmically-informed decision-making in public protection contexts in the UK justice system does appear to be proliferating[5]; and this is problematic. As this piece explores below, in the context of such 'high-stakes public sector decision making', there is the emerging issue that when it comes to the structures of such processes, 'many choices are baked-in'[6] as part of algorithmic tools in their procurement or roll-out.

The UN Special Rapporteur on Privacy has commented that in the context of surveillance, algorithmic processing of personal information is less intrusive than human processing of the same personal information[7]. But this position overlooks the transparency problems of algorithms and their opacity in their workings, and the potential injustices with regard to 'trade-offs' in algorithmic weightings driven by particular policy choices, or the risks of potential exacerbation of discrimination through the use of skewed data - all explored below. To balance a view of these risks, there is undoubtedly an acknowledged potential for

[3] Domingos prefers the term 'learner' as a short-hand for a longer phrase such as 'machine learning algorithmic tool or software'. See throughout, Pedros Domingos, *The Master Algorithm: How the Quest for Ultimate Machine Learning Will Remake Our World*, 2017 Penguin Books.

[4] See announcements at: https://www.gov.uk/government/publications/industrial-strategy-the-grand-challenges/industrial-strategy-the-grand-challenges

[5] Oswald and Grace found, through submitting a wave of FOI requests, half a dozen police forces in England and Wales using algorithmic analysis tools in 2016; while the campaign group Liberty also used FOI requests to find 14 police forces using them in 2018. See Oswald, Marion and grace, Jamie (2016), 'Intelligence, policing and the use of algorithmic analysis: a freedom of information-based study', *Journal of Information Rights, Policy and Practice*, 1 (1), p.8; and see Liberty, *Policing by Machine: Predictive Policing and the Threat to Our Rights*, 2019, from https://www.libertyhumanrights.org.uk/policy/report-policing-machine (accessed at 17.02.2019)

[6] Michael Veale, Max Van Kleek, Reuben Binns, 'Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision Making', CHI 2018 Paper 440, April 2018, p.2.

[7] See https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E (accessed at 26.07.2018)

algorithms deployed in the health and care context[8]. The New Economics Foundation have observed that in our increasingly 'scored society', algorithms could be equally likely to be 'emancipatory' or discriminatory[9]; with a crucial factor in the trajectory between one or the other determined by the extent to which our societies take steps to control or limit citizen profiling - and in the private sector as much as the public[10].

Of course there are growing efforts in terms of the modelling of good-practice for regulating algorithms, machine learning and the applications of 'big data' technologies. A community of academics and data scientists called 'Fairness, Accountability and Transparency in Machine Learning' (FAT/ML) have published five 'Principles for Accountable Algorithms' as well as a 'Social Impact Statement for Algorithms', for example[11]. And the Data Protection Act 2018 in the UK requires the Home Office to publish annual 'privacy impact assessments' in the roll-out of any technology such as its new-generation, joined-up 'Law Enforcement Data Service' (LEDS)[12]. However, it was perhaps an astute observation by the Council of Europe that doctrinal law might be better regulation overall, in relation to the risks of machine learning algorithms in the ways that they affect human rights values, compared to any combination of non-binding ethical frameworks and self-regulation[13]. The Council of Europe have also made the observation that 'meta-norms' in the deployment of machine learning may need more time to evolve in practice[14].

Jennifer Cobbe has recently highlighted that "[m]achine learning systems are known to have various issues relating to bias, unfairness, and discrimination in outputs and decisions, as well as to transparency, explainability, and accountability in terms of oversight, and to data protection, privacy, and other human rights issues", but also that "the processes and metrics for fair, accountable, and transparent machine learning developed through… research do not always translate easily to legal frameworks"[15]. It is important to focus, though, on the need

[8] See https://www.theguardian.com/technology/2018/jul/04/its-going-create-revolution-how-ai-transforming-nhs (accessed at 26.07.2018)

[9] See https://neweconomics.org/2018/06/controlled-by-calculations (accessed at 26.07.2018)

[10] See https://neweconomics.org/2018/07/whats-your-score (accessed at 26.07.2018)

[11] The five principles articulated by the FAT/ML group are: Responsibility; Explainability; Accuracy; Auditability; and Fairness - while each principle is contextualised with a few sub-points. See http://www.fatml.org/resources/principles-for-accountable-algorithms (accessed at 26.07.2018)

[12] See https://www.gov.uk/government/publications/law-enforcement-data-service-privacy-impact-assessment (accessed at 26.07.2018). This refers to the 'data protection impact assessments', required by Section 64(1) of the 2018 Act, if 'a type of processing is likely to result in a high risk to the rights and freedoms of individuals'. Should this be the case, an impact assessment must include, under Section 64(3), "(a) a general description of the envisaged processing operations; (b) an assessment of the risks to the rights and freedoms of data subjects; (c)the measures envisaged to address those risks; (d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned."

[13] See https://rm.coe.int/algorithms-and-human-rights-study-on-the-human-rights-dimension-of-aut/1680796d10 (accessed at 26.07.2018)

[14] See https://rm.coe.int/algorithms-and-human-rights-study-on-the-human-rights-dimension-of-aut/1680796d10 p.42 (accessed at 26.07.2018)

[15] Cobbe, Jennifer, Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making (August 6, 2018). A pre-review version of a paper in *Legal Studies*, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3226913 , pp.4-5.

for accountability standards to be articulated as duties and required standards on the organisations (here, police forces) that would implement algorithmic/machine-learning analytics in their work.

This piece attempts to address the same challenge, however, as recently addressed by Marion Oswald: How to use bodies of case law from the discipline of administrative law, rather than more porous ethical frameworks, to suggest how algorithms in 'high stakes' contexts such as policing might be better (re)regulated over time? As Oswald suggests:

> "The system of administrative law is not a barrier or 'antagonistic' to efficient government [instead] it is a 'creative' not destructive relationship, focused on improving the 'technique' of government, and thus the confidence of the citizen in its reasonableness and fairness… Developments in algorithmic intelligibility and explainability can improve 'techniques' of government, and administrative law principles can inform the requirements for such intelligibility, an approach with fairness as its goal."[16]

To signpost the structure of the approaches in the discussion that follows here: this paper moves from a consideration of UK algorithmic practices in criminal justice contexts, to a more theoretical, comparative approach to considering what may constitute algorithmic impropriety, and then on to a common law-centric examination of what the doctrinal roots of algorithmic impropriety must be said to be; before drawing contrast with the regulatory implications of the new Data Protection Act 208 as it applies to the use of algorithmic machine learning technologies in law enforcement terms.

Following this current introductory section, therefore, the second section of this paper examines the emerging picture of the practices of algorithmic intelligence analysis in the UK criminal justice context, with its features of the 'politics of public protection'; while the third section of this paper then seeks to give an outline of three different emerging categories of algorithmic improprieties. The fourth section of this piece takes the comparative approach of examining items of case law from three different jurisdictions that have seen their senior or appellate courts deal with claims of inappropriate deployment of algorithmic offender risk-prediction tools - albeit all three of these other jurisdictions are part of the accepted common law 'legal family'[17]. The fifth section of this paper then gives an overview of the current state of play in terms of common law standards of procedural impropriety, and which must structure, therefore, an idea of a developing doctrine of algorithmic impropriety. The sixth, seventh and eighth sections then, in turn, flesh out the three concepts of 'decisional opacity', 'data inequalities', and 'accuracy biases', respectively, which together form the triple-headed approach which this paper attempts to establish as 'algorithmic impropriety', using the current body of grounds of review from UK administrative law. The ninth section, in a discussion of the new Data Protection Act 2018, addresses some of the non-specific or incidental regulation of operation of algorithmic or machine learning tools in the criminal justice context that stems from Part 3 of that reforming statute. The tenth section of this paper offers a summary

[16] From Marion Oswald (2018) 'Algorithmic-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power', in a special issue on 'The growing ubiquity of algorithms in society: implications, impacts and innovations' of *Philosophical Transactions of the Royal Society A* **376** , p.6.

[17] See Anita Frohlich, 'Clustering Legal Systems' (2014), at https://comparelex.org/2014/04/06/legal-families-in-comparative-law/

of the arguments for a supplementary ground of review to be known as 'algorithmic impropriety', and looks ahead a little to the future regulation of algorithmically-informed 'high-stakes public-sector decision-making'.

2. Emerging practices in regulating algorithmic tools in the criminal justice context

The technological context of predictive algorithms in policing in the UK

When is a piece of predictive software a 'big data' analysis tool; or a 'machine learner'; or artificial intelligence deployed to conduct 'profiling' of individuals? Terms in the field overlap, and nomenclature is used on a shifting basis. This paper is likely guilty of this charge. As Privacy International and Article 19 have recently observed, "[p]olicy debates around AI and privacy are complicated by the fact that regulatory and policy discourses use the term to refer to a broad range of applications, usages and methods."[18] So it may be useful to set out some key ideas before this paper moves properly into its substantive section on administrative law and its application to algorithmic practices.

