Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Sentencing data-driven cybercrime. How data crime with cascading effects is tackled by UK courts

Maria Grazia Porcedda

School of Law, Trinity College Dublin, Ireland

ARTICLE INFO

Keywords:
Cybercrime
Data protection
Big data
Cloud computing
Technology neutrality
Sentencing

ABSTRACT

This paper contributes to research seeking to understand if and how legislation can effectively counter cybercrimes that compromise personal data. These 'data crimes', which are the 'dark side' of big data and the data economy enabled by cloud computing, display cascading effects, in that they empower disparate criminals to commit further crimes and victimise a broad range of individuals or data subjects. The paper addresses the under-researched area of sentencing, which, as the last step of the judicial process, plays a crucial role in how the law is interpreted and implemented.

This paper investigates courts' approach to the evolving technological environment of cybercrime captured by data crime and the cascade effect and whether the cascade effect can assist courts in dealing with data-driven cybercrime. The paper examines original data collected from UK courts, namely 17 sentencing remarks relating to cybercrime court cases decided in England & Wales between 2012 and 2019. The analysis shows that courts appreciate the impact of data crime and their cascading effects, but that the complexity of the offences is lost at sentencing, arguably due to the negative impact of systemic factors, such as technology neutral law and the lack of legal authorities.

After examining such systemic factors, the paper suggests how the cascade effect could aid sentencing by adding specificity and context to data crime. The paper ends with avenues for further research relating to debates on fair cybercrime sentencing and open justice.

1. Introduction

This article investigates the ability of courts to grapple with the evolution of cybercrime resulting from the wide uptake of cloud computing applications effecting the accumulation of data or big data. Big data spearheaded not only the data economy, but also the "digital currency of the cybercriminal"[1] causing 'data crime' and the 'cascade effect'. In this work, which is part of a wider research agenda investigating cloud crime,[2] data crime refers to the increasing prevalence

Abbreviations: SaaS, software as a service.

E-mail address: Maria-grazia.porcedda@tcd.ie

[1] Paul Hunton, 'Data Attack of the Cybercriminal: Investigating the Digital Currency of Cybercrime' [2011] 28 Computer Law & Security Review 201, 202. See generally Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2020* (2020).

[2] See fn 4, Section 3 as well as funding statement.

https://doi.org/10.1016/j.clsr.2023.105793

of cybercrimes that compromise data, particularly personal data,[3] whereas the cascade effect illustrates the way in which data crime takes form and spreads.[4] Accordingly, cyber-dependent crimes such as unauthorised access to computer systems for criminal purposes 'cascade' crime downstream, empowering criminals to commit further cyber-enabled crimes, such as the sale of data, [5] and cyber-assisted crimes more generally.

This paper asks, in particular, whether courts appreciate the evolving technological environment of cybercrime captured by data crime and the cascade effect and how they react to it, and suggests how the cascade effect can assist courts in better dealing with data-driven cybercrime cases. These are broad and largely unanswered questions, particularly because research is hampered by the lack of adequate data internationally. This work focusses on the UK and, for methodological reasons discussed in Section 3, specifically England & Wales. As there are no official reports on cybercrime in the UK, documentation is haphazard, and the literature, which is discussed in Section 2, either focusses on high profile cases or tackles the matter at a theoretical level. This study therefore addresses the scholarly gap by analysing the sentencing of data crimes, understood as data-driven cybercrimes spurred by applications such as cloud computing. To answer the questions, 17 sentencing remarks of cases decided in English and Welsh Courts between 2012 and 2019 were analysed.

Understanding how courts grapple with the evolution of cybercrime is relevant beyond scholarship. As the last step of the criminal justice process, sentencing can have an impact on the success or failure of the fight against cybercrime. It influences how the applicable law on cybercrimes is interpreted,[6] and which of the multiple objectives of the criminal justice system end up being privileged, including the reduction of crime by deterrence and the reform and rehabilitation of offenders.[7] Sentencing can thus have a considerable impact on the success, or failure, of the fight against cybercrime and the victimisation of data subjects.

There are currently no sentencing guidelines for the Computer Misuse Act 1990 (hereafter CMA1990) and this analysis suggests that refined guidelines for s.6 and s.7 of the Fraud Act 2006, as well as brand-new sentencing guidelines for the CMA 1990, may be in order. Equally important is the need to rely on all instruments available, and particularly the Data Protection Act 2018 (hereafter DPA 2018).

The article is organised as follows. Section 2 contains the state of the art and explains how this work contributes to different bodies of literature on courts and technology, as well as the criminal justice fight against cybercrime, and how it fills existing gaps. Section 3 illustrates the concepts of data crime and the cascade effect as well as the methodology informing this work, including an explanation on how to collect court data. Section 4 contains the analysis of the sentencing remarks. Section 5 discusses the findings and limitations of the research. The paper concludes with a recommendation to debate effective strategies to fight against cybercrime.

2. State of the art: cybercrime, tech law and sentencing

This paper draws from and seeks to contribute to works that appraise the legal responses to cybercrimes in general, and specific instances of cybercrime in particular (2.1) and to the research gap on the sentencing of cybercrime (2.2). This section ends with an introduction of the concept of technology neutrality, which will be relied on in the analysis of sentencing remarks (2.3).

2.1. *Cybercrime*

This article seeks to contribute to three bodies of cybercrime scholarly literature.[8]

The first is the adequacy of cybercrime legislation, which has come under scrutiny in countries across the globe.[9] Literature reviewing UK national legislation, including in a compar-

[3] As defined in Art 4(1) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such data (General Data Protection Regulation) [2016] OJ L 119/1. European Data Protection Board (EDPB), *Guidelines 1/21 on Examples regarding Data Breaches, v1.0* (2021).

[4] Data crime and its cascading effects were conceptualized in Maria Grazia Porcedda and David S. Wall, 'Data Crime, Data Science and the Law' in Vanessa Mak, Erik Tjon Tijn Tai and Anna Berlee (eds), *Research Handbook on Data Science & Law* (Edward Elgar 2018); Maria Grazia Porcedda and David S. Wall, 'The Chain and Cascade Effects in Cybercrime: Lessons from the TalkTalk Case Study' (IEEE Euro S&P 2019); Maria Grazia Porcedda and David S. Wall, 'Modelling the Cybercrime Cascade Effect in Data Crime' (IEEE Euro S&P 2021).

[5] Or even less sophisticated offences such as swatting, which means making hoax calls to emergency services so as to cause several armed police officers to show up at a specific address, typically of someone extraneous to the calls and, in cybercrime cases, whose data may have been leaked.

[6] Simon McKay (Editor), Audrey Guinchard, Peter Sommer, Lyndon Harris, Sebastian Walker, Amy Woolfson et al., 'Reforming the Computer Misuse Act 1990' (The Criminal Law Reform Now Network 2020), Annex C.

[7] Section 142 of the Criminal Justice Act 2003 as amended by section 57 of the Sentencing Act 2020 (discussed in Section 3.2).

[8] Cybercrime is a broad scholarly field. For textbooks, monographs, reports and literature reviewes, see generally: Majid Yar and Kevin F. S Steinmetz, *Cybercrime and Society (3rd Edition)* (Sage Publishing 2020); Alisdair A. Gillespie, *Cybercrime: Key Issues and Debates* (2019); Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press 2016); Susan Brenner and Bert-Jaap Koops (eds), *Cybercrime and Jurisdiction. A Global Survey* (TMC Asser Press 2006); Susan Brenner, *Cyberthreats and the Decline of the Nation-state* (Routledge 2014); David S Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007); Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press 2010); Marleen Weulen Kranenbarg and E. Rutdger Leukfeldt (eds), *Cybercrime in Context: the Human Factor in Victimization, Offending, and Policing* (Springer 2021); Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (International Telecommunication Union, Geneva, 2012); Stearns Broadhead, 'The Contemporary Cybercrime Ecosystem: A Multi-disciplinary Overview of the State of Affairs and Developments' [2018] 34 *Computer Law & Security Review* 1180.

[9] In the CLSR, see: Felix E. Eboibi, 'A Review of the Legal and Regulatory Frameworks of Nigerian Cybercrimes Act 2015' 33 700; Kinfe Micheal Yilma, 'Ethiopia's New Cybercrime Legislation: Some Reflections' 33 250; Duryana binti Mohamed, 'Combating the Threats of Cybercrimes in Malaysia: the Efforts, the Cyberlaws and the Traditional Laws' 29 66; Felicity Gerry and Catherine Moore, 'A Slip-

ative perspective,[10] typically focusses on the CMA1990 and the Fraud Act 2006.[11] Some works focus on specific issues, such as young cyber offenders[12] and security researchers.[13] The Criminal Law Reform Now Network report (hereafter CLRNN report) released in 2020 found "the Computer Misuse Act 1990…not fit for purpose to tackle current policing and national security challenges" [14] and points to directions for review. This research adds to this strand of literature, particularly by providing evidence, in the form of original data, to buttress claims theorized at various points by the literature.

A second strand of cybercrime literature assesses the ability of legislation to keep up with technological changes, such as the Internet of Things.[15] 'Cloud computing' has been widely discussed in cybercrime circles for its impact on the collection of electronic evidence.[16] This research adds to the literature by investigating how the use of cloud computing, and phenomena derived from it, are affecting the cybercrime ecosystem.

Thirdly and lastly, cybercrime is typically classed into categories of offences;[17] here I rely on the classic subdivision into 'cyber-dependent', 'cyber-enabled' and 'cyber-assisted' crimes.[18] The first relates to offences that would not exist without network and information systems and typically are 'against the machine', such as hacking. The second category covers offences that predate network and information systems but are greatly magnified by them, typically fraud and other economic crimes. The latter concerns offences that largely take place in the offline world and for which network and information systems are incidentally useful, such as online recruitment of potential terrorists or online grooming of children for abuse.

Each category benefits from a body of dedicated research, although it is understood that the categories are somewhat artificial,[19] within and across groups[20] – admittedly the distinction between cyber-enabled and assisted crimes is not always clear-cut. Indeed, offending often spans more than one category and can entail several offences from each group at once. For instance, the steps an intruder needs to take to commit cyber dependent crime, as exemplified by the kill chain,[21] and Hunton's cybercrime execution stack[22] typically involve multiple sections of the CMA1990 and Fraud Act 2006 (and Data Protection Act 2018, see Section 4).

The big data 'revolution' and the data economy are accelerating the blurring of boundaries within and between categories. For years, data, typically personal within the meaning of §5 DPA2018/ Art 4(1) GDPR, has been sought through a variety of avenues and traded within illicit data markets.[23] The concept of 'data crime'[24] intends to capture the suite of cybercrimes that prey on – primarily personal – data, whereas the cascade effect seeks to show how cloud computing and big data are, among other things, causing the three categories of cybercrime to collapse into one another (Section 3).

pery and Inconsistent Slope: How Cambodia's Draft Cybercrime Law Exposed the Dangerous Drift Away from International Human Rights Standards' 31 628; Ting Zhang, 'A Comparative Study on Sanction System of Cyber Aider from Perspectives of German and Chinese Criminal Law' 33 98.

