scripted

Volume 17, Issue 2, August 2020

Book review: *Investigating Cybercrime*

Jan-Jaap Oerlemans
The Netherlands: Amsterdam University Press, 2017. 448 pages.
ISBN 978-90-8555-109-6. € 49.95.

A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe

Qianyun Wang
The Netherlands: Wolf Legal Publishers, 2017. 360 pages.
ISBN 9789462403451. € 34.95.

Reviewed by Paul De Hert and George Bouchagiar***

DOI: 10.2966/scrip.170220.431

* Professor, Law Science Technology & Society, Vrije Universiteit Brussel, Brussels, Belgium, paul.de.hert@vub.be; Associate Professor, Tilburg Law School, Department of Law, Technology, Markets, and Society, Tilburg, The Netherlands, paul.de.hert@tilburguniversity.edu
** Doctoral Researcher in Criminal Law and Technology , Faculty of Law, Economics and Finance, University of Luxembourg, Luxembourg,

Luxembourg, georgios.bouchagiar@uni.lu; Vrije Universiteit Brussel, Brussels, Belgium, georgios.bouchagiar@vub.be

1 *Investigating Cybercrime*

Oerlemans' *Investigating Cybercrime* (PhD study) is a volume in the series of the Meijers Research Institute and Graduate School of the Leiden Law School and part of the Law School's research programme 'Effective Protection of Fundamental Rights in a pluralist world'. It is an extremely useful tool for readers interested in the regulation of methods used in cross-border unilateral cybercrime investigations.

The book addresses the adequacy of regulation of the above methods by the Dutch criminal procedural law. To the author, this 'adequacy' is inextricably linked to the provision of necessary evidence-gathering tools and of minimum safeguards for human rights' protection. As such, adequacy is tested on the basis of the right to privacy, protected under Article 8 of the European Convention on Human Rights (ECHR). This context, analytically examined in Chapter 1, justifies the choice of Dutch law as the appropriate legal framework against which the assessment of adequacy can be carried out. The Netherlands, a member of the Council of Europe bound by the ECHR, already uses digital investigative methods; and its civil law system entails the 'criminal procedural legality principle' – a particularly strong version of the principle of legality.

Chapter 2, providing a typology of cybercrime, mainly discusses technology-as-a-target and technology-as-a-tool to better explain ways in which such crime can affect investigations. The author addresses evidence-gathering methods, as well as the crucial challenges of anonymity, encryption, and, most importantly, jurisdiction to identify four key digital investigative methods: gathering publicly available online information, issuing data production orders to online service providers, applying undercover investigative methods online, and performing hacking as an investigative method.

Thereafter, Article 8 of the ECHR is discussed in Chapter 3 to detect the normative demands capable of underlying the regulation of the four methods. After analysing the scope of the right to privacy and the conditions of justified interference, i.e. legality ('in accordance with the law'), legitimacy, and proportionality, the chapter draws particular attention to the criterion of 'in accordance with the law'. The sub-elements of this criterion, accessibility, foreseeability, and quality of law, are chosen to perform the assessment of adequacy.

Chapter 4 studies case law of the European Court of Human Rights on nondigital counterparts of the four digital methods to examine the seriousness of interference and the quality of law demanded by the Court. Despite difficulties in drawing comparisons between contemporary methods and techniques of the previous century, the research treats the ECHR as a living instrument and provides valuable insights into the desirable quality of law for each of the four methods.

The study then naturally progresses to the examination of how the Dutch legal regime can be improved to meet the desired adequacy. In Chapters 5–8, the author tests, for each identified method, the criteria of accessibility, foreseeability, and quality of law. Particularly useful recommendations, mainly directed to the Dutch legislator, are also offered.