In the criminal justice context that this paper largely sits within, 'algorithmic intelligence analysis' is both the product and the use of machine learning-type predictive software tools. These tools can, for example, make measurements of the likelihood of (re)offending by individuals, by comparing their data against the patterns in large datasets, to produce profiles of their behaviour ('high risk', or 'low risk' perhaps) that are compiled by the tools themselves, using vast combinations of particular data points i.e. 'big data'. These machine learning tools (or 'learners'[19]) are used not just by the police, or other overtly criminal justice agencies, but increasingly across a resources-strapped UK public sector more generally. Often it is hoped that smarter, algorithmically-informed decision making can save costs to enhance the wider efficacy of a public body or organisation. Databases are increasingly pooled between organisations, as so far as technical solutions and regulation allows; and as multi-agency information sharing about public protection risks has become increasingly the norm. Databases of intelligence are augmented in their efficacy by the use of 'open source intelligence' and surveillance approaches to inform decision-making in some contexts. The products of police intelligence analysis can be used to inform ‘predictive policing’ and the patrolling of particular geographic areas by police officers; or the risk assessment in relation to the (re)offending of an individual convicted or suspected of a proclivity to commit certain categories of offences; and the targeted safeguarding of victims or locations from crime. Machine learning-based or algorithmic tools are not entirely overlapping with the scope of true artificial intelligence [20] - as they are more an application of 'big data' technologies.

Most of the algorithmic technologies used in the policing context of course deal with offenders (though some, for example the Gangs Matrix operated by the Metropolitan Police,

[18] Privacy International and Article 19, *Privacy and Freedom of Expression in the Age of Artificial Intelligence*, (2018) from https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf p.22.

[19] See throughout, Pedros Domingos, *The Master Algorithm: How the Quest for Ultimate Machine Learning Will Remake Our World*, 2017 Penguin Books.

[20] Google have been anticipating the regulation of true artificial intelligence by publishing their own 'AI ethics code': see https://www.blog.google/topics/ai/ai-principles/ (accessed 24.07.2018)

use data about victims in an offender risk analysis). Many of the better-known algorithmic policing technologies predict the risk of violent offending in particular physical spaces; and chief amongst these is PredPol[21]. However, within physical spaces occupied by crowds, the use of machine learning technology to examine the appearance of individuals and their faces in order to detect offenders wanted for offences or with outstanding warrants for their arrest. South Wales Police have been trialling their use of such facial recognition technology, in a laudably transparent way, and have admitted publically to a high rate of 'false positives' (mistaken detections, resulting in a literally unwarranted police stop of an individual) in their use of such technology at the football Champions League cup final, in Cardiff in 2017[22]. Campaign group Big Brother Watch have weighed in on the issue of the privacy risks and the corollary threats to personal liberty of this practice, particularly while this technology is largely inaccurate at the moment, and relatively lightly regulated to boot[2324].

In another relatively high-profile trial of algorithmically predictive policing of offenders, albeit it in the charging decision context, Durham Constabulary have been training their algorithmic 'Harm Assessment Risk Tool' (HART) to inform decision-making by custody officers in the future. HART will eventually be used to advise custody officers as to where offenders deemed of a suitably low-enough risk can be diverted away from normal criminal process (and possible prison sentences) via out-of-court disposals in a programme called Checkpoint[25]; a combined system that when fully operationalised could keep many offenders well away from the short prison sentences that are damaging for re-offending rates. While HART was criticised for initially using Experian 'Mosaic' data for profiling purposes as a data point amongst more than 30 data points[26], in its developmental and pilot phases as a tool, such criticisms are perhaps overblown. ('Mosaic' data from Experian has been withdrawn from the dataset HART will draw upon.) Yes, Experian would otherwise have been making a profit from relatively unaccountable profiling that feeds into 'high stakes public sector decision making'; but if such decision-making by algorithms can be made more accurate through the use of such private-sector-origin data, or at least need to be 'trained' on such data, then surely the true goal of more accurately-informed 'high stakes' decisions is a worthy compromise?

In terms of algorithmic policing tools being used to manage victim complainants and their reports of crime, the most high-profile example to date is the 'EBIT' system of case handling and investigation triage being used in trial areas by Kent Police, and which has been inspected favourably by HMICFRS, following only a little inquiry into whether victims

[21] See http://www.predpol.com/ (accessed 24.07.2018)

[22] See https://www.south-wales.police.uk/en/advice/facial-recognition-technology/ (accessed 24.07.2018)

[23] See https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals (accessed 24.07.2018)

[24] See Joe Purshouse and Liz Campbell, 'Privacy, Crime Control and Police Use of Automated Facial Recognition Technology', [2019] Crim. L.R. Issue 3, forthcoming.

[25] See https://www.durham.police.uk/Information-and-advice/Pages/Checkpoint.aspx (accessed 24.07.2018)

[26] See https://bigbrotherwatch.org.uk/all-media/police-use-experian-marketing-data-for-ai-custody-decisions/ (accessed 24.07.2018)

would object to an algorithm being involved in 'shelving' their report of a crime[27]. The process and legal position of explaining to, or otherwise notifying victims that an algorithm has recommended their case or complaint be shelved is a delicate and difficult one. At the time of writing, the Kent Police website contained no clear information on the EBIT system, and so it is unclear how individuals could easily find out more about the role of the EBIT system in handling their complaint or report of a criminal offence.

Emerging practices in regulation and self-regulation

Recently, the Information Commissioner's Office have found that the manner of the operation of a 'Gangs Matrix' by the Metropolitan Police in London was a breach of UK data protection law, and possibly the public sector equality duty under the Equality Act 2010[28]. As part of the response to this finding from the ICO, the Mayor's Office for Police and Crime have conducted a review of the use of the Gangs Matrix over a five-year period, June 2013 to May 2018. In the period June 2017 to May 2018, 82.3% of people on the Matrix were BAME, 99% Male, and 55.6% under 18 years of age[29]. (One cannot escape the fact that the Matrix has to an extent become a means of managing and calibrating the criminal punishment of thousands of black teenage boys in London). So the use of an algorithmic tool to profile possible gang members is, on this prima facie view, a contentious practice that interferes with the 'group privacy' of "algorithmically assembled groups"[30]. The Gangs Matrix tool also draws greatly on online, open-source intelligence, or 'OSINT', too. So there are issues here around the 'reasonable expectation of privacy' test as applied in this context. Overall, then, it is possible to conclude as Mittelstadt has done, and in relation to tools such as the Gangs Matrix for example, that "[a[dvances in data analytics necessitate new protections for the privacy interests of ad hoc groups formed by algorithmic classification"[31]. The development in the UK courts of a 'reasonable expectation of privacy' test for the engagement of Article 8 ECHR has been problematic of late, in the police intelligence context, since so much of the information that would be recorded on police systems about individuals who might complain of an interference with their right to private life will be - in some manner - public or open-source information. Data processed by a 'machine learner' could often include a mix of information which, in terms of its processing in a law-enforcement context, would not give rise to a 'reasonable expectation of privacy'. Additionally, this same jurisprudence has highlighted that:

> "… the absence of a statutory power does not mean that the actions [of intelligence analysis] are not in accordance with the law. For these purposes, the exercise of the powers must be governed by clear and accessible rules of law, governing the scope

[27] (HMICFRS, 2018: 8): https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/peel-police-effectiveness-2017-kent.pdf

[28] See Information Commissioner's Office, 2018a, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/information-commissioner-s-investigation-into-the-metropolitan-police-service/ (accessed 17.02.2019) and Information Commissioner's Office, 2018b, Gangs Matrix Enforcement Notice.

[29] Mayor's Office for Policing and Crime (MOPAC), *Review of the Metropolitan Police Service Gangs Matrix*, December 2018, p.25.

[30] Mittelstadt, Brent. "From individual to group privacy in big data analytics." *Philosophy & Technology* 30.4 (2017): 475-494, 475.

[31] Mittelstadt, Brent. "From individual to group privacy in big data analytics." *Philosophy & Technology* 30.4 (2017): 475-494, 491.

> and application of measures, as well as minimum safeguards concerning duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction."[32]

65% of individuals on the Gangs Matrix in September 2018 were ranked with a 'green' profile (as opposed to 'amber' or 'red'), and therefore scored as a low-risk of gang membership and gang-related criminal activity. Importantly, many of those low-risk individuals were regarded as no risk at all. This raised questions for the MOPAC, and highlighted the need for reform of data retention policy used by the Metropolitan Police in relation to the Matrix and in response to the ICO Enforcement Notice:

> "We recommend a thorough reappraisal of the individuals in the Green category, with a focus on: those that currently score 'zero-harm'; those that have never had a harm score or have remained in the Green category for their entire time on the Matrix; and those under the age of 18. This reappraisal should begin as soon as possible and be concluded no later than 31st December 2019. This reappraisal should consider whether: the level of risk they present justifies their continued inclusion; their inclusion is consistent with the published purpose of the Matrix; and whether their inclusion is compatible with Article 8 (2) of the [ECHR]. Where an individual does not meet these criteria, they should be removed from the Matrix."[33]

The MOPAC report concluded overall that:

> "Both the Operating Model and the training should have a particular focus on ensuring… that the right people are on the Matrix; that people are added and removed in a standardised, evidence-based manner; that they can be removed and that the 'gang' label will not 'follow' them; [and]that local Matrices are refreshed regularly so that individuals don't stay on any longer than necessary…"[34]

Some of these police data management and information governance concerns are issues that the HMIC report *Building the Picture* would have foretold[35], but the algorithmic technology underpinning the Gangs Matrix exacerbates these issues, resulting in wholesale and semi-permanent, quite possibly very damaging *belief revision* about individuals profiles in the

---

[32] *R (Butt) v Home Secretary* [2017] EWHC 1930 (Admin) at para. 238.