[10] Clough (2010) (n 8).

[11] Among many: Oriola Sallavaci, 'Combating Cyber Dependent Crimes: The Legal Framework in the UK' [2016] 630 *Communications in Computer and Information Science* 53; Stefan Fafinski, 'The UK Legislative Position on Cybercrime: A 20-Year Retrospective' [2009] 3 *Journal of Internet Law*; David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*; Lachlan Urquhart, 'Exploring Cybersecurity and Cybercrime: Threats and Legal Responses' in Lilian Edwards (ed) *Law, Policy and the Internet* (Hart Publishing 2018); Maureen Johnson and Kevin M. Rogers, 'The Fraud Act 2006: The E-Crime Prosecutor's Champion or the Creator of a New Inchoate Offence?' [2007] *21 International Review of Law, Computers & Technology* 295; Richard Walton, 'The Computer Misuse Act' 11 *Information Security Technical Report* 39.

[12] David S. Wall, 'Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Implications for Regulation and Policing' in Roger Brownsword, Elaine Scotford and Karen Yeung (eds), *The Oxford Handbook of the Law and Regulation of Technology* (Oxford Univeristy Press 2017).

[13] Audrey Guinchard, 'The Computer Misuse Act 1990 to Support Vulnerability Research? Proposal for a Defence for Hacking as a Strategy in the Fight against Cybercrime' [2018] 2 *Journal of Information Rights, Policy and Practice*.

[14] McKay et al. (2020) (fn 6), 30.

[15] Lachlan Urquhart and Derek McAuley, 'Avoiding the Internet of Insecure Industrial Things' 34 *Computer Law & Security Review* 450

[16] Among many: Jospeh J. Schwerha, *Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"* (Council of Europe Project on Cybercrime, 2010); Stephen Mason and Esther George, 'Digital Evidence and 'Cloud' Computing' [2011] 27 *Computer Law & Security Review* 524; Cybercrime Convention Committee (T-CY), *Criminal Justice Access to Data in the Cloud: Challenges*. Discussion paper prepared by the T-CY Cloud Evidence Group (2015); Dan Jerker B. Svantesson and Lodewijk van Zwieten, 'Law Enforcement Access to Evidence via Direct Contact with Cloud Providers – Identifying the Contours of a Solution' [2016] 32 *Computer Law & Security Review* 671; M Taylor, J. Haggerty, D. Gresty and R. Hegarty, 'Digital Evidence in Cloud Computing Systems' [2010] 26 *Computer Law & Security Review* 304.

[17] Council of Europe, Convention on Cybercrime, CETS n. 105 23 November 2001; Wall (2007) (n 8); Yar and Steinmetz (2020) (n 8).

[18] See generally, Wall (2017) (n 12); on cyber-dependent and cyber-enabled crime see also https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.

[19] Gercke (2012) (n 8).

[20] The authors of the CLRNN dissect CMA offences, which belong in the cyber-dependent crime category, and conclude they "have not been sufficiently theorized" McKay et al. (2020) (n 6), 123.

[21] E Hutchins, M Cloppert and R Amin, *Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* (Lockheed Martin 2011).

[22] Hunton (2011) (n 1).

[23] Françoise Gilbert, 'Breach of System Security and Theft of Data: Legal Aspects and Preventive Measures' [1992] *11 Computers & Security* 508; Hunton (2011) (n 1); Alice Hutchings and Thomas J. Holt, 'A Crime Script Analysis of the Online Stolen Data Market' [2015] 55 *British Journal of Criminology* 596; Thomas J. Holt, Olga Smirnova and Yi Tin Chua, *Data Thieves in Action: Examining the International Market for Stolen Personal Information and Cybercrime* (Palgrave MacMillan 2016); R Wainwright and F Cilluffo, *Responding to Cybercrime at a Scale: Operation Avalanche – a Case Study*, Issue Brief # 2017 –03 (2017); Alice Hutchings and Holt Thomas J., 'The Online Stolen Data Market: Disruption and Intervention Approaches' [2016] 18 *Global Crime* 11; J Saunders, 'Tackling Cybercrime – the UK response' [2016] 2 *Journal of Cyber Policy* 4; Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018* (2018).

[24] Porcedda and Wall (2018) (n 4).

2.2. *Courts and cybercrime: sentencing*

In general, there is no comprehensive review of cybercrime judgments in England and Wales to date. Cybercrime-related sentencing works have thus far focussed on the role of neurodiversity[25] and public perception.[26] The CLRNN report brought a much-needed discussion of practical and theoretical issues concerning sentencing of cybercrime offenders.[27]

Following the authors of the CLRNN report, part of the problem is that sentencing has traditionally played a lesser role in legal theory, and has only recently started commanding the attention it deserves.[28] Sentencing may be the last step of the criminal justice process, but it influences how the applicable law on cybercrimes is interpreted,[29] and which of the multiple objectives of the criminal justice system defined in the Criminal Justice Act 2003, as modified by the Sentencing Act 2020 are privileged. There are currently no sentencing guidelines on the CMA 1990.

Even so, the CLRNN report focusses on Court of Appeal cases, much like the rest of the legal and criminological literature which relies on cases from hierarchically higher courts.[30] Yet, the vast majority of cybercrime cases are heard and sentenced at Magistrates' and Crown Court level, whose sentencing remarks are not commercially reported. As a result, there is a dearth of data to build literature on,[31] which contributes to the lack of a comprehensive case law review.

There are no studies scrutinizing how the courts' interpretation of cybercrime law is affected by technologies such as cloud computing, as captured for instance by data crime and the cascade effect (Section 3). There are also no works appraising sentencing in light of such changes. This article seeks to fill the gap by discussing sentencing of cybercrime and highlighting some shortcomings, eg with regard to the sentencing of young offenders. The data collection and analysis for this article was completed in 2019, before the passing of the Sentencing Act 2020.

2.2.1. *The interpretation of technology neutral cybercrime law vis-à-vis the evolution of the cybercrime ecosystem*[32]

A discussion of the interpretation of cybercrime law at sentencing must be cognisant of the interplay between the technological environment enabling cyber-offending and how cybercrime law is written. Europol's quote that "cybercrime is an evolution, not a revolution[33] hints at the role of the technological environment enabling cybercrime. Accordingly, the fundamentals of cybercrime remain unchanged in the face of the offenders' adaptation to technical change. The technological environment enabling cybercrime underpins both cybercrime discourse and law.

The lack of definition of key terms, such as 'computer' in the CMA 1990[34] reflects the underlying regulatory approach to 'cyber' law[35] that goes by the shorthand of 'technology neutrality'. Technology neutrality means to neither favour, specify, force nor discriminate against[36] a specific technology, although the concept can be couched in many manners and is thus inherently ambiguous.[37] Technology neutrality finds as many supporters as it has detractors, as I review elsewhere.[38]

The purpose of introducing technology neutrality is to be cognizant of its potential role in the work of courts. Indeed, cybercrime instruments are seldom amended and when they are, revisions are carefully worded to avoid any references to specific technologies that could make them quickly obsolete. The task of interpreting legislation in light of the changing technological environment, and the creative ways found by offenders to exploit it, is left to courts.

Without condemning technology neutrality as a regulatory technique, scholars have pointed to a number of issues in the interpretation by courts of technology neutral law. For instance and as mentioned above, the authors of the CLRNN report stress how the lack of definition of key terms such as 'computer' have led to an overreach of the CMA 1990.[39] Greenberg highlights four shortcomings or 'problems'[40] caused by

[25] Penny Cooper, 'Sentencing: Autism Spectrum Disorder–R. v Mudd (Adam Lewis)' *Criminal Law Review* 243

[26] Alessandro Acquisti and Ross Anderson, 'Perception versus Punishment in Cybercrime' [2019] 109 *Journal of Criminal Law and Criminology* 313.

[27] McKay et al. (2020) (n 6), 115.

[28] Jose Pina-Sánchez, 'Defining and Measuring Consistency in Sentencing' in Julian V. Roberts (ed), *Exploring Sentencing Practice in England and Wales* (Palgrave Macmillan 2014); Jose Pina-Sánchez and Linacre, 'Enhancing Consistency in Sentencing: Exploring the Effects of Guidelines in England and Wales' [2014] 30 *Journal of Quantitative Criminology* 731; Mandeep Dhami and Ian Belton, 'Using Court Records for Sentencing Research: Pitfalls and Possibilities' in Julian V. Roberts (ed), *Exploring Sentencing Practice in England and Wales* (Palgrave Macmillan 2014).

[29] McKay et al. (2020) (n 6), Annex C.

[30] Clough (2010) (n 8); Urquhart (2018) (n 8, 15); NF MacEwan, 'The Computer Misuse Act 1990: Lessons from its Past and Predictions for its Future' [2008] 12 *Criminal Law Review* 955; Fafinski (2009) (n 11).

[31] Dhami and Belton (2014) (n 28).

[32] See funding and acknowledgments sections for credits on this portion of the literature review.

[33] Europol, *IOCTA 2020* (n 1).

[34] McKay et al (2020) (n 6).

[35] The Law Commission, *Criminal Law. Computer Misuse* (1989).

[36] Jerry Mashaw and David L. Harfst, 'From Command and Control to Collaboration and Deference: The Transformation of Auto Safety Regulation' [2017] 34 *Yale Journal on Regulation* 167; Brad. A Greenberg, 'Rethinking Technology Neutrality' [2016] 100 *Minnesota Law Review* 1495.

[37] As noted by Bert-Jaap Koops, 'Should ICT Regulation be Technology Neutral?' in Bert-Jaap Koops and others (eds), *Starting Points for ICT Regulation* (TMC Asser Press 2005); Lyria Bennett Moses, 'Regulating in the Face of Socio-Technical Change' in Roger Brownsword, Elaine Scotford and Karen Yeung (eds), *The Oxford Handbook of the Law and Regulation of Technology* (Oxford University Press 2017); Chris Reed, *Making Laws for Cyberspace* (Oxford University Press 2012); Martin Cave and Tony Shortall, 'How Incumbents can Shape Technological Choice and Market Structure – the Case of Fixed Broadband in Europe' [2016] 18 *Info* 2; Greenberg (2016) (n 36).

[38] For a debate, see above. Maria Grazia Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law. A Law, Policy and Technology Analysis* (Hart Publishing 2023), ch 5.

[39] McKay et al. (2020) (n 6).