Chapter 9 addresses desirability and legitimacy of the application of the four methods unilaterally across States. Here, the author sees legal certainty through the lens of the rule of law, instead of that of Article 8 of the ECHR. This frame and broader understanding allow for the precise identification and better comprehension of the legal implications of such unilateral application. It is not only the potential infringement of territorial sovereignty at stake, but also individual dangers; people risk being subjected to national laws other than those of the territory of their location. After a challenging comparative analysis of the

Dutch (civil law) and the US (common law) approach to the regulation of investigative methods, the chapter discusses their potential unilateral application by Dutch law enforcement authorities.

Chapter 10, highlighting jurisdictional challenges, stresses the need to reconceptualise the Dutch criminal procedural law, as well as to recognise the existence of cross-border unilateral digital evidence-gathering activities and to regulate them at an international level.

Chapter 11, finding regulation provided for by Dutch criminal procedural law inadequate, proposes recommendations of both national and international dimensions.

This book, of approximately 400 pages, is well-documented and definitely worth reading by all those interested in the general intertwining of cybercrime and privacy, but also by more specialised audiences focused on challenges posed by existing evidence-gathering activities.

It should, however, be borne in mind that Oerlemans' approach focuses solely on the legality test mentioned in Article 8, paragraph 2 of the ECHR ('is the legal basis for a limitation of Article 8 ECHR adequate?'). Oerlemans rightly summarises the essence of this test ("the more heavy an interference the more detailed regulations need to be")[1] and beautifully demonstrates how this formulation of the test should guide the legislator. The message is, however, not complete, since the author excludes from his analysis the necessity-test equally implied by Article 8 of the ECHR.[2] There might be a legal basis with enough detail, but is the interference really necessary in a democracy based on the rule of law? In this regard, useful insights could be drawn from the Court's recent

---

1 See, for example, Oerlemans' intelligible figures at pp. 78 and 91.

2 In case law, there is a propensity not to proceed to the necessity-assessment when legality-demands are left unsatisfied.

case law on subscribers' data:[3] what could meet legality, given detailedness of rules,[4] might fail to satisfy necessity, when going beyond the individual level[5] and toward bulk contexts.[6] If we combine the legality and necessity tests, we can better understand the author's approach toward regulating collection of subscriber data by law enforcement authorities. Oerlemans finds this interference not "particularly serious",[7] but nevertheless proposes detailed regulation. In our view, this treatment does not necessarily follow from the legality test (the heavier the interference, the more detailed the regulations) but can only be understood in the light of an integrated approach bringing in not only legality and detail, but also necessity. Collection of subscriber data by law enforcement authorities should not be made too easy, not because it is the heaviest of all interventions, but because it is not always necessary in a democratic state.

2 *A Comparative Study of Cybercrime in Criminal Law*

On a slightly different note, Wang's book focuses on substantive criminal law; albeit, it also addresses procedural provisions, where jurisdiction-related issues are brought up for discussion. The publication is peculiarly useful to readers interested in the regulation of and approaches to cybercrime across national and international regimes.

As Chapter 1 explains, the book mainly deals with cybercrime as 'genuine cybercrime' (new offences independent of traditional crimes) and as computer-

---

3 *Breyer v Germany*, Application no. 50001/12 (ECtHR, 30 January 2020) ('*Breyer*').

4 *Breyer*, para. 83.

5 To Oerlemans, privacy interference resulting from the obtaining of subscribers' data is placed below the "very serious" level (pp. 199–201); similarly, to the Court, interference resulting from the storing of such data can be of a 'rather limited nature'; *Breyer*, para. 95.

6 *Breyer*, Dissenting Opinion of Judge Ranzoni, paras. 14 and 26. Regarding necessity, the Court reiterates that the interference must address a 'pressing social need' and be proportionate to the legitimate goal pursued; *Breyer*, para. 88.

7 See Oerlemans' suggestions at p. 113.

facilitated crime (assisted by technologies and already addressed by criminal law). To assess how legislation can be adjusted to regulate cybercrime, the research investigates the historical evolution of cybercrime-related law and examines approaches to cybercrime in the jurisdictions of China, the Council of Europe (CoE), the United States, England and Wales, and Singapore.