[33] Mayor's Office for Policing and Crime (MOPAC), *Review of the Metropolitan Police Service Gangs Matrix*, December 2018, p.40. In support of this approach, it could be noted that a similar necessity regarding deletion was recently highlighted by the European Court of Human Rights in *Catt v UK* (43514/15) 24 January 2019. The Court concluded at 119 that "in the absence of any rules setting a definitive maximum time limit on the retention of [police intelligence] data the applicant was entirely reliant on the diligent application of the highly flexible safeguards in the [police policy] to ensure the proportionate retention of his data. *Where the state chooses to put in place such a system, the necessity of the effective procedural safeguards becomes decisive... Those safeguards must enable the deletion of any such data, once its continued retention becomes disproportionate.*" [emphasis added]

[34] Mayor's Office for Policing and Crime (MOPAC), *Review of the Metropolitan Police Service Gangs Matrix*, December 2018, p.55.

[35] HMIC, *Building the Picture: An Inspection of Police Information Management*, 2015, at https://www.justiceinspectorates.gov.uk/hmicfrs/our-work/article/building-the-picture/ (last accessed 24.07.2018)

Matrix tool, as De Bruin would have it[36], concerning potentially very low risk or no-risk individuals; perhaps greatly harming their decisional autonomy. Elements of personal liberty, privacy and equality are a high tariff to set for an operational tool which, it is reported by the officers who must use it, is not fit for purpose. Furthermore, the perception of an algorithmic tool as unjust may actually be counter-productive and damaging As Daragh Murray and Pete Fussey observed about the Gangs Matrix: "Discrimination, arbitrariness and a lack of transparency can only lead to dissatisfaction, distrust and alienation from the state. When they occur, it's not just human rights that are violated – it's the very goals which technology was deployed to serve."[37]

Overall, the Gangs Matrix case study offered here shows that 'high stakes public sector decision-making' that draws on algorithmic intelligence analysis may not be predicated in any case, currently, on specific statutory provisions, but it is regulated to a considerable degree not just by human rights law and administrative law, but by the Equality Act 2010 and the newer provisions of the Data Protection Act 2018. However, there are as yet considerable unknowns as to what should be considered to be the proportionate storage or *use* of algorithmically-generated predictions of risk as a type of police intelligence, as a section of this paper will explore below. There are also related issues of determining the level of intrusion that is arguably required to be reached before authorisation (and accountability therefore) is required under the Regulation of Investigatory Powers Act 2000, for the obtaining of the OSINT data that can form part of the set of data points to be used by an algorithmic assessment tool[38].

3. Algorithmic improprieties?

A problem for (self-)regulation stemming from a lack of case law?

The key issue with human rights law in the UK as something to use to challenge the effects and processes of algorithmically-based decision-making, where the rights principally at risk could be those concerning a fair hearing, or respect for private and family life, or freedom from discrimination etc., is that there is, at the time of writing, no case law to speak of. Human rights law in the UK, at the time of writing, may be based largely on the Articles of the European Convention on Human Rights, but there is no jurisprudence at all from the UK courts or the European Court of Human Rights on 'high-stakes public sector decision making' using 'learners'. In a different area of the discipline of information law, Mark Taylor was at one time confronted by a lack of directly relevant case law on the issue of the regulation of genetic data processing for research purposes; and Taylor noted that "…the lack of case law, and the absence of any precise formula for evaluating proportionality, does leave some doubt about when [an interference with an] individual's right to a private life would be justified…"[39]. However, we do have the benefit of being able to undertake a deliberative-style micro-comparison of the approaches of courts and tribunals in Canada, New Zealand and Wisconsin (USA) to issues of potential 'algorithmic impropriety', however, in

[36] De Bruin, Boudewijn. "The liberal value of privacy." *Law and Philosophy* 29.5 (2010): 505-534, 512.

[37] Daragh Murray and Pete Fussey, 'Police are using big data to profile young people, putting them at risk of discrimination', from https://theconversation.com/police-are-using-big-data-to-profile-young-people-putting-them-at-risk-of-discrimination-96683 (last accessed 18.05.2018)

[38] See *R (Butt) v Home Secretary* [2017] EWHC 1930 (Admin).

[39] Taylor, Mark. *Genetic data and the law: a critical perspective on privacy protection*. Vol. 16. Cambridge University Press, 2012, p.73.

considering how the UK courts would prioritise structures and standards in their approach to dealing with claims for judicial review of algorithmically-informed decision-making.

One section of this paper, below, is intended to explore the idea that while there are practices in algorithmically-informed or algorithmically-based decision-making that data protection law or (some) human rights law might tolerate, there is the issue of common law values aiming to prevent procedural impropriety which might not tolerate the same practices. Part of the argument presented below is that using administrative law grounds of judicial review, we should develop a parallel concept of 'algorithmic impropriety' alongside, and in order to augment, our developing concept of 'algorithmic justice'.

Seen from a positive perspective, there is no doubt that machine learning and algorithmic analysis in public-sector, public protection-oriented decision-making has the potential to radically transform the levels of accuracy and efficacy in the deployment of state resources, by cutting through the fog of innate human biases and those vagaries of the 'gut feeling'. This can be needed because, as Daniel Kahneman and Amos Tversky observed in their classic 1973 paper 'On the Psychology of Prediction':

> "In making predictions and judgments under uncertainty… people do not appear to follow the calculus of chance or the statistical theory of prediction. Instead they rely on a limited number of heuristics which sometimes yield reasonable judgments and sometimes lead to severe and systematic error."[40]

In calling for the development of a standard of (unacceptability in) 'algorithmic impropriety', this paper is only reminder that technology has consistently and unceasingly driven legal reform, conceptually and doctrinally. In many ways, the rise of 'algo-cops'[41] and their machine learning-driven intelligence analysis is just the latest in a long line of technological innovations in policing[42], as an emanation of state power, which the legal and political constitution in the UK must reflexively bring under its own control. Great technological leaps forward can also have transformational constitutional effect, and for the communal good, as Hildebrandt has explained:

> "While the printing press first allowed the rule by law (the sovereign using written codes as a means to rule his subjects), it later enabled the rule of law (the internal division of sovereignty that separates the enactment of legal rules by the legislator from their interpretation in a court of law)."[43]

So the nature of increasingly algorithmically-informed administrative discretion, and the growth in decision-making, based upon the same, in rights-sensitive contexts, could well first present new challenges, and new ways of doing things - but ultimately in time should produce

---

[40] Daniel Kahneman and Amos Tversky in 'On the Psychology of Prediction', quoted in Michael Lewis, *The Undoing Project: A True Story*, Penguin Books, 2017, p.196.

[41] Luisa Hess, 'Die Algo-Cops', from http://heute-morgen-uebermorgen.digital/blog/2017/09/19/sind-algorithmen-die-besseren-polizisten/ (accessed 24.07.2018)

[42] Jane Wakefield, 'Future cops: How technology is set to change policing', from http://www.bbc.co.uk/news/technology-22954783 (accessed 24.07.2018)

[43] Mireille Hildebrandt, 'Profiling and AmI', in Kai Rannenberg, Denis Royer and Andre Deuker (eds.), *The Future of Identity in the Information Society: Challenges and Opportunities*, 2009, Springer, p.300.

new models of oversight and then, eventually, new formulae for *legal* codes applicable to the most powerful predictive *computer* codes.

This section of this paper briefly introduces the notions of three dimensions of 'algorithmic impropriety', namely 'decisional opacity', 'data inequality' and 'accuracy bias'. Basic descriptions of these can be given as follows:

Decisional opacity

This element of algorithmic impropriety concerns the idea that an algorithm or a 'machine learner' is a 'black box' - with the finest levels of detail concerning the way decisions are made by a tool obscured by the statistical complexity of the manner in which the tool makes that decision. In this way, the extent to which the 'reasoning' of a machine-learning-based tool is 'opaque' or unfathomable to nearly all people, and potentially every person that tried to understand in totality the rationale for a prediction, for example, of a risk of re-offending. This raises issues of natural justice, as this paper explores, below; since natural justice is the premise of being able to understand the evidence or the basis of an accusation of wrongdoing.

Data inequality

Data inequality arises from the issue that machine learning algorithms must learn from something - and will make predictive decisions on the basis of past-created or previously generated data in whichever context it operates. This creates, potentially, the risk of data legacy-based injustices, or 'data inequality'; since the collection of data itself can be unfairly skewed or discriminatory, based on practices and trends of collection of the data concerned.