[40] Greenberg (2016) (n 36).

technology neutrality on judicial decision-making in the context of copyright. First, the promise of technology neutrality to anticipate 'known unknowns' creates a problem of prediction. Secondly, technology neutrality "amplifies the general jurisprudential challenge of determining what the law governs and whether it should",[41] which he calls the problem of 'the penumbra'. Thirdly, the problem of perspective embodies the question whether judges will implement the law by looking at technological output or its design, as tech neutrality can be applied to both. Finally, technology neutrality suffers from the problem of 'pretense', whereby the socio-political context in which technology is developed and adopted is ignored. Greenberg's third problem, that of perspective, was also addressed by Chandler[42] and Grabowski,[43] who suggest it could be caused by technology that is too complex, leading courts to either legitimize its social acceptance[44] or 'disregard duty'[45] to interpret the law in light of its functioning. Elsewhere I suggest that technology neutrality also causes 'indeterminacy loops' in the interpretation of technology law that courts cannot close. [46]

In this research, technology neutrality comes to the fore in the analysis of sentencing remarks; in this guise, the research adds to the literature by offering an example of the interpretive issues arising from technology neutral legislation in a cybercrime context. I then propose how data crime and its cascading effects can act as a tool to conceptualise the complexity that the technology neutral applicable law is unable to render.

3. The cascade effect of data crime and research design

After illustrating the meaning of the cascade effect, and how it was developed, I discuss how sentencing remarks were collected and how they are analysed in this research.

3.1. *The cascade effect: what it is and how it was developed*

The cascade effect conceptualises the impact on cybercrime of applications such as cloud computing and big data. Cloud computing is a shorthand for solutions ranging from programs available to any Web end-users (Software as a Service or SaaS) to resources central to the functioning of the Internet (Infrastructure as a Service). This is reflected in the existing ISO/ITU international standard,[47] which broadly defines characteristics that make up the cloud, namely 'access', 'scalable', 'elastic' and 'shareable' as well as 'resources'. Binding definitions, such as that contained in the NIS Regulations 2018 transposing the EU Directive on Network and Information Systems,[48] do not reduce the breadth of applications falling under the umbrella of cloud.

In spite of its unclear contours, the paradigm of cloud computing has had a game-changing effect on the IT sector. It has supported growth in connectivity and processing power, thereby leading to the production of data that is of massive size and volume, i.e. big data. Understood as either a technical[49] or social resource,[50] big data is at the heart of economic and business investment,[51] whether licit or not.

Cybercriminals were inevitably drawn to big data and analytics. Symantec's account of a dramatic increase in attacks that target data[52] chimes with news that over one third of EU Member States reported incidents relating to illegal acquisition of data.[53] These figures illustrate a double trend in cybercrime: the increase in unauthorized access to data for financial reward or intelligence gathering[54] and the proliferation of markets to trade the illicit acquisition of such data[55] alongside cybercrime paraphernalia. 'Data crime' tries to capture this double trend.[56]

Data crime, made possible by cloud applications and big data, creates cascading effects in cybercrime. The effects refer to cyber-dependent crimes that 'cascade' crime downstream to enable cyber-enabled and even cyber-assisted cybercrimes to take place. As a consequence, data crime is likely to engage the whole regulatory spectrum of norms on cybercrime.

---

[41] ibid, 1529.

[42] Jennifer A. Chandler, 'The Autonomy of Technology: Do Courts Control Technology or Do They Just Legitimize its Social Acceptance?' (2007) 27 *Bulletin of Science, Technology and Society* 339

[43] Mark Grabowski, 'Are Technical Difficulties at the Supreme Court Causing a "Disregard of Duty"?' [2011] *Journal of Law, Technology & Internet* 93.

[44] Chandler (2007) (n 42).

[45] Grabowski (2011) (n 43).

[46] Porcedda (2023) (n 38), ch 5.

[47] International Telecommunication Union (ITU) and International Organization for Standarization (ISO), *International Standard ISO/IEC 17788, Information Technology - Cloud Computing - Overview and Vocabulary, Recommendation ITU/T Y.3500* (International Telecommunications Union 2014). The definition reads "Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Examples of resources include servers, operating systems, networks, software, applications, and storage equipment."

[48] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union [2016] OJ L194/1 (NISD).

[49] Kenneth Neil Cukier and Viktor Mayer-Schoenberger, 'The Rise of Big Data. How It's Changing the Way We Think About the World' *Foreign Affairs* <https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data>.

[50] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' [2015] 30 *Journal of Information Technology* 75

[51] European Commission, 'Building a European Data Economy' (Communication) COM(2017) 9 final.

[52] Symantec, *Internet Threat Security Report 2019* (2019).

[53] Europol, *IOCTA 2018* (n 23), 7 and 22.

[54] Hutchins, Cloppert and Amin (2011) (n 21); Gareth Corfield, 'US govt Accuses Four Chinese Army Soldiers of Hacking Equifax and Siphoning 145m Americans' Personal Info' *The Register* (20 February 2020) <https://www.theregister.co.uk/2020/02/10/china_hacked_equifax_charges/>.

[55] Hutchings and Holt (2015) (n 23); Holt, Smirnova and Chua (2016) (n 23); Saunders (2019) (fn 23); Wainwright and Cilluffo (2017) (n 23); Europol, *IOCTA 2018* (n 23).

[56] Porcedda and Wall (2018) (n 4).

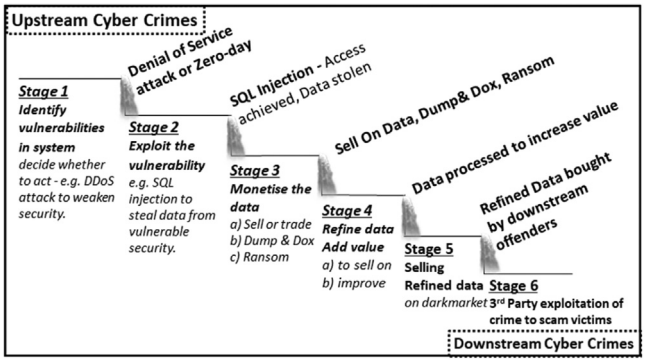

Fig. 1 – The cybercrime cascade effect.[57]

Data crime and the cascade effect cover real-world phenomena that are otherwise addressed heuristically. For instance, Europol stresses that "access to data allows criminals to carry out various forms of fraud. Such data is also available on the dark web, which is often a key enabler of many other forms of illegal activity."[58] However, both the processes surrounding data crime and the cascade effect, as well as their technological enablers, are not fully conceptualised and backed by data. This article is part of a line of work that aims to bridge the gap.[59]

The cascade effect explains how contemporary data crime entails both a vertical effect, which is described in the quote from Europol above, as well as a horizontal one, in that data crime is likely to generate multiple, distributed and unplanned data crimes. The result is that completely unrelated individuals, with no desire or intention to collude, can enable one another to perpetrate a range of cybercrimes against a range of victims equal to or more harmful than those carried out by gangs. This is because the reach of cloud and scale of big data can allow one offender, in certain circumstances, to unleash a range of possibilities for other actors to exploit, causing a seeming 'crime frenzy' resulting in vastly amplified harms. To paraphrase Hunton, "unlike a single physical criminal activity that results in monetary gain", *data crime* "has the potential to be repeated numerous times to commit [multiple] illicit activities."[60]

Fig. 1 and Table 1 represent the cascade effect as a number of steps corresponding to a cybercrime opportunity. Steps 1–3 of the cascade are upstream crimes that roughly correspond to categories of cyber-dependent crime, whereas steps 4–6 are downstream crimes that largely correspond to cyber-enabled (facilitated by the internet) and cyber-assisted (where the internet is incidental) crimes. The first step in Table 1 allows for crimeware-as-a-service to be treated as a factor triggering the cascade effect, though it is not, strictly speaking, a data crime. Steps 3 to 5 make up the 'vicious cycle of monetization', whereby data can be fed back into crime in a seeming endless cycle; in practice, stages 3 to 5 can happen in parallel, or one of the steps may be skipped. Each step also harbours the potential for tipping or pinch points where upstream crimes cascade further downstream. These 'pinch points' are locations where law enforcement, crime prevention and regulatory resources can be directed to make for more effective action.[61]

A different way to represent the cascade is as a decision tree diagram, where each stage of the diagram could be undertaken by different and unrelated actors. Fig. 2 shows the decision tree relating to steps 3–5 of the cascade effect, or the 'vicious cycle of monetization'. The tree illustrates the choices available to unrelated individuals, or groups of individuals, who gained access to the data by completing step 2. In this sense, the cascade effect complements models that describe chains of data attacks,[62] or kill chains,[63] but unlike those, it describes the relational or social enablers for the creation of multiple, overlapping chains.

The cascade effect was developed on the basis of cases drawn from two databases that collate media reports of court cases on cybercrimes sentenced in the UK: Hutching's computer crime database[64] and Turner's CMA 1990 database.[65] Reliance on media reports is inevitable as there are no commercial reports on cybercrime cases to date and other web resources are incomplete;[66] this has far-reaching implications which are addressed in the discussion section. Hutching's 550 entries on individuals, refined through Turner's database, were clustered into a group of 247 cybercrime incidents, as many cases involved groups of individuals acting together.

To conceptualise the evolution of cybercrime, the entries were analysed using grounded theory, because such a theory is about change, the conditions affecting change and the consequences of such change.[67] Following the process of grounded theory, the analysis and data collection go hand in hand, allowing the analysis to direct the subsequent collection of data (the research process guides the researcher)[68] and subsequent literature review.[69] I then engaged in purposive sampling based on four attributes – finalized cases, cloud relevance, apparent cascade and the availability of sentencing remarks.

The first attribute – selecting only sentenced cases – rests on the need to maximize the certainty, quality and amount of data about each case, even though this was not always possible as explained in the discussion section. The second attribute, cloud relevance, is a broad category. It encompasses both cases manifestly about cloud computing applications –

[57] © [2021] IEEE. Reprinted, with permission, from Porcedda and Wall (2021) (fn 4).
[58] Europol, 'Internet Organised Crime Threat Assessment (IOCTA) 2019', 7
[59] Alongside Porcedda and Wall (2018; 2019; 2021) (n 6).
[60] Hunton (2011) (n 1).
[61] Porcedda and Wall (2019) (n 4).
[62] Hunton (2011) (n 1).
[63] Hutchins, Cloppert and Amin (2011) (n 21).
[64] Alice Hutchings, *Cambridge Computer Crime Database* (2020).
[65] Michael Turner, *Computer Misuse Act 1990 Cases, Computer Evidence* (2020).
[66] Eg.. lawpages.com and judiciary.uk. Lawpages.com was consulted early on in the process and the databases cited draw from materials included therein.
[67] Juliet Corbin and Anselm Strauss, 'Grounded Theory Research: Procedures, Canons, and Evaluative Criteria' [1990] 13 *Qualitative Sociology*, 9.
[68] Ibid.
[69] Ciarán Dunne, 'The Place of the Literature Review in Grounded Theory Research' [2010] 14 *International Journal of Social Research Methodology* 111.