Accuracy bias

Human beings can be consciously or unconsciously bias, but the designers of 'learners' must choose, consciously, how to weight a point of data in a tool that makes decisions algorithmically - and must do so, therefore, consciously. This creates the notion that an algorithmic tool can recommend decisions in a comprehensive, but to some people, biased manner - again causing problems around natural justice, or in this context, 'algorithmic impropriety'.

Linking elements of 'algorithmic impropriety' to classic values of administrative law

This paper makes links between these three key elements of 'algorithmic impropriety' to classic values of administrative law, and proceeds to argue, in sections below, that certain of these classic values can form the basis of a model of 'algorithmic impropriety'. Firstly, though, it is important to note that some critical commentators, such as Jamie Bartlett, take a pessimistic of recent efforts to regulate machine learning, or algorithmically-augmented, decision-making; and call for new methods of accountability. Bartlett has written that:

> "Secretly designed algorithms are already creating data-led bias and invisible injustices and we urgently need a democratic mechanism to hold them to account. Our lawmakers - whether national or international - must create accountability officials who, like [the[IRS or Ofsted inspectors, have the right to send in technicians with the requisite skills to examine Big Tech algorithms, either as random spot-checks or in relation to a specific

> complaint. While it may no longer be easy to 'look under the bonnet' of modern algorithms, careful examination and oversight are still possible."[44]

Of course this paper takes the concerns of commentators such as Bartlett on board. These concerns may well represent real regulatory risks, and there may be a need for new accountability mechanism for algorithms of different kinds, but this paper now goes looking for legal solutions that may already exist, and in fact do exist, as this paper will argue, below. It is the case that existing legal protections can be augmented with an understanding of 'algorithmic impropriety' as based on 'decisional opacity', 'data inequality' and 'accuracy bias', as introduced above. In much the same way, as Privacy International and Article 19 have recently argued:

> "…there is a tendency to assume that the technology poses challenges that are so radically new that all existing laws, regulations and standards are no longer applicable or appropriate. The 'flipside' of that discourse is to demand regulation of the technology itself, regardless of how and where it is applied. To avoid succumbing to any of these fallacies, there is a need to examine how existing discourses, such as human rights law, data protection, sectoral privacy regulation, and research ethics, relate to different applications and methods of AI."[45]

In listing these 'existing discourses', however, Privacy International and Article 19 have placed little emphasis on common law values of *procedural impropriety* - not listing their inclusion in the relevant discourses quoted above. This piece hopes to help to address that gap in the discourse.

4. Comparative common law approaches to dealing with arguable algorithmic improprieties

One reason why a concept of algorithmic impropriety should be developed from common law values of procedural impropriety is simply that, currently, as lawyers or legal scholars we are faced with a lack of truly relevant case law in the UK on the use, directly, of algorithmically-informed 'high stakes public sector decision-making'. But there are a number of decisions in other common law jurisdictions globally which judges in the UK, for example could draw upon if faced with a novel piece of litigation in this regard. It helps, conceptually, then, that there is an available theory of a common law 'legal family' around the globe[46] - since this allows us to take a useful *deliberative* comparative approach (as outlined by Sandra Fredman[47]), while exploring possible algorithmic impropriety in the UK legal context by using these legal findings from other common law jurisdictions. The three cases of *Loomis*,

---

[44] Jamie Bartlett, *The People vs Tech: How the Internet is Killing Democracy (and how we save it)*, 2018, 211.

[45] Privacy International and Article 19, *Privacy and Freedom of Expression in the Age of Artificial Intelligence*, (2018) from https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf p.22.

[46] See Anita Frohlich, 'Clustering Legal Systems' (2014), at https://comparelex.org/2014/04/06/legal-families-in-comparative-law/ (accessed at 17.02.2019)

[47] See Fredman, Sandra. "Foreign Fads or Fashions? The Role of Comparativism in Human Rights Law." *International & Comparative Law Quarterly* 64.3 (2015): 631-660.

Ewert and *Hemopo*, each explored a little in this piece, below, are a useful starting point in this deliberative comparative approach to exploring a concept of algorithmic impropriety.

A deliberative comparison on the issue of algorithmic improprieties between common law jurisdictions might have real value. There are acknowledged strengths in terms of procedural protections in the common law: Sedley LJ observed in *Wooder* that the common law allows for more effective standards of natural justice, that apply to administrative (governmental) as well as judicial (and tribunal) contexts, than the ECHR, for - and reminded us that Section 11 of the Human Rights Act 1998 protects the extension of rights under the common law where they can go further and offer more for claimants in judicial review than the Convention might do, that is, than under Article 6 ECHR and the right to a fair hearing[48].

Importantly, as Timothy Endicott has explained, the Strasbourg court finds due process rights a requirement amongst only judicially made decisions, while the common law instead has extended procedural protections to the context of decisions made by administrative or governmental bodies. However, the UK courts have noted that administrative decision-making can be driven by subject expertise that looks and feels, potentially, like a factor that would otherwise constitute unlawful bias in decision-making[49]. The concept of apparent bias in making an administrative decision is something we must return to consider in an algorithmic context, below.

There are some obvious grounds of review in a typology of administrative law which do not connect, traditionally, with procedural impropriety; such as the notion of illegality, for example, in the form of an unlawfully fettered discretion. Specifically, in relation to this classic ground of fettering discretion, we must ask ourselves, particularly in relation to fully automated, algorithmically based decision-making, whether the use of such a machine learning tool runs the risk of breaching the rule in *British Oxygen*, that 'someone with something new to say' should, in principle, be heard - that is, they should be able to make their argument as to the difference in treatment they require under a particular policy[50]. Even an algorithmically-derived decision which is implemented with human final approval, sign-off or oversight, in some variation of the notion of 'the human in the loop'[51], might fall afoul of a claim based on the principle of an unlawful fettering of discretion, given the tendency, in theory, of human beings to grow over time to merely approve what a machine learner recommends, in a case of what is sometimes known as 'hyper-nudge'[52] or 'automation bias'[53]. The doctrine of proportionality can also be brought to bear on the 'high stakes' use of algorithms in the criminal justice context. In another example of a more substantive element

---

[48] *R (Wooder) v Feggetter* [2002] EWCA Civ 554, at 46.

[49] Timothy Endicott, *Administrative Law*, 3rd ed. Oxford University Press, 2015, p.165.

[50] *British Oxygen Co Ltd v Minister of Technology* [1971] AC 610, 625.

[51] See Citron, Danielle Keats, and Frank Pasquale. "The scored society: due process for automated predictions." *Wash. L. Rev.* 89 (2014): 1.

[52] See Yeung, Karen. "'Hypernudge': Big Data as a mode of regulation by design." *Information, Communication & Society* 20.1 (2017): 118-136.

[53] See Cobbe, Jennifer, 'Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making ', (August 6, 2018). A pre-review version of a paper in *Legal Studies*, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3226913 or http://dx.doi.org/10.2139/ssrn.3226913 (accessed 17.02.2019), p.9.

of 'algorithmic impropriety', and in relation to appellate case law such as *Quila*[54], we could also ask, to what extent is the inclusion of any one point of data in an algorithmic analysis part of a 'fair balance' in the use of an algorithmic tool, applying the final limb of a four-part proportionality test?

The next section of this paper looks in more detail at specifically *procedural* grounds of review from the common law that would be used to challenge algorithmically-based decision-making, and where these grounds of review, as a package, amount to 'algorithmic impropriety'.

5. Procedural impropriety in the common law

'Procedural impropriety' is a package concept, not in usage by all administrative lawyers or judges, but famously outlined by Lord Diplock in one of the classic English administrative law cases, known commonly as *GCHQ*[55]. Lord Diplock preferred the term 'procedural impropriety', noting that:

> "…what procedure will satisfy the public law requirement of procedural propriety depends upon the subject matter of the decision, the executive functions of the decision-maker (if the decision is not that of an administrative tribunal) and the particular circumstances in which the decision came to be made."[56]

As Timothy Endicott has explained in his authoritative *Administrative Law*, "[f]air procedures give the persons affected an appropriate role in the process"[57]. However, Endicott's position is also that "…due process… means proportionate process"[58]. This probably means that the starting point for any assessment in judicial review of the involvement of a machine learning tool in some particular instance of 'high stakes public sector decision-making' is actually likely to be an assessment of the degree to which the algorithm's protection of an outcome was the most key, central or influential factor in a final public protection or clinical decision being reached.

In a crucial relationship with this principle of the extent to which an algorithmic prediction is influential or even determinative (summoning the prospect, perhaps, of automated decision-making) is the principle of the extent to which an algorithmic prediction or decision can be readily challenged. The administrative law package of rights concerned with 'natural justice' give some core guidelines as to what extent the application of an algorithm be challenged,

---

[54] Wilson LJ outlined the four-part proportionality test in *R (Quila) v Secretary of State for the Home Department* [2011] UKSC 45 at 45 as:
"(a) is the legislative objective sufficiently important to justify limiting a fundamental right?;
(b) are the measures which have been designed to meet it rationally connected to it?;
(c) are they no more than are necessary to accomplish it?; and
(d) do they strike a fair balance between the rights of the individual and the interests of the community?"

[55] *Council of Civil Service Unions v Minister for the Civil Service* [1985] AC 374

[56] *Ibid.*

[57] Timothy Endicott, *Administrative Law*, 3rd ed. Oxford University Press, 2015, p.53.

[58] Timothy Endicott, *Administrative Law*, 3rd ed. Oxford University Press, 2015, p.181.

applying the classic case of *Ridge v Baldwin* [1964] AC 40. In *Ridge* at 132, Lord Hodson concluded "three features of natural justice stand out - 1) the right to be heard by an unbiased tribunal; 2) the right to have notices of charges of misconduct, and 3) the right to be heard in answer to those charges". These three features of natural justice give rise to three obvious concerns about the applications of algorithms in any criminal justice context:

1. the problem of the designers of machine-leanring tools for criminal justice applications purposefully choosing algorithmic 'sensitivity' over 'specificity' in the 'thinking' of an tool's predictions, in order to produce the greatest accuracy in one area of those predictions; at the risk of lesser accuracy in another regard[59] (the issue of 'trade-off's as a kind of conscious *process* bias, discussed below): for example, a preference for predicting as many high-risk offenders as possible in a cohort, with inherently less regard for inaccurately mis-predicting a greater number of offenders as 'high risk', and when they would otherwise be more likely to be predicted 'low risk';
2. the problem of effective notification of individuals that an algorithm has informed or determined a decision about them (and although with regard to automated decision-making this is to an extent now a requisite under Part 3 of the Data Protection Act 2018, discussed below, the subtleties of this are highly likely to be problematic given the first issue identified here, and particularly in the context of algorithmically-driven or 'supported', but not *automated*, decision-making);
3. the ability of individuals being able to challenge algorithms and their application to their own progress or capture by the criminal justice system is crucial, as noted above, but is particularly prone to being undermined by failures to meet the first two principles discussed in relation to the composite of natural justice, again, as above.

'Natural justice' grounds would then provide an initially strong framework for the challenge via judicial review, say, of the application of an algorithmic analysis or prediction. Those who would deploy a technological approach that draws on a machine learning algorithm would need to be very conscious of the establish 'test' in the common law for what is commonly termed 'apparent bias' as a ground of review, and the way that it interrelates with the principles of natural justice.

For a starting point, Timothy Endicott reminds us that the "rule against bias governs both judicial and administrative decision-making"[60]. In *Porter v Magill* [2001] UKHL 67 at 103 the House of Lords identified the test for presumed or apparent bias as: "The question… whether the fair-minded and informed observer, having considered the facts, would conclude there was a real possibility that the [decision-maker] was biased." So the initial question this would raise in the minds of a judge, conducting a review of the lawfulness of the use of an algorithm in a criminal justice context, would be: to what extent can the operation of an algorithm create unfair, 'apparent' bias as a matter of law, applying *Porter*?

Some of the substantive grounds of review connected to the concept of illegality could be said to be much more procedural in feel, and so might readily be used to challenge an algorithmic analysis or prediction and the application of the same as part of a decision-making process in criminal justice contexts. The variant of illegality that readily springs to

[59] Thanks to Alex Patterson, University of Sheffield PhD candidate at the time of writing, for his explanation of statistical sensitivity and specificity in the context of this paper.

[60] Timothy Endicott, *Administrative Law*, 3rd ed. Oxford University Press, 2015, p.165.

mind is the taking into account of 'irrelevant considerations', or the contrasting but equally problematic failure to take relevant considerations into account. Such illegality could be seen in the recent decision in *Radford*[61], where the convicted sex offender and 'Black Cab Rapist' John Worboys (now going by John Radford) had been (unlawfully) deemed fit for early release from his custodial sentence only because, in the reasoning of Sir Brian Leveson P, Mr Justice Jay and Mr Justice Garnham (at 163), information as to scores of alleged offences (beyond those for Worboys had been convicted and imprisoned) had improperly gone unconsidered by the Parole Board in their decision-making process:

> "…in strict public law terms the issue for us is whether we could be confident that this additional material could make no difference to the outcome, in other words that the Parole Board would inevitably have taken the view that it is irrelevant. It would be impossible for us so to conclude."

One wonders whether the circumstances of the *Radford* decision shows that, certainly, some decision-making in the criminal justice system might well be more accurate if algorithmically-informed - but also that human decision-making is the only kind able to sensitively weigh up the kind of issues presented in the instant case. This obviously entails information that is available, with investigation, to consider about the risk of offending, here, but this also entails considering information that is ultimately qualified by both its nature (relating to allegations and complaints, albeit of the most serious kind) and the availability of information which is so crucial and probative in its certainty to aid decision-making (meaning the 12 offences, here, for which Radford was convicted and imprisoned). It is worth noting, after all, that Leveson P and Jay and Garnham JJ determined in Radford that the decision to release such a prolific offender only part-way through his sentence was not unlawful in the sense of irrationality or *Wednesbury* unreasonableness (133):

> "A risk assessment in a complex case such as this is multi-factorial, multi-dimensional and at the end of the day quintessentially a matter of judgment for the panel itself. This panel's reasons were detailed and comprehensive. We are not operating in an appellate jurisdiction and the decision is not ours to make. We are compelled to conclude that the decision of the panel must be respected."

Endicott has highlighted that there is a category of decisions where the courts must act with some margin of deference to decision-makers who are taking certain considerations into account, namely when there are "[g]rounds for a good decision that are not specified by law, but which no reasonable decision-maker would ignore or which no reasonable decision-maker would act on…"[62]. But, as a result, "…if the claimant cannot say that the law specifically demands or forbids consideration of a particular fact or ground of decision, but only that good reasoning requires attention to it, then the courts should hesitate to decide what counts as good reasoning"[63].

There is, of course, the common law ground of review referred to as the 'duty to give reasons'. The recent *Daniels* case on the composition of the Grenfell inquiry panel and its terms of reference is a useful and recent case example of how this standard in decision-

---

[61] *R (DSD and others) v Parole Board of England and Wales and others* [2018] EWHC 694 (Admin)
[62] Timothy Endicott, *Administrative Law*, 3rd ed. Oxford University Press, 2015, p.281.

[63] Timothy Endicott, *Administrative Law*, 3rd ed. Oxford University Press, 2015, p.282.

making operates in public law terms[64]. In *Daniels*, a challenge was made on the basis that the Prime Minister had failed to adequately give reasons to explain why the inquiry panel hearing evidence on the Grenfell Tower fire disaster should not consider broader connected themes in the context of the fire and the tragic loss of life is entailed - namely government social housing policy and the governance of local authorities, etc. - and a broader inquiry panel composition accordingly.

The duty to give reasons is a most flexible standard at common law. However, it remains that the need to explain the operation of an algorithmic tool will always arise to some extent, given the nature of the rights and duties at stake in that context, and in order that a criminal justice agency meets those (flexible) standards of the 'duty to give reasons' in common law terms.

6. Decisional opacity

At this juncture however, we are turning to consider the first of the three key themes presented in this paper on the components of what I am terming 'algorithmic impropriety'. This is the theme of 'decisional opacity' - connecting with the theme of risks to natural justice as discussed above. An example of 'decisional opacity' I would give here is the judgment in *Loomis* by the Wisconsin Supreme Court. (In considering the 'algorithmic impropriety' theme of 'data-driven inequalities' below, an example is given of both *Offender Assessment Policies (Tame Hemopo)* (2005) WAI 1024 from New Zealand, and *Ewert v Canada* 2015 FC 1093 and 2016 FCA 203; while in discussing the third and final theme of 'known accuracy biases' and public policy considerations this piece deploys an analysis of case studies available from academic literature on the 'trade-offs' built into several algorithms in criminal justice-related tools to date.)

Cathy O'Neil has observed of the recent crops of algorithms or 'machine learning' tools that:

> "Opaque and invisible model are the rule, and clear ones very much the exception… Even when such models behave themselves, opacity can lead to a feeling of unfairness."[65]

Such lack of transparency has been observed in the case of *Loomis v State of Wisconsin* (2016)[66]. Loomis claimed his sentencing - aided by an algorithmic tool (COMPAS, developed by Equivant[67]) - had involved an unlawful lack of due process. As Oswald et al have commented:

> "the Wisconsin Supreme Court rejected the idea that the algorithmic assessment of an appropriate sentence for Loomis was unconstitutional, even though the inner algorithmic workings and data weightings were not revealed to the defendant due to commercial confidentiality. Loomis had argued that this situation offended the 'Due Process Clause' under the Fifth and Fourteenth Amendments of the US Constitution, which stipulate that there shall be no interference with life, liberty or property without

[64] *R (Daniels) v May* [2018] EWHC 1090 (Admin)
[65] Cathy O'Neil, *Weapons of Maths Destruction: How Big Data Increases Inequality and Threatens Democracy*, p.28

[66] *Loomis v State of Wisconsin* (2016) WI 68

[67] See http://www.equivant.com/solutions/case-management-for-supervision (accessed at 28.07.2018)

> due process of law. But the Wisconsin Supreme Court found that the COMPAS 'forecast' or assessment was not 'determinative' for the sentencing decision, and that sufficient discretion resided in the role of the sentencing judge to maintain this rather opaque assessment process as constitutional."[68]