Table 1 – Cascade steps and tipping points.[57]

Step	Cascade	Tipping point
1	Learning about a vulnerability/ creation thereof Software on sale to exploit vulnerability	Disseminating the knowledge
2	Exploiting the vulnerability Software bought to exploit vulnerability	Exploiting the vulnerability by multiple individuals
3	Valuable info obtained (dump)	Doxing or ransom + dox
4	Putting up data for sale	Information sold
5	Retaining information for (future) use	Data stuffing for resale
6	Attack is publicized	Pretexting or hoaxing
7	Monetisers	Use of money mules

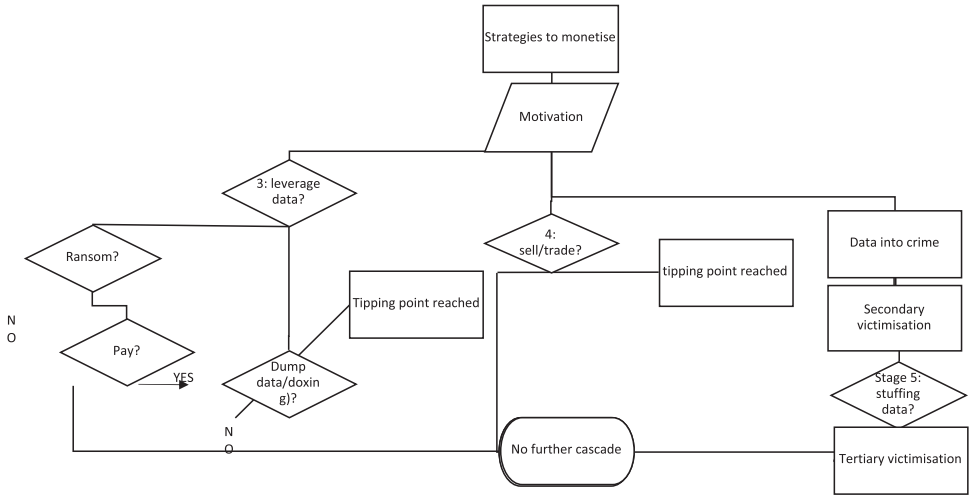

Fig. 2 – Steps 3 to 5 or the vicious cycle of monetisation of data[57].

typically, but not only, SaaS– where the cloud was either the main target or conduit of the cybercrime, and cases where the use of cloud computing could be inferred (e.g. because of the volume of data which suggests the existence of a platform to store and process vast data). The third attribute is the potential presence of cascade, assessed through the analysis of news reports; this was typically but not only identified based on the presence of 'big data', both at upstream and downstream level, that is cyber-dependent and cyber-enabled/assisted crime respectively. The three attributes allowed to narrow the search down to 34 'cybercrimes incidents' concerning 101 individuals,[70] which were further sampled on the basis of the fourth attribute: availability of sentencing remarks. The latter proved to be problematic, as discussed next.

3.1.1. *Obtaining sentencing remarks from English and Welsh courts*

Copies of sentencing remarks and other court materials which are not reported can only be obtained by applying for transcripts; this requires authorisation from the Court in which the sentence was passed. However, only sentencing remarks of courts that routinely record their trials or sentencing hearings can be requested. For courts which do not routinely record trials, such as Magistrates' Courts,[71] the only option is to request notes held by lawyers representing the parties or by the judge with a view to issuing the sentence.

Materials related to trials or sentencing hearings which were recorded are usually logged onto a system (Digital Audio Recording or DAR). Transcripts are provided by transcription companies for a fee determined by the duration of the sentencing hearing, and calculated on multiples of 71 words,[72] which are the standard units for sentencing remarks, as well as on the urgency of the file.

At the time of writing, sentencing remarks of English and Welsh Crown Courts are transcribed by six companies (previously four): Auscript, Epic Europe Ltd, Opus 2 International Ltd, Marten Walsh Cherer, the Transcription Agency and Ubiqus,[73] each having 'monopoly' over one geographical area of England

[70] Porcedda and Wall (2021) (fn 4).

[71] As described at: https://www.gov.uk/apply-transcript-court-tribunal-hearing (last accessed 16 October 2019).

[72] As the length of the hearing is typically not known upfront, this makes it difficult to anticipate the cost of data collection for a given research project.

[73] Ministry of Justice, 'Apply for a transcript of a court or tribunal hearing' <https://www.gov.uk/apply-transcript-court-tribunal-hearing> and the guidelines: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/807467/ex107-gn-eng.pdf (last accessed 18 May 2021).

and Wales. Sentencing remarks can only be requested from the company which has the 'monopoly' over a specific Crown Court. For instance, this means using the services of Ubiqus for Southwark Crown Court and Opus2 for Leeds Crown Court. Consequently, it is not possible to rely on a single transcription company to access court materials located in the different geographical areas. Sentencing remarks in Scotland are not transcribed[74] and consequently, the one case identified for this research had to be left out. Thus the analysis focusses on 33 instead of 34 cases decided in English and Welsh Courts, as opposed to the UK as a whole.

The application process is complicated by the fact that, in order to access the sentencing remarks, it is necessary to identify the name of the judge deciding the case and the case number, information which are respectively seldom and never available in media reports. Consequently, the relevant courts need to be approached twice. First, to obtain the name of the judge and case number and second, after having obtained a quote from the transcription company, to apply for permission to obtain the remarks. The process can take longer than six months and can be inconclusive: for this research it was possible to identify only 20 sentencing remarks related to 17 of the 34 cases initially selected, that is 50% of the sample.

I comment on the implications of this outcome in Section 4. Here I reflect upon the approach of courts to the sentencing of cases used to develop the cascade effect model.

3.2. *Sentencing remarks and criteria of analysis*

The purpose of this research is to critically reflect upon the approach of courts, and by extension the criminal justice system, to the evolution of cybercrime resulting from the uptake of cloud computing and evaluate the relevance of data crime and the cascade effect for the sentencing of cybercrimes. The findings are based on the analysis of 20 sentencing remarks of court proceedings in England & Wales relating to 17 of the 34 cases used to develop the cascade effect – as many sentencing remarks as could be accessed.

Table 2 illustrates the 17 cases. The first column lists the case number, the second the number of the case study with respect to the 34 cases used to develop the cascade effect, thereby enabling to compare the findings illustrated in this study to those contained in related studies.[75] The third column lists the case name and the last shows the presence of cascade as a dummy variable; n* and y* indicate that additional material, for instance pre-sentence reports, is needed to ascertain the absence or presence of cascade.

The sentencing remarks were coded according to two criteria. First, I looked at the presence of 'direct' references to data crime and the cascade effect, either as part of a discussion of the technological environment enabling the offence, or as direct references to cloud computing and big data. Second, I looked at the presence of 'indirect' references to the cascade effect through 'markers': these are the *reach* of cybercrimes as a marker for the cloud (in terms of the territorial reach and number of individuals impacted), *scale* or *volume* as a marker for big data, and the *relational import of the cyber offence* as a marker for the 'crime frenzy' typical of the cascade effect. These criteria serve a triple purpose. First, corroborating the findings with respect to the likely presence or absence of cascade effect. Secondly, assessing whether the presence of cascade effects had an impact on sentencing. Thirdly, pointing to how the cascade effect could facilitate sentencing or the broader criminal justice approach to cybercrimes.

To assess whether the presence (or absence) of cascade effect had an impact on sentencing, the analysis focusses on the criteria to determine the seriousness of the sentence, with particular reference to the level of harm, including mitigating and aggravating factors. The choice of criteria was in line with the Criminal Justice Act 2003 applicable at the time of the analysis. Seriousness and its subcomponents of harm, aggravating and mitigating factors are amongst the principles listed in the seriousness guidelines that give substance to the Criminal Justice Act 2003. The Sentencing Council guidelines were first adopted in 2004 and subsequently revised in July 2019,[76] a year before the adoption of the Sentencing Act 2020.[77] These generic principles provide criteria for sentencing in the absence of an offence-specific guideline, as is the case for the CMA 1990, the primary instrument for cyber-dependent crime.

The guidelines recommend reaching, first and foremost, a provisional sentence based on the combined assessment of the seriousness of the offence and the purpose of the sentencing. The seriousness depends on culpability and harm; the two versions of the guidelines diverge in the degree of detail followed to interpret the law. In the 2019 Guidelines culpability depends on the role, level of intention and/or premeditation and the extent and sophistication of planning. The 2019 Guidelines describe harm as being actual, intended or potential and to primary or secondary victims, who can be the public at large. There are five purposes of sentencing stated in S 142 of the Criminal Justice Act 2003, as amended by S 57 of the Sentencing Act 2020: punishing offenders; reducing crime, including by deterrence; reforming and rehabilitating offenders; protecting the public; and the making of reparation by offenders to persons affected by their offences.

This work appraises how the cascade effect influences the assessment of a subset of the components of seriousness, namely harm, mitigating factors and aggravating factors. Such a choice does not ignore that the determination of seriousness is a composite process and includes the determination of culpability, however, culpability is only looked at in passing in these pages because the model does not address motivation at this point in time (although may do so in the future[78]).

[74] Based on private conversation with a representative of the Scottish Sentencing Council in July 2019.

[75] Chiefly Porcedda and Wall (2021) (n 4).

[76] Sentencing Council, *Overarching Principles: Seriousness. Guideline* (2004); Sentencing Council, *General Guideline, Overarching Principles* (2019).

[77] The new principles became effective in October 2019 and, as a result, cannot constitute a benchmark to assess the correctness of any sentence analysed in this paper, nor is this the desired outcome of this research. The same applies to the reforms contained in the Sentencing Act 2020.

[78] That the overall assessment of seriousness is a composite process means that it may well be influenced by the selection of the purposes of sentencing. One element brought to surface by the analysis of sentencing remarks is the potential interference between the conceptualization of culpability of young offenders

Table 2 – Sentencing remarks and presence of cascade.

N.	Case Study	Case Name	Cascade (dummy)
1	(1)	R v Mennim, R v Pearson	Y
2	(4)	R v Hallam, R v Benson	Y
3	(6)	R v Akinwolemiwa	N
3	(6A)	R v Ogbogbor	N
4	(10)	R v Markuta	Y
5	(11)	R v Beddoes, Randhawa and Sangha	N*
6	(13)	R v Hussain	Y
7	(15)	R v Jeffery	N*
8	(16)	R v Davis, R v Al-Bassam, R v Ackroyd, R v Cleary	Y
9	(17)	R v Martin (appeal)	Y*
10	(18)	R v Simkus, R v Kurach	N*
11	(19)	R v Skowron,	N*
11	(19A)	R v Ptach	N*
12	(24)	R v Oshodi and Anor, Jabeth and Hamid, R v Butt, R v Okala, R v Eve,	Y
13	(32)	R v Turner, Mcdonagh; Drage; Coombes	Y
14	(30)	R v Kostromina, R v Milka, R Prakochyk	N*
15	(CT)	R v Allsopp (appeal)	Y
15	(CT)	R v Kelley	Y
16	(31)	R v West	Y
17	(33)	R v Ojo and Agbaje	N*

4. UK courts, data crime and the cascade effect

Here I discuss, first, whether judgments mention the cascade effect either directly or indirectly, by means of the following indirect 'markers': the *reach* of cybercrimes as a marker for the cloud, *scale* or *volume* as a marker for big data, and the *relational import of the cyber offence* as a marker for the 'crime frenzy' typical of the cascade effect. Secondly, I look at the link between the presence or absence of cascade effect and the sentence adopted by judges. I discuss proposals for how the cascade effect could support sentencing in Section 5.

4.1. *Direct and indirect reference to the cascade effect in sentencing remarks*

The sentencing remarks analysed in this research do not contain any *direct* mentions of 'cloud computing' and 'big data'. Specific technological applications are typically mentioned when such applications are relevant to the facts of the case. For instance, one sentencing remark mentioned Skype and Yahoo, two SaaS applications used to commit the cybercrimes the defendant was being sentenced for.

In some cases the judge sums up how technology was involved in the *iter criminis*; however, there is no standard practice for describing technology. For example, in one case the judge touched on the subject briefly: You succeeded in hacking into the personal account of [victim] which contained about 150 names of her friends, her contacts, her associates with addresses and telephone numbers, some or all of this you then posted on the internet …thereafter she received abusive emails and phone calls from abroad".[79]

In another case, the judge delves into more details "…A principal piece of software, or malware, used to achieve these ends was a so-called Trojan computer virus, known as Zeus. When injected into the target computer network, Zeus operates by logging keystrokes and form grabbing. It is therefore highly efficient in stealing banking information. It is also used to steal usernames and passwords […] when logging in to their bank account through websites."[80]

In sum, the sentencing remarks rarely directly refer to the technological environment enabling the cascade effect and data crime.[81] A useful prism to make sense of such an absence is the regulatory technique of technology neutrality. Accordingly, lawmakers specify neither the technological environment in which cyber offences take place, nor the tools enabling such offences, such as 'cloud computing', and they also avoid buzzwords, such as 'big data'. Such vagueness inevitably impacts the ability of courts to engage in a discussion of the

who misused computers and the purposes of sentencing of such cyber offenders, especially when they are no longer minors (see Section 5.2). The cascade could also assist in the assessment of culpability, as discussed in the conclusions.

[79] His Honour Judge Loraine-Smith in *R v Hussain* (Southwark Crown Court).

[80] His Honour Judge Price KC in *R v Beddoes* (Kingston-upon-Thames Crown Court), § 21.

[81] Ie 'directly' referring to data crime and the cascade effect, either as part of a discussion of the technological environment enabling the offence, or as direct references to cloud computing and big data.

technology surrounding a specific case,[82] which for Chandler fosters a generalised acceptance of the technology.[83]

Conversely, the sentencing remarks analysed in this research contain indirect references or 'markers', depending on whether a case displayed presence or absence of the cascade effect.

In cases featuring potential cascade (Y*),[84] courts seem to devote less time to discussing the underlying technology. Sometimes the sentencing remarks point to the fact that offenders were in possession of illegally acquired data, for which however they were not charged, indicted and consequently not sentenced.

In the sentencing remarks concerning cases that display cascade effects (Y), references to the *reach, scale* or *volume and relational import of a cyber offence* are respectively interpreted as a marker for cloud computing, big data and the 'crime frenzy' typical of the cascade effect.

Reach is understood as the physical decoupling and platformisation enabled by cloud computing and the related increased user base. Since the cloud informs both applications and infrastructure, it is often difficult to distinguish between the reach effected by the cloud and that achieved by the Internet in general. For instance, an indirect reference of reach can be found in Judge Gledhill KC's sentence in R v West, whereby ""When members of the public decide to become customers of companies such as Just Eat, Sainsbury's, Argos, Ladbrokes, Uber, Asda and other organisations named in this indictment, they regularly have to provide (…) sensitive personal details". Just Eat, Uber and Ladbrokes have either vastly increased their user base thanks to cloud computing or are cloud native.[85] Reach is a weak marker, in that it relies on inferences based on prior knowledge or on further research.

Examples of scale/volume are "your skills were used to gain access to a staggering volume of personal details – *8.1 million people*"[86] and "throughout 2011 you were engaged in an extensive campaign, hacking Sony online entertainment, harvesting details of *some 26.4 million customers*".[87]

The following quote points to the relational aspect of the cascade: "The offending was sophisticated. It involved the acquisition of information about stolen credit card data, by *your joining and being trusted as a member of the in-fraud chatroom*, by your *requiring of that information from people outside of this jurisdiction*, to whom you paid money for that information".[88]

Quotes showing overlapping scale/volume and relational markers are:

"The forum was a meeting place for people interested in computer hacking and the use of hacked data for fraud. For instance, *Yahoo's computer was hacked* by a forum user and the *data* of 450,000 people *was published on the Internet*"…You alone were responsible for setting up the website; through it, *you encouraged others* to involve themselves in crime. Many people's data was affected."[89]

> *"This fraud could not have been perpetrated without you hacking into masses of accounts from Egypt, to this country, and selling on personal bank details, and details of peoples' ID's, for commissions for percentages of amounts in their accounts. This… crime [was] compromising untold numbers of victims' accounts"*.[90]

In R v Mennim and Pearson, Recorder Mulligan said: *it enabled you to access highly confidential information and to, and this is very significant in my view, expose"…"many, many, many, many individuals to the risk of attack by fraudsters." "The use to which that information could have been put, it is hard really to imagine"…."I accept it is a fair point that it may well be that others had access to that same information and it is not a perfect science really, calculating in this case the potential loss and the potential for harm"*.

As for cases with unlikely cascade (N*), i.e. where there may have been cascade but information is insufficient to confirm it happened, the occasional references to cascade markers are not accompanied by a discussion of the related reach, scale or relational element of the crime. This could possibly signify the absence of cascade and the consequent lack of analysis of the import of big data for reaching a sentence. However, a different interpretation is that it might be worthwhile to investigate either the origin of the data used by offenders to pursue their cybercrimes, or which they were in possession of for the offending.

4.2. *Relevance of the cascade effect in sentencing remarks*

Does the presence or absence of 'cascade' affect sentencing? Where present, are cascade markers used to arrive at the sentence? I set to answer these questions by understanding if the presence of cascade markers affects the assessment of seriousness, that is harm, aggravating and mitigating factors. To answer the question, it is necessary to take into account the authorities used in making the assessment.[91] The first authority is sentencing guidelines, including those for analogous offences, in the absence of guidelines specific to the offence at hand. The second is *stare decisis*, which, in the case of cybercrime, typically means sentencing judgments of the

[82] See especially: Chandler (2007) (n 42); Grabowski (2008) (n 43); Greenberg (2016) (n 36); Lilian Edwards, 'Dawn of the Death of Distributed Denial of Service: How to Kill Zombies' 24 *Cardozo Arts and Entertainment Law Journal* 23 in relation to R v Caffrey cited in Urquhart (2018) (n 11); Porcedda (2023) (n 38).

[83] Chandler (2007) (n 42), 8. It is beyond the scope of this paper to investigate whether technology neutrality is the cause or the symptom of such a technological acceptance.

[84] Where for instance it cannot be excluded that offenders purchased or otherwise obtained the data necessary for their offending through the monetization cycle (steps 3-5 of the cascade effect).

[85] See for instance: https://cloud.google.com/customers/just-eat; https://medium.com/@webmaster_86047/how-uber-airbnb-made-billions-through-cloud-computing-b98ba108a7fc; https://www.scc.com/testimonials/entertainment-retail/ladbrokes/.

[86] Mr Recorder A Mulligan in *R v Mennim, R v Pearson* (Southwark Crown Court), emphasis mine.

[87] His Honour Judge Taylor in *R v Davis, R v Al-Bassam, R v Ackroyd, R v Cleary, R v Jeffery* (Southwark Crown Court), emphasis mine.

[88] His Honour Judge McReath in *R v Hallam, R v Benson* (Southwark Crown Court), emphasis mine.

[89] Mr Recorder Lavander KC in *R v Markuta* (Southwark Crown Court), emphasis mine.

[90] His Honour Judge Robbins in *R v Oshodi, Jabeth, Hamid, Butt, Okala and Eve* (Southwark Crown Court).

[91] These are the legal authorities applicable at the time; all cases were decided before the adoption of the 2019 Sentencing Guidelines and Sentencing Act 2020.

Court of Appeal and sentencing guidelines for analogous offences, in the absence of guidelines specific to the offence at hand. In other words, sentencing, and the role of cascade towards sentencing, depends on the instruments chosen to charge an offender with a crime, as well as the existence of authorities drawn from hierarchically higher courts; I discuss each in sequence. The last section addresses how hierarchically lower courts, which deal with the majority of cybercrime cases, make use of these two authorities in the case studies reviewed in this research, and the impact of the observed cascade effect on sentencing.

4.2.1. *The role of authorities*

4.2.1.1. Sentencing guidelines: the law chosen to indict The question of which instrument is chosen to indict an offender is very relevant when it comes to cybercrime, as there often is more than one instrument under which an alleged criminal conduct can be prosecuted. The CMA 1990 has notably resulted in few prosecutions, and cybercrime cases are often prosecuted as frauds;[92] Gillespie notes the CMA 1990 "may not be used where alternative legislation exists".[93] Sections 3A of the CMA 1990, 6 and 7 of the Fraud Act 2006 and s.170 of the DPA 2018 (s.55 of the DPA1998) display overlaps. The offences corresponding to S.170 in the old DPA 1998 were theoretically punishable with a maximum custodial sentence of two years pursuant to s.77 and s.78 of the Criminal Justice and Immigration Act. In practice, however, the implementing acts were never adopted, "despite repeated lobbying by the ICO".[94]

As an aside, the fact that the CMA1990 is seldom relied on begs the question as to whether the choice of instrument to indict is tied to the type of punishment that the criminal justice system desires to inflict.[95] Answering this question would seem to be particularly pressing for young offenders: the average age of those arrested for cyber-dependent crimes is below 18.[96] Whichever the approach chosen,[97] the instrument relied upon for a given count affects the interpretation of seriousness, because each instrument is governed by different authorities.

4.2.1.2. Court of Appeal sentencing judgments as authority and the cascade effect The Court of Appeal has pronounced itself on cases of cybercrime. Here I analyse Appeal sentences relied upon in the cases selected for this study: *R v Mangham* (2012), *R v Mudd* (2017) and *R v Martin* (2013); the latter is also one of the 34 case studies originally selected for this work, alongside *R v Allsopp*.