One would imagine that this crucial factor in the outcome in *Loomis*, namely that the use of algorithm was advisory as opposed to fully determinative or binding in the decision on an appropriate sentence by a judge in the criminal courts, as a matter of *policy*, would be readily adopted in the UK courts in much the same manner. But to take the view that any algorithm was 'advisory only' in a sentencing (or bail, or charging, or any other risk-assessment-type process in the criminal justice system) would strongly suggest the side-lining of arguments in administrative law concerned with 'unlawful delegation of powers'[69]. After all, as Lord Bridge observed, "the so-called rules of natural justice are not engraved on tablets of stone", before going he went on to explain that:

> "To use the phrase which better expresses the underlying concept, what the requirements of fairness demand when any body, domestic, administrative or judicial, has to make a decision which will affect the rights of individuals depends on the character of the decision-making body, the kind of decision it has to make and the statutory or other framework in which it operates. In particular, it is well-established that when a statute has conferred on any body the power to make decisions affecting individuals, the courts will not only require the procedure prescribed by the statute to be followed, but will readily imply so much and no more to be introduced by way of additional procedural safeguards as will ensure the attainment of fairness."[70]

However, one would hope, despite how contextualised any judgment as to a potential breach of natural justice must inevitably be, it surely remains that strong evidence that an advisory-only algorithm had become fully determinative in practice would allow a strong challenge on the grounds of an unlawful 'fettering of discretion'.

7. Data-driven inequalities

'Data legacy' injustices such as patterns and trends of racial disparities in recorded information across the criminal justice system raises concerns of flaws that might exist in the design of an algorithm, otherwise constructed objectively fairly, that will draw on 'big data' that is tainted by human collection or input biases. As Domingos has put it: "Machine learning is a kind of knowledge pump: we can use it to extract a lot of knowledge from data, but first we have to prime the pump."[71] As such, in the deployment of algorithms in the criminal justice sphere, there could be a problem with a "… a pernicious feedback loop."[72]

---

[68] Marion Oswald, Jamie Grace, Sheena Urwin & Geoffrey C. Barnes (2018) Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, *Information & Communications Technology Law*, DOI: 10.1080/13600834.2018.1458455 p.238.

[69] See *Barnard v National Dock Labour Board* [1953] 1 All ER 1113

[70] *Lloyd v McMahon* [1987] UKHL 5, page 11.

[71] Pedros Domingos, The Master Algorithm: How the Quest for Ultimate Machine Learning will Remake Our World, 2017 Penguin Books, p.64.

[72] Cathy O'Neil, *Weapons of Maths Destruction: How Big Data Increases Inequality and Threatens Democracy*: (p.87)

A pioneering study by Brantingham, Valalisk and Mohler on the arrest-rate-by-ethnicity effects of using machine-learning, predictive police area-patrolling found a number of 'null' results, including the finding that their statistical "analyses do not provide any guidance on whether arrests are themselves systemically biased" against black and Latino individuals, and the finding that "arrest rates for black and Latino individuals were not impacted, positively or negatively, by using predictive policing"[73]. But "while the mechanisms driving… observed patterns of racial disparity" in terms of criminal justice outcomes including arrest rates, charges and so forth are "difficult to disentangle", there is "little doubt" they exist[74].

In the case of *Loomis* in 2016, the Wisconsin Supreme Court, despite its dismissal of the claims by Loomis that the use of a sentencing algorithm was unconstitutional for lack of due process protection, did however identify that "concern that risk assessment tools may disproportionately classify minority offenders as higher risk, often due to factors that may be outside their control, such as familial background and education" [75]. For another example, as Big Brother Watch have observed:

> "…many facial recognition algorithms disproportionately misidentify black people and women. In the context of law enforcement, biased facial recognition algorithms risk leading to disproportionate interference with the groups concerned – whether through police stops and requests to show proof of identity, or through the police's storage of 'matched' biometric photos… However, the commercial facial recognition software used by South Wales Police and the Metropolitan Police, NEC's NeoFace Watch, has not been tested for demographic accuracy biases."[76]

An interesting case study (and one in many senses ahead of its time) is the report from the Waitangi Tribunal in New Zealand[77] that presented a failure to respect *kaupapa maori* ('a

---

[73] Brantingham, P. Jeffrey, Matthew Valasik, and George O. Mohler. "Does Predictive Policing Lead to Biased Arrests? Results from a Randomized Controlled Trial." *Statistics and Public Policy* 5.1 (2018): 1-6, p.5.

[74] Brantingham, P. Jeffrey, Matthew Valasik, and George O. Mohler. "Does Predictive Policing Lead to Biased Arrests? Results from a Randomized Controlled Trial." *Statistics and Public Policy* 5.1 (2018): 1-6, p.2.

[75] *Loomis v State of Wisconsin* (2016) WI 68, para. 62.

[76] Big Brother Watch, *Face Off: The lawless growth of facial recognition in UK policing*, May 2018, p.16.

[77] The Treaty of Waitangi (1840) is interpreted and applied as a 'living instrument' by the Tribunal, itself created by the Treaty of Waitangi Act 1975. The Tribunal applies the following principles:

- "to act with utmost good faith towards Maori ;
- "actively to protect the interests of Maori ;
- "to consult with Maori on policies that affect them ;
- "to treat Maori equally with non-Maori ; and
- "to remedy breaches of the Treaty when these are identified."

From the claim by Tame Hemopo, presented in summary at page 3 of the *Offender Assessment Policies* case report, available at: https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_68001752/Offender%20Assessment%20Policies.pdf (accessed 28.07.2018)

way of doing things from a Maori worldview'[78]) in respect of the claim cited as *Offender Assessment Policies (Tame Hemopo)* (2005) WAI 1024. In the *Hemopo* case, algorithmic offender management software (that was deployed with Maori offenders only) over-estimated a risk of recidivism due to a flawed notion of *whanau* ('family'[79]) which was weighted negatively in the assessment of an individual's likelihood of re-offending and gang crime. The Waitangi Tribunal found that the algorithm concerned had been developed in a problematic way, since "certain shortcomings in the department's management of the process by which [the algorithm had been] designed, implemented, and evaluated mean[t] that the Treaty principle of active protection of Maori interests [had] not been upheld".[80]

The constitutional values of the Treaty of Waitangi were of immense benefit in the *Hemopo* case in terms of being able to demonstrate the unfairness and the injustice of an algorithm consciously (and incorrectly) built on a cultural or ethnic criterion. In an even more progressive manner, the Canadian courts had first determined, in relation to the use of an algorithm that predicted offender risk, that the *absence* of evidence the algorithm concerned is non-discriminatory can be unlawful, in the decision in the Court of Appeal case of *Ewert v Canada* 2015 FC 1093. However in another Court of Appeal judgment in the same case (*Ewert v Canada* 2016 FCA 203) the court held that as a matter of proper legal procedure it was for the *claimant* to establish evidence of discrimination in the operation of the actuarial tests that comprised the algorithm concerned. In essence, in the view of the Court handing down the two judgments in *Ewert*, there was a paucity of evidence, much of it conflicting, as to the culturally biased effects and operation of algorithmic profiling tools.

What had been at issue in *Ewert*, before it was recently repealed, was the language of Corrections and Conditional Release Act s.4 (g) which stipulated that: "... correctional policies, programs and practices respect gender, ethnic, cultural and linguistic differences and are responsive to the special needs of women, aboriginal peoples, persons requiring mental health care and other groups...", and s.4 (1) of the Act, which had provided that "The Service shall take all reasonable steps to ensure that any information about an offender that it uses is as accurate, up to date and complete as possible." In addition, Section 7 (right to liberty) and Section 15 (right to equal benefit of the law without discrimination) of the Canadian Charter of Rights and Freedoms were used by the courts in the *Ewert* decisions to provide a wider interpretive framework - but as noted above, the claim was eventually rejected because of a shift in the Court of Appeal's understanding of the applicable burden of proof.

A lesson to draw from the combined insights of the *Loomis*, *Hemopo*, and *Ewert* for the UK as a jurisdiction is that there is probably some strength in using a combination of challenges to algorithms based on racially- or culturally-skewed data, by drawing on grounds of claim such as Article 14 of the ECHR (the right to freedom from discrimination) in conjunction with Article 6 ECHR (the right to a fair hearing) and/or Article 8 ECHR (the rights to respect for private life); and also in conjunction with the public sector equality duty to have due regard to the need to reduce discrimination under S.149 Equality Act 2010. A discriminatory

[78] From https://yournz.org/2017/02/22/what-is-kaupapa-maori/ (accessed at 28.07.2018)

[79] "Whānau is often translated as 'family', but its meaning is more complex. It includes physical, emotional and spiritual dimensions… Whānau can be multi-layered, flexible and dynamic. Whānau is based on a Māori and a tribal world view." From https://teara.govt.nz/en/whanau-maori-and-family/page-1 (accessed at 28.07.2018)

[80] *Offender Assessment Policies* case report, available at: https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_68001752/Offender%20Assessment%20Policies.pdf (accessed 28.07.2018), pp.16-17.

difference in treatment, such as the disproportionately higher profiling for risk based in part on the ethnicity of an individual and as calculated by an algorithm that drew on this as a data point, would then be subject to a test as to whether it was 'manifestly without reasonable foundation'[81] in the manner in which it interfered with Article 14 ECHR and at least one other right, as applicable. This ground of challenge could be supported with an argument, if the facts supported such an approach, that the public body or law enforcement officials concerned, in procuring or rolling-out the algorithm being challenged, had not had the requisite 'due regard' to distinct equality objectives under the 'public sector equality duty' - including the lack of consultation, evidence-gathering or impact-assessment, for example[82]. These grounds of challenge could supplement the common law grounds, of course, of a breach of natural justice, an unlawful fettering of discretion, and so forth, that were outlined in an earlier section of this paper, above.