Appeal cases display an appreciation of the reach, scale and relationality of contemporary cybercrimes, and the damage they carry, which are considered in this work as markers of the cascade effect. *In R v Martin*, Leveson LJ held the view that "the prevalence of computer crime, its potential to cause enormous damage, both to the credibility of IT systems and the way in which our society now operates, and the apparent ease with which hackers, from the confines of their own homes, can damage important public institutions, not to say individuals, cannot be understated".[98] Likewise, in *R v Mudd*, Gross LJ quoted Judge Topolski KC's words "Offending of this kind … has the potential to cause great and lasting damage, not only to those directly targeted but also to the public at large. It is now impossible to imagine a world without the internet. There is no part of life that is not touched by it in some way".[99] The Court further added that it is of the "first importance that courts send a clear message: illegal activities of this nature on this scale are not a game; they will be taken very seriously by the courts".[100]

Not only do these authorities, which are often quoted in the cases analysed in this article, attach high seriousness to cybercrime in light of its ease and prevalence, but also, the assessment of seriousness is entangled with the objective of punishment. In *R v Martin*, Leveson LJ said "The fact that organizations are compelled to spend substantial sums combating this type of crime, whether committed for gain or out of bravado, and the potential impact on individuals such as those affected in this case only underlines the need for a deterrent sentence".[101] Elsewhere, Lord Justice Leveson felt it to be "of the first importance that … illegal activities of this nature … will be … punished accordingly", which "can only be by way of immediate custody".[102]

The case law is, however, not settled with respect to the assessment of seriousness; this is where the cascade effect could prove particularly useful (see Section 5). As there are no guidelines specific to cybercrime, there does not exist a binding list of mitigating or aggravating circumstances. In two cases the court listed aggravating features that, it is argued here, are markers of the cascade effect: first, *the size of user databases and large number of attacks*,[103] which relates to volume; second, attempts to *reap financial benefit by the sale of information* which has been accessed, and third, *whether information*

[92] MacEwan (2008) (n 32); Wall (2017) (n 11); McKay et al. (2020) (n 6).
[93] Gillespie (2019) (n 8), 18.
[94] Out-law, *ICO prosecutes under Computer Misuse Act* (2018).
[95] Gillespie (2019) (n 8) states that the limited reliance on the CMA 1990 perhaps reflects "the need for the [CPS] to consider what the most appropriate charges are, including reflecting on what would give the sentencing judge the most suitable powers of disposal in the event of a conviction", p 18. See also T Newburn, *Criminology (third edition)* (Routledge 2017); P Carter, *Correctional Services Review* (2003). Should the objective pursued be to maximise the punishment of offenders, then the CPS would be more inclined to rely on instruments punishing a certain conduct with the highest maximum sentence. Such a position would be consistent with the fact that both the rate of incarceration and the sentence severity has increased in the past decade. This could also help to explain the reliance on the Fraud Act 2006 as opposed to the CMA 1990; computer misuse was added to Annex 1 of the Serious Crimes Act 2007 only in 2015, when the CMA itself was amended to add new offences and provide for higher penalties. However, according to the authors of the CLRNN report, the two Acts attract similar penalties: McKay (2020) (fn 9), 20.
[96] National Crime Agency, *Pathways into Cybercrime, Intelligence Assessment* (2017).
[97] Justice Committee House of Commons, *The Crown Prosecution Service: Gatekeeper of the Criminal Justice System* (2009).
[98] *R v Martin* EWCA Crim 1240 para 43.
[99] *R v Mudd* [2017] EWCA Crim 1395 para 35.
[100] Ibid para 50.
[101] *R v Martin* para 42.
[102] *R v Mudd* para 50.
[103] Ibid, para 28.

is *passed onto others*,[104] both of which relate to the relational element of the cascade.

The cascade effect intends to conceptualise the importance of actual versus potential damage, a point featured in *R v Mangham*, where the Court granted leave to appeal and reduced the length of the sentence because, as Cranston LJ KC said, "the information hacked had not been passed on to anyone and … there was no financial gain involved. The judge was correct, in our view, to identify the damage … but it may be that he gave too much emphasis to the potential damage".[105] In the language of the cascade effect, the appellant had reached a stage but not gone beyond the tipping point, thereby causing less harm than he could have otherwise caused. The approach in *Mangham* was criticised in the appeal to *R v Martin*, where the Court noted that "it is of little moment to the victims of such crimes that the offender may be motivated by bravado within a community of like-minded souls, rather than by financial gain. The capacity for harm is very great either way. Actual damage or financial benefit would substantially aggravate an offence".[106] I now turn to discuss the weight of these authorities on sentences pronounced by Magistrates' and Crown Courts in the cases under analysis and the relevance of the cascade effect therein.

4.2.2. *Magistrates' and Crown Court sentencing remarks and relevance of the cascade effect*

Table 3 captures the link between the relevance of cascade in the case studies and in the sentencing remarks. There, under 'sentencing remarks',Y/N indicate whether the court relied on cascade markers to arrive at the sentence (Y) or not (N).

Among cases featuring cascade (Y), cascade markers were relevant for the assessment of seriousness (harm, aggravating and mitigating circumstances) in at least six instances (*R v Mennim and Pearson; R v Hallam and Benson; R v Markuta; R v Hussain; R v Oshodi* et al.*; and R v Turner* et al.). There are two cases featuring cascade where cascade markers partially contributed to arriving at the sentence (*R v Davis* et al.*; R v West*). In three cases displaying cascade effects, *R v Martin, R v Allsopp and R v Kelley*, sentencing does not draw on cascade markers. What is striking is that authorities, whether sentencing judgments of the Court of Appeal or sentencing guidelines, do not seem to be influential vis-à-vis the cases sampled for this research. Even when data crime and cascade markers are present, they do not necessarily inform the courts' assessment.

Among cases with potential or no cascade (Y*, N*, N), irrespective of whether cascade markers are mentioned, data crime or cascade markers do not inform the assessment of seriousness. The one exception is *R v Jeffrey*, where the cascade did not happen as the doxed data was cancelled before anyone could access it. This outcome may be due to the fact that there is no settled authority on cybercrimes in general and the CMA1990 in particular. The role of the specific instrument under analysis does not seem to make a difference either.[107]

5. Discussion: merits of the cascade model, unexpected findings and limitations

I begin the section by discussing how the cascade model could support sentencing and the criminal justice system at large. The difficulty of researching cybercrime sentencing not only highlights limitations for this research, but also yields self-standing findings and policy recommendations.

5.1. *Merits of the cascade model for the criminal justice system*

This works aims to assess whether the cascade effect can be useful to assist the sentencing of cybercrime, and related criminal justice aims. The sentencing remarks of cases featuring cascade display the presence of cascade markers almost across the board, but the importance of those markers in the determination of seriousness varies. Importantly, cascade markers are not relied upon in the assessment of seriousness for the defendants arrested in relation to the TalkTalk 2015 data breach that informed the conceptualisation of the cascade effect within this research.[108] For what concerns sentencing remarks of cases with potential or no cascade, presence of cascade markers is haphazard and irrelevant for the determination of seriousness of the offence, with the exception of *R v Jeffrey*.

Far from invalidating the cascade effect,[109] these findings help show the cascade effect's relevance for the criminal justice system as, it is argued, the disconnect between the cascade and sentencing originates from the lack of guidance and from the nature of settled authorities. The concepts of cascade effect and data crime could help in the determination of seriousness as follows. Each step of the cascade effect could assist in the determination of harm. First, a case concerning, say, step 1 would be in the realm of potential damage and should attract a lower penalty; conversely, a case in steps 3 to 5 would have caused actual damage, thereby attracting a higher penalty (subject to mitigating circumstances, as discussed above). Secondly, since the cascade effect helps conceptualising tiers of victimhood,[110] the cascade could help to determine victimhood and contribute to the understanding of harm. Furthermore, reaching a tipping point could constitute an aggravating factor or, conversely, not reaching it could be a mitigating factor. An illustration of this is in Fig. 3, which shows step 3 of the cascade, whereby the offender has breached the security of a system and obtained informa-

[104] *R v Mangham* EWCA Crim 297, para 19.
[105] Ibid para 23.
[106] *R v Martin*, para 37. The court's stance has been rightly criticized by the authors of the CLRNN report, because it makes previous sentencing "useful only as minimum benchmarks" McKay et al (2002) (fn 9), 127.
[107] Differences in the length of sentence have not been taken into account, as this would require the identification of comparable cases.
[108] Porcedda and Wall (2019) (n 4).
[109] And bearing in mind the fact that this analysis is based on a sample: a different sample of cases may offer different insight.
[110] Porcedda and Wall (2021) (n 4).

Table 3 – Sentencing remarks and decision based on cascade.

N.	Case Name	Cascade	Sentencing Remarks
1	R v Mennim, R v Pearson	Y	Y
2	R v Hallam, R v Benson	Y	Y
3	R v Akinwolemiwa	N	N
3	R v Ogbogbor	N	N
4	R v Markuta	Y	Y
5	R v Beddoes, Randhawa and Sangha	N*	N
6	R v Hussain	Y	Y
7	R v Jeffery	N*	Y
8	R v Davis, R v Al-Bassam, R v Ackroyd, R v Cleary	Y	Y*
9	R v Martin (appeal)	Y*	N
10	R v Simkus, R v Kurach	N*	N
11	R v Skowron	N*	N
11	R v Ptach	N*	N
12	R v Oshodi and Anor, Jabeth and Hamid, R v Butt, R v Okala, R v Eve	Y	Y
13	R v Turner, Mcdonagh; Drage Coombes	Y	Y
14	R v Kostromina, R v Milka, R Prakochyk	N*	N
15	R v Allsopp (appeal)	Y	
15	R v Kelley	Y	N
16	R v West	Y	N
17	R v Ojo and Agbaje	N*	Y*

tion of value, which he or she may capitalise in a variety of ways.[111]

There are at least two complementary ways in which the criminal justice system could benefit from the cascade model and its various elements. The first is to appreciate the complexity of the conduct, so as to take into account all legal instruments of relevance to that conduct. This includes data protection legislation, which was never relied upon in the proceedings discussed here, even where personal data was compromised and misused, with obvious consequences for data subjects.[112] Data protection legislation is relevant to the fight against cybercrime in light of its overlaps with information security, its emphasis on prevention[113] and its creation of compensation for the harm suffered by victims. Remedies are a way of protecting the public, which is an objective of sentencing often cited in judgments, but not as prominently pursued in practice as deterrence. Judge Gledhill KC summarised this aptly in the opening passages of the remarks sentencing West (aka *Curvoisier*):

> "When members of the public decide to become customers of companies (…) and other organisations named in this indictment, they regularly have to provide personal details (…) Such customers rightly expect that their highly sensitive details will remain private and confidential. The companies themselves are only too well aware of the need for security, and take every precaution to ensure that no unauthorised person has access to that material, let alone is able to misuse it. Regrettably, as this case has demonstrated, security of information held electronically, is at best, poor. (…) This case should be a wake-up call to customers, companies and the computer industry, to the very real threat of what is now known as cybercrime, and cybercrime as this court well knows, is on the increase".