[81] For a contextualised discussion of an application of this test in the welfare claims context, please see T. Raine, 'The Value of Article 14 ECHR: The Supreme Court and the "Bedroom Tax"' U.K. Const. Law Blog (28th Nov 2016) (available at https://ukconstitutionallaw.org/) (accessed at 28.07.2018)

[82] The 'PSED' is embodied in Section 149 of the Equality Act 2010, which requires, in essence, that:

> "(1) A public authority must, in the exercise of its functions, have due regard to the need to—
>
> (a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;
>
> (b) advance equality of opportunity between persons who share a relevant protected characteristic[82] and persons who do not share it;
>
> (c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it."

8. Known accuracy biases and public policy

At this juncture in this piece, it is appropriate to consider the third and final element of any argument concerning 'algorithmic impropriety' - that of 'known accuracy biases', and the way these can develop in the process of creating and deploying an algorithm according to public policy priorities.

To begin with, so as to avoid overstating the problem, we should consider the idea that an algorithm will only be, most likely and ordinarily, deployed in only an advisory capacity. As a result, a claimant in judicial review, one would imagine, would run up against the issue that an algorithm built with expertise, and that advises an expert decision-maker, would not necessarily be an issue that entails a decision is "compromised by the use of specialist knowledge or expertise", as Lord Hope identified in *Gillies v Work and Pensions Secretary (Scotland)* [2006] UKHL 2 at 23, when concluding that expertise wielded by a tribunal member did not have the same quality as bias in the sense of an unlawful bias.

Indeed, it is much harder in principle to argue against the lawful use of algorithms where they are merely tools to which a human expert or evaluator can adduce a degree of scepticism or open-mindedness, as is required (setting aside the other issue that such an expert user may become jaded and subject to a degree of acquiescence to an algorithm's predictions over time, discussed below). Indeed, as Cathy O'Neil has noted:

> "For all of their startling power, machines cannot yet make adjustments for fairness, at least not by themselves. Sifting through data and deciding what is fair is utterly foreign to them and enormously complicated. Only human beings can impose that constraint."[83]

So what about seeing a challenge to the use of an algorithm as complemented by a parallel challenge to the fairness of the process used to set policy priorities in designing it? In a recent piece about the Durham Constabulary HART project, researchers explained that there are issues around the motivations of the human beings (read *policymakers*) setting the ratios of different kinds of errors (and the emphases for accuracies this creates) in constructing and rolling-out an algorithm:

> "…the random forests technique treats different types of errors as being differentially 'costly'. The errors with the highest costs are avoided, and therefore occur less frequently than those that are less costly. These costs are set deliberately prior to the model's construction, and in Durham were arrived at after a series of test models were presented to senior members of the Constabulary. The HART model intentionally favours (i.e. applies a lower cost to) cautious errors, where the offenders' levels of risk are over-estimated. Under-estimates of the offenders' actual risk levels, referred to as dangerous errors, are assigned a higher cost and therefore occur less frequently. While both of these examples are errors in forecasting, the consequences and community impact are very different. The ratio of these two costs was set so that the model produces roughly two cautious errors for each dangerous error."[84]

---

[83] Cathy O'Neil, *Weapons of Maths Destruction: How Big Data Increases Inequality and Threatens Democracy*: (p.155)

[84] Marion Oswald, Jamie Grace, Sheena Urwin & Geoffrey C. Barnes (2018) Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality, *Information & Communications Technology Law*, DOI: 10.1080/13600834.2018.1458455 p.228)

Some authors have described this ratio-setting to prefer 'errors' of different kinds, to establish policy priorities, as the creation of 'trade-offs' in the construction of algorithms. However:

> "…the various tradeoffs [sic] need to be presented and available as tuning parameters that can easily be adjusted. Such work is underway, but the technical challenges are substantial. There are conceptual challenges as well, such as arriving at measures of fairness with which tradeoffs can be made… in the end, it will fall to stakeholders - not criminologists, not statisticians and not computer scientists - to determine the tradeoffs. How many unanticipated crimes are worth some specified improvement in conditional use accuracy equality? How large an increase in the false negative rate is worth some specified improvement in conditional use accuracy equality? These are matters of values and law, and ultimately, the political process. They are not matters of science… [and] one cannot expect any risk assessment tool to reverse centuries of racial injustice or gender inequality. That bar is far too high."[85]

In summary, then, it "cannot be overemphasised that these tradeoffs result from stakeholder policy preferences built into the forecasts."[86] This would allow a detailed examination, as part of an administrative court's determination as to the lawfulness of the use of an algorithm, as to the framing and approach of the relevant 'stakeholders' or policymakers in making choices over the qualities of the algorithm at the (re)development stage. This process could be scrutinised using the framework of the common law grounds of review as outlined above, earlier in this piece. In addition, the PSED or thematically-similar human rights grounds of non-discrimination could also be addressed to this formative process for an algorithm.

The next section of this piece discusses the extent to which Part 3 of the new Data Protection Act 2018 offers arguments for the review of control of an algorithm to be used in the criminal justice context, to augment the notion of 'algorithmic impropriety' that draws on the common law grounds of review presented above, and centred around key considerations of the right to restriction of processing (of data points in an algorithm).

9. Discussion of the impact of the Data Protection Act 2018

This section of this piece addresses the most pertinent provisions of the Data Protection Act 2018, and in particular part 3 of the 2018 as it applies to the way algorithms process the personal data of individuals in the law enforcement and criminal justice context. Part 3 of the 2018 is underpinned by the EU Law Enforcement Directive on data processing for law enforcement purposes, and contains a number of safeguards on fair and lawful criminal justice-specific data processing that a claimant party would want to bring to bear if possible on the argued mis-use of an algorithmic tool and in seeking judicial review of the adoption or deployment of the tool.

---

[85] Berk, Richard, et al. "Fairness in criminal justice risk assessments: the state of the art." *arXiv preprint arXiv:1703.09207* (2017), p.35.

[86] Berk, Richard A., Susan B. Sorenson, and Geoffrey Barnes. "Forecasting domestic violence: A machine learning approach to help inform arraignment decisions." *Journal of Empirical Legal Studies* 13.1 (2016): 94-115, 104.

As the 2018 Act is still new, what I would view as the most powerful argument afforded to those who would challenge the use of an algorithmic tool to make a prediction about their own personal risks of re-offending, for example, would be the measures in the 2018 Act that require the restriction of the processing of data that cannot be proven to be accurate. (Section 47(3) of the DPA 2018 requires that processing should be restricted where "it is not possible to ascertain whether it is accurate or not".)

The key hypothetical question (at this stage) is: Can an algorithmic prediction of risk be proven to be accurate (if or when challenged/reviewed)? This raises two particular points for me. Firstly: As a matter of logic, a prediction of risk is only proven accurate with the passage of time - but a court could take the purposive approach and determine that Parliament would intend for predictions made as accurately as possible and revised as required in order to keep them as accurate as possible - an approach that would chime with the similarly powerful 'right to rectification' in the provisions of, again, Part 3 of the 2018.

However, and secondly: We have seen that policymakers in criminal justice in practice will be presented with packages of choices around which 'trade-offs' to use to make certain types of predictions an algorithmic or machine learning tool as accurate as possible - which entails that for high risk offenders, or low risk offenders, or for individuals ranked in whatever particular kind of classification of offender in the circumstances concerned, there is a chance that an algorithm will have been 'tweaked' to mean that they have been profiled in a group that is less-accurately score than might otherwise have been. Would a court, presented with expert evidence on the ramification of the trade-offs chosen and deployed in the use of one particular algorithm accept that the resulting prediction is in good faith (or to the requisite standard that the court determines) an accurate one for the purposes of Section 47(3) DPA 2018? For that matter, given the discussion above, would the same court be minded to determine that the same algorithm built with those trade-offs, and which had had a persuasive effect on a decision-maker when, say, a person's liberty was at stake, was in fact operating in breach of natural justice and its first strand of fairness of freedom from bias?