The second way in which the criminal justice system could benefit from the cascade model is to use the cascade to formulate aggravating and mitigating circumstances, potentially as part of updated guidelines for s.6 and s.7 of the Fraud Act 2006 and brand new guidelines for the CMA 1990; CMA-specific guidelines are also recommended by the CLRNN.[114] Three such aggravating circumstances found by authorities I mentioned above are "*the size of user databases and large number of attacks*",[115] "attempts to *reap financial benefit by the sale of information* which has been accessed", and "*whether information*

[111] © [2021] IEEE. Reprinted, with permission, from Porcedda and Wall (2021) (fn 4). Ways of capitalising the offence include those discussed in Hunton (2011) (n 1).

[112] For the cases cited here, the relevant instrument was the Data Protection Act 1998. See a discussion of the limits of the DPA 1998 in Porcedda and Wall (2019) (n 4); McKay et al (2020) (n 6), 108.

[113] Maria Grazia Porcedda, 'Brexit, Cybercrime and Cyber Security. From en Masse Opt-out to Creative Opt-in in the AFSJ and Beyond?' in Helena Carrapico, Antonia Niehuss and Chloe Berthelemy (eds), *Brexit and Internal Security. Political and Legal Concerns in the Context of the Future UK-EU Relationship* (Palgrave Macmillan 2019); Porcedda and Wall (2019) (n 4). See Porcedda (2023) (n 38), ch 5.

[114] McKay et al. (2020) (n 6), 128.

[115] *R v Mudd* para 28.

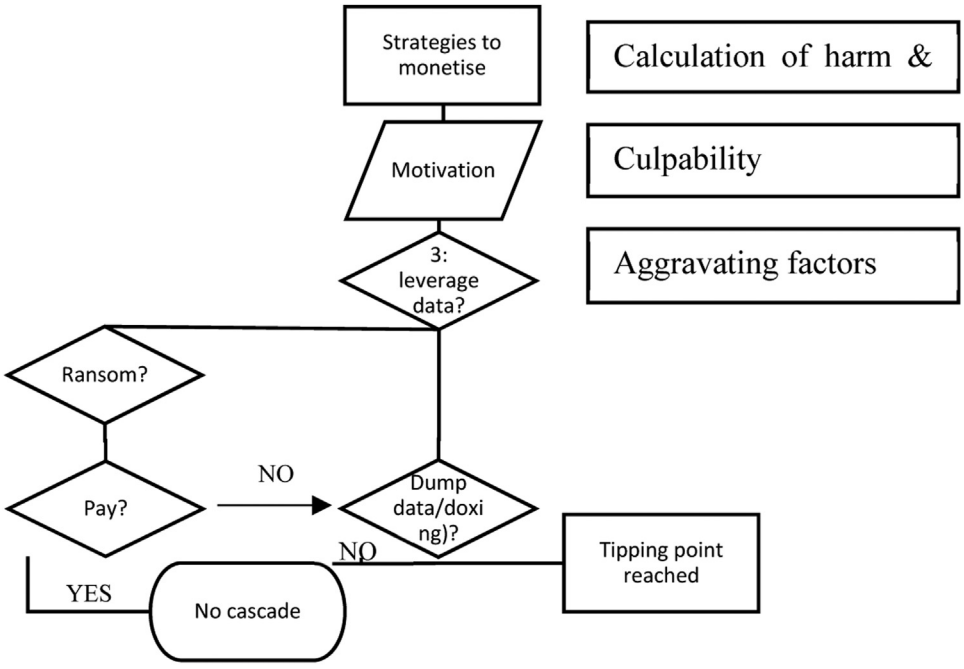

Fig. 3 – Use of the cascade effect for the determination of seriousness of a cybercrime.

is passed onto others".[116] Another factor mentioned in *Mangham* is "the nature of the damage caused to the system itself and to the wider public interest such as national security, individual privacy, public confidence and commercial confidentiality".[117] Factors such as the scale of offending and the gross intrusion into the private lives of individuals can also be found in R v Gamble, which was not relied on in this research (see below).[118] Where the offender goes on to exploit a vulnerability and triggers a cascade effect, attempts to inform the owners of a system vulnerable to exploits could point to lower culpability or act as a mitigating factor.

As for cases featuring potential cascade, the question is whether it is worthwhile to investigate either the origin of the data used by offenders to pursue their cybercrimes, or the data they were in possession of. This is something that could be done in cooperation with relevant organisations, e.g. the relevant law enforcement branch together with the Information Commissioner's Office.

5.2. *Limitations, additional contribution and related recommendations*

5.2.1. *Limitations*

Limitations stem both from the research design and the inherent difficulty of researching the courts' approach to cybercrime. One limitation concerns the use of sentencing remarks, whose narrative can become all-encompassing only together with additional material, such as pre-sentence reports.

Another source of limitation is that each attribute of the purposive sampling carries the risk of selection bias. Firstly, relying solely on 'finalised' cases, to use the language in Hutchings' database, creates a selection bias and the findings risk being dated. The sentencing remarks analysed here mostly predate 2019 because of delays in the courts in sentencing cases. Complex cases can take even longer; by means of example Mr Kelley, one of the individuals arrested in November 2015 for the TalkTalk data breach,[119] was only sentenced in June 2019. At the time when the cases for further analysis were being identified, a range of cases were still ongoing. Not only are the findings backward-looking, but they also risk obsolescence, because the technology, the legal framework or policy may become outdated. Moreover, relying on online media reports carries the risk of information disappearing from the public domain; in Hutchings' database, a portion of cases could not be further investigated for this reason.

Secondly, focusing on cases that have a cloud dimension, which is the object of the broader research within which this study was conducted, may have resulted in underemphasising relevant technological or societal factors.[120] What is more, at times it was difficult to ascertain the presence of cloud computing with certainty; the cloud has become, to cite Chandler, "part of the cultural wallpaper"[121].

[116] *R v Mangham* para 19. These authorities have anyway limits, as identified in Mckay et al. (2020) (n 6), 126.
[117] *R v Mangham* para 19.
[118] R v Gamble (Leicester Crown Court, sentencing at Criminal Court), see <https://www.judiciary.uk/wp-content/uploads/2018/04/r-v-gamble-sentencing.pdf>.
[119] Porcedda and Wall (2019) (n 4).
[120] Among these, the anonymous reviewers cite encryption and the dark web.
[121] Chandler (2007) (n 42), 8.

Thirdly, news reports' focus on matters that 'interest the public'[122] means that important features of reported cases may have been left out or misreported. This, in turn, could have misled the identification of cascade potential, causing either oversampling or down sampling. For instance, a relevant case not included in this research was that of R v Gamble, the founder of the group Cracka with an Attitude.[123]

Finally, it was only possible to obtain less than half of the sentencing remarks for a host of reasons I discuss above (Section 3) and elsewhere,[124] and the remarks found were not always those relating to the main proceeding. A broader sample of cases could lead to stronger or even altogether different findings.

5.2.2. *Findings beyond the cascade effect: technology neutrality, young offenders and open justice*

The limitations just discussed stem from problems to do with researching cybercrime with data and interestingly open up the road to self-standing policy recommendations. First, the difficulty of identifying the relevance of a given technological application, such as the cloud, for a specific case questions the role of technology neutrality in law and court practice (Section 2.1). A conclusive analysis warrants further research; for instance, it may be that technology neutral legislation would work well in tandem with specialised courts on cybercrime, akin to what Southwark Crown Court is for fraud, but it will be for future work to discuss this point.

Secondly, the time lag between arrest and sentencing is a known issue, for instance, with respect to the length of remand, which has particularly serious consequences for young offenders.[125] This is also a relevant issue with respect to sentencing itself, as the rules that apply to sentencing depend on age at the time of the finding of guilt, rather than of arrest. A number of the cases under analysis involve the sentencing of young adults who were minor at the time of offending and when they were arrested, but who were considered adult when found or pleaded guilty. The Sentencing Children and Young People Guidelines[126] clarify that the purposes of youth justice should be to prevent the offending and that the approach to sentencing should be focussed on the individual rather than the offence.[127] As a result, custodial sentences should only be measures of last resort. Pursuant to s. 142A of the Criminal Justice Act, which had not been brought into effect when this research was conducted,[128] youth justice should not pursue the reduction of crime, including its reduction by deterrence.[129] A careful consideration of the need to protect young offenders while achieving a deterrent effect can be found in Haddon-Cave J's reasoning in R v Gamble.[130] At the time of writing, the Sentencing Act 2020 appeared set to solve this issue.[131]

However, cybercrime is now seen as serious crime to be deterred and for which young offenders should be punished. Courts disagree as to the appraisal of seriousness, particularly potential harm and what constitutes aggravating and mitigating circumstances. Lack of financial gain, lack of understanding of the consequences of one's actions and immaturity seem to be common features among young cyber offenders, who apparently drift from gaming into cybercrime out of intellectual curiosity.[132] Neurodiversity is another recurring factor among young offenders charged with cybercrimes.[133] While these features would normally be seen as mitigating circumstances,[134] there is no agreement as to their role for cybercrime. Some Courts, particularly in the Appeal cases, seemingly overlook these features, as well as the 'gaming' and 'intellectual challenge' motives, because of the harm caused by the specific cyber offence.

In essence, this raises an important question: how should the criminal justice system respond to young cyber offenders with a profile that includes elements which, under different circumstances, would be seen as mitigating features? Other areas of youth justice may hold the answer to this question; this paper contributes towards raising the importance of investigating the fairness of sentencing (section 2.3), but answering the question is beyond this research. However, answering the question may inform proposals to either amend the law, or make specific provisions in existing guidelines, or else draw up new guidelines, alongside existing Prevent strategies.[135]

Thirdly, the unreported nature of cybercrimes, compounded with the difficulty of obtaining court materials, explains why media reports are often the only resource available for investigations that look into the narrative of cyber-

---

[122] Rebecca Moosavian, 'Deconstructing 'Public Interest' in the Article 8 vs Article 10 Balancing Exercise' [2015] 6 *Journal of Media Law* 234.

[123] Iam grateful to one anonymous reviewer for bringing this to my attention.

[124] Dhami and Belton (2014) (n 28). Maria Grazia Porcedda, 'The Strange Case of Researching Cybercrime with Sentencing Remarks' (2nd Methods and Data in Sentencing Research: Quantitative and Qualitative Approaches Conference).

[125] Newburn (2017) (n 97).

[126] Sentencing Council, *Sentencing Children and Young People Guidelines* (2017).