If a court determined that the particularities of the 'trade-offs' built into an algorithm, that are chosen by policymakers, have rendered the predictions it makes ones that should be restricted from processing, this begs a follow-up question: what is the exact meaning of 'restriction' of processing? ICO guidance on this would suggest that a prediction about an individual (which is after all personal data identifying a person and, say, their risk of (re)offending) should be made unavailable for those criminal justice professionals who would otherwise be able to access it or share it, since, in the words of the ICO: "Restriction could involve measures such as transferring data to a separate system, or limiting the access through the use of passwords and other access controls".[87]

In terms of other rights offered by the new Data Protection Act 2018 and, moreover, its roots in the EU General Data Protection Regulation (2016) and the Law Enforcement Directive (2016), Wachter et al have criticised arguments for interpreting these instruments in such a way as to establish the combined 'rights' to an 'explanation' (the right to subject access, the right not to have personal data subject to automated processing, and the right to be notified of data processing), and arguing that there is in essence only a weaker right to be informed of

[87] See https://ico.org.uk/for-organisations/guide-to-law-enforcement-processing-part-3-of-the-dp-act-2018/ (accessed at 28.07.2018)

the use of the processing of personal data (by an algorithm or otherwise, therefore)[88]. Certainly, the safeguards on automated processing of law enforcement-related personal data found in Part3 of the DPA 2018, and which stem of course from the LED, are procedurally and substantively weak - yes, a person must be informed that they have been subject to an automated decision, perhaps as a result of an algorithmic tool deployed by the police or another criminal justice agency - but not only must they choose to assert their rights (and how many would?), they ultimately have only the right for a human being to re-make the decision[89]. It would be difficult to prevent a human officer from making the exact same decision as an 'algo-cop' unless they were prevented from accessing the prediction of the latter, unless or should the algorithmic prediction have been restricted, perhaps, from further processing/consideration on the basis of a joint challenge using the 'right to restriction' under Section 47 DPA 2018.

Of course and admittedly, this set of points ignores the issue that Citron and Pasquale identified, that the use of algorithms in criminal justice and other sensitive contexts would best be deployed in a fashion requiring 'human in the loop' monitoring, and so not automated in the DPA 2018 sense at all[90]. The DPA 2018 requires impact assessments when data processing is likely to result in a high risk to the rights and freedoms of natural persons in the criminal justice or law enforcement context[91], and these assessments could be procedurally crucial to stave off 'hyper-nudge'[92]or 'automation bias'[93] in the use of 'human in the loop' law enforcement algorithms, in practice and in the longer term - as a thorough impact assessment should include determining evidence as to the extent to which algorithms have come to dictate professional decision-making in a particular setting.

10. Conclusions: The regulation of algorithmically-informed decision-making

Perhaps we can maintain that human rights law and data protection law might actually be best augmented by the common law grounds of natural justice, fettering discretion, and so forth as an amalgam of 'algorithmic impropriety', in order to most rigorously challenge an objectionable algorithm on the widest array of grounds.

The standards of due process values in the common law may be shifting and changeable, but ultimately they may be more intolerant of 'algorithmic impropriety' than some bodies of legal discourse - the proportionality principle is after all designed to be flexible, and governs the most obvious application of Article 8 ECHR, while the concept of the right to a fair hearing

---

[88] Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Why a right to explanation of automated decision-making does not exist in the general data protection regulation." *International Data Privacy Law* 7.2 (2017): 76-99, 77.

[89] See Section 50, Data Protection Act 2018.

[90] See Citron, Danielle Keats, and Frank Pasquale. "The scored society: due process for automated predictions." *Wash. L. Rev.* 89 (2014): 1.

[91] Section 64, Data Protection Act 2018

[92] See Yeung, Karen. "'Hypernudge': Big Data as a mode of regulation by design." *Information, Communication & Society* 20.1 (2017): 118-136.

[93] Cobbe, Jennifer, Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making (August 6, 2018). A pre-review version of a paper in *Legal Studies*, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3226913 , p.9.

under Article 6 ECHR would inevitably be asserted as one complied with by a public body using an algorithm in an advisory-only capacity. The future applications of corresponding rights in the EU Charter of Fundamental Rights are, sadly, being excised by the process of Brexit, of course[94]. And the principle of non-discrimination as a matter of European human rights law presupposes that there would be evidence to draw upon that an algorithm had been built in such a way as to make predictions that were discriminatory in effect and to a disproportionate extent which was manifestly without reasonable foundation. I would suggest that the public sector equality duty (PSED), with its requirement for 'due regard' to the issues of equality concerned in the stages of actually building the algorithmic (necessitating the use of equality impact assessments and evidence-gathering, in effect) might be at least as useful as the human rights law framework sketched here when it comes to a group sharing a protected characteristic actually challenging that self-same algorithm. As for data protection law, a testing of the application of Part 3 of the Data Protection Act 2018 (and the underpinning Law Enforcement Directive), which would be the provisions applicable in determining the lawfulness or otherwise of an algorithm deployed in the law enforcement context, has yet to occur in the UK courts.

Andrew Selbst, for one, has outlined the need for 'algorithmic impact statements' or assessments, based around a six-part model of regulatory thinking: a) to 'rigorously explore and objectively evaluate all reasonable alternatives…', b) to 'evaluate their comparative merits…', c) to look for alternatives outside the local jurisdiction, d) to 'include the alternative of no action', e) to acknowledge preferred alternatives in impact assessments, and f) to include 'appropriate mitigation measures not already included in the proposed action or alternatives'[95]. Specialist procedural safeguards such as 'algorithmic impact assessments' conducted as Selbst suggests, for example, could be crucial - as algorithms in criminal justice are as ethically-sensitive and potentially as liberties-infringing as any new technology introduced in that most complex and important societal arena[96].

From the example given above of Kent Police and their EBIT algorithm, an inspection of an algorithm in policing contexts has already taken place by HMICFRS - and South Wales Police have stated on their website the range of regulators, including the ICO, that they worked with in deploying 'Identify', their facial recognition project (and which collaboration presumably informed their approach to delivering notifications/notices to those people subject to a false positive identification in real time operations etc.). The current lack of a single specialist regulator for the use of algorithms in 'high stakes' decision-making (given the sharing of the role in the UK currently, *de facto*, between the ICO and HMICFRS) is not *necessarily* a problem from a human rights compliance perspective (although I confess it would be my preference), so long as we give sufficient respect to, and encouragement and facilitation toward, those claimants who would use judicial review as the avenue to challenge an algorithm of concern. As the Court of Appeal for England and Wales observed in *R (XX) v Secretary of State for the Home Department* [2016] EWCA Civ 597 at 25, in that case not in

[94] The EU (Withdrawal) Act 2018 will sever the Charter of Fundamental Rights of the EU from the raft of EU law otherwise incorporated into UK law as 'retained EU law'. The European Union (Withdrawal) Act 2018, section 5(4) states bluntly that: "The Charter of Fundamental Rights is not part of domestic law on or after exit day".

[95] Selbst, Andrew. "Disparate Impact in Big Data Policing." (2017). p.172-173.

[96] See https://bscpolicingnetwork.com/2018/06/14/getting-the-ethics-right-in-police-technology-projects/ (accessed at 28.07.2018)

relation to the use of algorithmic tools, but in relation to criminal record disclosure schemes for public protection purposes:

> "There is no general requirement of an independent overseer though of course it is right to say that the judicial review jurisdiction provides a supervisory discipline to ensure the legality of individual decisions… it takes its place at the apex of a set of arrangements that is full of detailed provisions for the achievement of balanced proportionate decisions, and of course the application of those provisions is liable to scrutiny in the judicial review court."

So for the courts themselves, softer regulation or even police/criminal justice agency self-regulation may be an acceptable option for the control of algorithmic tools in criminal justice contexts, on the basis of relying on judicial review as the overall and final control on algorithmic mis-use.

There is a growing body of case studies of the use of algorithmic tools in criminal justice settings, suggesting that the controversies perceived over the use of such tools will fade over time as their use becomes normalised and routinized. It is likely that tools like EBIT in Kent be used with more serious offence types over time by that force and others. For serious sexual and violent offences however, one would imagine that ultimately there would be public policy barriers, and perhaps eventually, legal barriers to the regular and standardised use of an algorithmic tool which allows the police a *statistical* rationale to side-line and de-prioritise complaints of the worst crimes.

Notably, an advocacy group or an individual claimant victim of a most serious offence might have a strong human rights claim in challenging the de-prioritisation of their complaint, if an algorithm analysing investigation files had not been overseen by a human professional sensitive of public protection priorities and victim vulnerabilities, since *Commissioner of Police of the Metropolis v DSD and another* [2018] UKSC 11 suggests that 'conspicuous or substantial, egregious and significant errors' in police decision-making will lead to an operational breach of Article 3 EHCR. Thus the Kent E-BIT system of oversight of victims' complaints and resulting investigations, resulting in human professional judgment being applied before an investigation into a serious offence is discontinued and a case 'shelved', is a form of 'human in the loop' regulation of the EBIT algorithm that simply has to be maintained as a core standard as a result. As William S. Isaac has concluded, "…agencies that attempt to implement algorithmic decision support should take steps to develop internal and external accountability, ensure operational transparency, and be aware of the long run impact of those tools on their communities"[97].

[97] Isaac, William S. "Data Dreaming: The Myth of Objective Data in the Artificial Intelligence Era of Policing." *Comparative Politics Newsletter* 34.2: 45, 49.