[127] Ibid § 1.2

[128] The different treatment of young offenders should follow, in any case, from the ratification of the United Nations Convention on the Rights of the Child (General Assembly, 1989) by the UK, and in particular Art. 37 and particularly " (b) (…) The arrest, detention or imprisonment of a child shall be in conformity with the law and shall be used only as a measure of last resort and for the shortest appropriate period of time" (https://www.ohchr.org/en/professionalinterest/pages/crc.aspx). I am indebted to Dr Eszter Parkanyi for this point.

[129] Sentencing Council (2017) (n 128) § 1.10.

[130] See especially §71, 74 and 90.

[131] Sentencing Council, 'Sentencing Code' (2020) <https://www.sentencingcouncil.org.uk/sentencing-and-the-council/sentencing-code/>

[132] Andrew Goldsmiths and David S. Wall, 'The seductions of cybercrime: Adolescence and the thrills of digital transgression' [2019] 19(1) *European Journal of Criminology*; National Crime Agency (2017) (n 98).

[133] Cooper (fn 25), part 7; McKay et al (2020) (6); see also R v Gamble.

[134] Sentencing Council, *General Guideline, Overarching Principles*.

[135] National Crime Agency, *Cyber crime: Preventing Young People from Getting Involved* (2019). Committee on the Rights of the Child, *General Comment No. 25 on Children's Rights in Relation to the Digital Environment* (2021). I am indebted to Dr Eszter Parkanyi for this point.

crimes.[136] The fact, however, that cybercrime cases may either be misreported or disappear from the reach of the public domain, and therefore research, because they are only reported by newspapers and the relevant URLs become either obsolete or broken, impacts both on the rule of law and open justice. This state of affairs has such far-reaching consequences that a separate article is warranted, however it points to the need to discuss the standards of reporting of court proceedings,[137] as well as a platform for accessing such materials beyond quantitative-led endeavours such as the CREST database,[138] which is not, in any way, easy to access.

6. Conclusions: recommendations and further research

The nature of cybercrime constantly adapts to its enablers; cloud computing and big data are giving prominence to data crime – a variety of cybercrime powered by the availability of data, especially of a personal nature– which has the ability to cascade downstream. The cascade model is comprised of at least 6 steps, each featuring a tipping point which, if reached, enables the offending to progress to the next stage and trigger a crime frenzy. Further, the cascade effect acts both vertically *and* horizontally: each stage unleashes possibilities for actors unconnected to the primary offender, thereby enabling a web of distributed cybercrimes. The model is complementary to conceptualisations produced, for instance, by Hutchins et al. and Hunton.

The question addressed by this paper is how courts grapple with such changes and whether the cascade effect could assist the courts in passing equitable judgments. The paper looks into sentencing remarks of 17 cases decided in England and Wales between 2012 and 2019. The sample, drawn from an initial selection of 34 cases and determined by the availability of court data, includes cases with varying degree of cascade: Y (cascade), Y* (likely cascade), N* (unlikely cascade) and N (no cascade). The analysis looked at the presence of explicit markers of the cascade effect– references to cloud computing and big data, also as part of the analysis of technology – as well as implicit ones – the reach, volume and relational elements of an offence typical of the cascade effect. The analysis unveils the presence of markers of cascade effect in cases featuring cascade and potential for cascade (both Y and Y*), which suggests that Courts appreciate the impact of data crime and their cascading effects. However, sentencing remarks typically refer to markers of the cascade effect in an implicit manner, unless a specific cloud application was used, or targeted, by the offender. This is in keeping with the broad and technology neutral nature of cybercrime legislation, and buttresses works by authors such as Chandler, Grabowski and Greenberg, who stress the detrimental impact such legislation has on the work of courts, works to which I have added elsewhere.[139]

The analysis then focussed on whether the implicit cascade markers are used to appraise the seriousness of the offence and help reach the sentence. The analysis shows that the impact of data crime and its cascading effects is used inconsistently to assess the seriousness of the offence and therefore sentence the offender, thereby exposing imbalances in the criminal justice approach to cybercrime.[140] This finding is explained, in part, with the lack of consistent authorities, resulting partly from multiple instruments allowing to prosecute cyber offenders and partly from the absence of sentencing guidelines for the CMA 1990 (let alone s.170 of the DPA 2018). The cascade effect could assist in closing the imbalances or gap by providing a conceptualisation of the harms, victims and motivations relating to each step of the cascade model, as well as aggravating circumstances tied to the reaching of tipping points. In turn, these conceptualisations could inform either the reliance on a broader set of instruments for the conviction, or the drawing up of sentencing guidelines for the CMA 1990.

Like all qualitative research, the analysis has limitations tied to sampling. However, each limitation harbours findings that contribute to different bodies of research and point to policy changes. First, the starting point for this analysis was the identification of sentencing remarks by means of newspaper articles, for want of cybercrime reports. Such lack of reporting has serious consequences not only for the ability to conduct cybercrime research, but also for the open justice principle as a whole.[141] Further down the line, court materials are difficult to obtain because they are not freely available and are provided by private companies acting as the 'intermediaries' between the public and Courts. Observance of solutions found in other European jurisdictions may inspire novel approaches more in line with open justice principles. Thirdly, it seems apt to investigate whether specialised cybercrime courts could compensate for the interpretive shortcomings of technology neutral legislation. Finally, the research points to the difficulty of reconciling the list of mitigating factors and the appraisal of potential harms with the typical profile of the cyber offender. The ever-increasing seriousness of cybercrime clashes with an offender profile that features what would usually be mitigating circumstances (lack of financial interest, immaturity, young age), making it difficult for courts to consistently fulfil the objectives of sentencing and establish a standard. There is a serious risk that young offenders may be overly punished

[136] This is an issue even for victims and defendants. Monidipa Fouzder, 'Give Victims Sentencing Transcript, Baird tells HMCTS chief' (2019) <https://www.lawgazette.co.uk/news/give-victims-sentencing-transcript-baird-tells-hmcts-chief/5101314.article> ; Leslie J. Moran, 'Mass-mediated Open Justice: Court and Judicial Reports in the Press in England and Wales' [2013] 34 *Legal Studies*.

[137] The problem affects other categories of publicly-held materials, as discussed in relation to FOIs by Coral Sirdifield, David Denney, Rebecca Marples and Charlie Brooker, 'Researching Healthcare Availability for Probation Clients: an Illustration of Methodological Challenges and Lessons in Surveying Organisations' [2019] 15 *British Journal of Community Justice* 1.

[138] And ad hoc studies, such as those occasionally carried out by the Council of Europe.

[139] Porcedda (2023) (n 38).

[140] Pina-Sánchez (2014) (n 28).

[141] Among many: Michael Bohlander, 'Open Justice or Open Season: Should the Media Report the Names of Suspects and Defendants?' [2010] 74(4) *Journal of Criminal Law and Criminology* 321; Vanessa Yeo, 'Access to Court Records: the Secret to Open Justice' [2011] *Singapore Journal of Legal Studies* 510; Moran (2013) (n 138).

to serve the purposes of deterrence, against guidance and in defiance of the rights of the child, and with little impact on the reduction of cybercrime. All such findings are beyond the scope of this paper but open up very interesting avenues for further research, to which the data crime and cascade models can possibly be applied.

Funding

Data collection, research and presentation of the first draft of this paper at the 2nd Human Factor in Cybercrime conference were funded by UK's Engineering and Physical Sciences Research Council, CRITiCal ('Combatting cRiminals In The Cloud' - EPSRC EP/M020576/1) project. The research was conducted at the University of Leeds, which granted ethical approval, and the final draft submitted from Trinity College Dublin, where the initial ethical approval was acknowledged. The section on technology neutrality draws from research conducted for the ANTICS project, funded by Enterprise Ireland Grant n CS20202036.

Declaration of Competing Interest

I hereby declare that I have disclosed all relationships and funding sources and that there are no outstanding competing interests.

Data availability

The authors do not have permission to share data.

List of court cases

R v Kostromina, R v Milka, R Prakochyk, Croydon Crown Court, 2 October 2011

R v Mennim, Rv Pearson, Southwark Crown Court, 31 March 2012

R v Jeffery, Southwark Crown Court, 13 April 2012

R v Hussain, Southwark Crown Court, 27 July 2012

R v Beddoes, Randhawa and Sangha, Kingston-upon-Thames Crown Court, 19 March 2013

R v Oshodi, Jabeth, Hamid, Butt, Okala and Eve, Southwark Crown Court, 10 May 2013

R v Davis, R v Al-Bassam, R v Ackroyd, R v Cleary, R v Jeffery, Southwark Crown Court, 16 May 2013

R v Akinwolemiwa, Croydon Crown Court, 16 May 2014

R v Ogbogbor, Croydon Crown Court, 17 May 2014

R v Martin (appeal) [2013], EWCA Crim 1420

R v Simkus, R v Kurach, Southwark Crown Court, 23 December 2014

R v Hallam, R v Benson, Southwark Crown Court, 21 July 2015

R v Ojo and Agbaje, Basildon Crown Court, 8 January 2016

R v Markuta, Southwark Crown Court, 22 September 2016

R v Skowron, Croydon Crown Court, 16 December 2016

R v Turner, Mcdonagh, Drage and Coombes, Peterborough Crown Court, 30 January 2017

R v Ptach, Southwark Crown Court, 15 March 2017

R v West, Southwark Crown Court, 25 May 2018

Regina v Allsopp (appeal) [2019] EWCA Crim 95

R v Kelley, Central Criminal Court, 10 June 2019

Acknowledgment

I would like to thank the various judicial agencies which have helped me in conducting this research, former colleagues from the Centre for Criminal Justice Studies at the University of Leeds and the CRITiCal project, and current colleagues at the School of Law of Trinity College Dublin. In addition to Prof David S. Wall, special thanks to Prof Jose Piná-Sanchez, Dr Eszter Parkanyi, Dr Rebecca Marples, Prof. David Prendergast and Dr Ilaria Zavoli, for comments and suggestions which greatly helped improving the draft, and Ms Silvia Vailati for the assistance she provided with respect to the technology neutrality literature review in the context of the ANTICS project at Trinity College Dublin. I also wish to thank the anonymous reviewer(s) who carefully scrutinised and greatly helped to improve this work.

My gratitude goes to the participants in a number of conferences, whose comments have greatly helped in shaping this work: the SLSA 2019 conference (University of Leeds), the 2nd Human Factor in Cybercrime conference 2019 (Vrije Universiteit Amsterdam), BILETA 2019 (Queen's University Belfast) and 2021 (University of Newcastle) conferences, the lunchtime seminar (2021) of the School of Law at Trinity College Dublin, the IALS Financial Crime: Challenges and Responses 2021 Conference and the Council of Europe 2021 Octopus Conference. Finally, I wish to thank IEEE for granting permission to reproduce a number of figures and tables in this article. All mistakes are mine, the views expressed in this paper are my own and do not reflect those of either funding or judicial agencies.