Starting with China, Chapter 2 reveals the broadened scope of cybercrime and inconsistencies in law. For instance, the 'two points one dimension' approach was introduced in 2009 to draw a firm line between genuine cybercrime and traditional crimes facilitated by technology; albeit, this line was erased by subsequent amendments, which treated – and penalised – preparatory activities (related to technology-facilitated crimes) as cybercrimes.

Chapter 3 discusses the CoE's regime, which – though not national – can be comparable due to its detailed provisions. The analysis of the Convention on Cybercrime demonstrates the CoE's desire to harmonise national laws. Moreover, two clear lines are drawn by the author; one reflecting the desire of the Convention's drafters and distinguishing between genuine cybercrime and technology-facilitated crimes; and another inspired by the provisions of the Convention and differentiating between crimes against computer systems and crimes against data. Wang also highlights some important limitations to the systematic regulation of cybercrime and stresses jurisdiction-related problems. Namely, no criteria of substance are set out to precisely define cybercrime and the territorial principle cannot always address cybercrime's non-territorial aspects.

After examining historical developments of the United States' regime, Chapter 4 discusses contemporary, wide (yet precise) approaches to cybercrime; that is, the text of the United States' legislation (meaning the Computer Fraud and Abuse Act), which, though clear, is broad enough to cover – and criminalise – behaviours targeted at almost any type and use of computers. Such approaches

nevertheless allow for legal inconsistencies (e.g. in the understanding of computer and data). The chapter also finds a tendency to emphasise general interests (e.g. national security) over online freedom.

Chapter 5 is dedicated to England and Wales. The examination of its 'half-way' approach, relying upon new legal provisions to address genuine cybercrime but also upon existing laws to regulate technology-facilitated crime, shows hesitance in the introduction of new offences. Such introduction is, however, allowed, when deemed absolutely necessary. This was the case with new provisions introduced in and after 2006 to supplement the 1990's regime (i.e. the Computer Misuse Act) and protecting data and the function of computers.

Singapore's legal provisions, discussed in Chapter 6, seem to suffer from a lack of originality. This could be due to inspiration drawn from several jurisdictions, like the English approach to hacking. Furthermore, the Singaporean regime does not distinguish between computer and data-related offences. And, as the chapter suggests, its enforcement strategies seem to reflect prioritisation of governmental over individual interests.

Chapter 7 analyses and draws comparisons between jurisdictions. It provides useful insights into four key issues that address the question of how law can be adapted to regulate cybercrime. First, the research argues for the necessity of concrete laws to govern cybercrime. Second, it discusses the computer *and* data approach (preferred over one-sided computer *or* data perspectives) as the most adequate legal approach to cybercrime. Third, in light of failures of existing principles, it calls for 'creative thinking' to resolve jurisdictional challenges. Fourth, it suggests that the Convention on Cybercrime could contribute to the conceptualisation of cybercrime-specific laws; being open to members as well as non-members, it could perform the role of a global harmonising instrument supporting the computer *and* data perspective.

Wang's book is of approximately 350 pages and includes a specific bibliography, as well as appendices with relevant provisions. It is well-structured and comprehensive with figures explaining the modus operandi of contemporary techniques (like phishing), tables summarising findings (or comparing legal provisions), and diagrams (e.g. providing statistical information). The study can definitely be recommended to those interested in global, regional, or national approaches to cybercrime regulation.

3 Comment: The Need to Tackle Jurisdictional Challenges

Taken together, the two publications have one thing in common. They reveal the acute need to address what seems to be at the heart of cybercrime regulation: jurisdictional challenges. Perhaps the answer lies in the optimal, rather than absolute, harmonisation;[8] in making – to the extent possible – same behaviours punishable,[9] while, at the same time, respecting national diversity. An international approach to cybercrime, promoting general legal principles, could be combined with national initiatives, setting out more detailed rules, to achieve appropriate balances and optimal results.

There seems to be no ready-made recipe; and cooperation among states, as well as between state and non-state actors, could allow for combining national

---

[8] In this regard, flexible harmonisation has been discussed as a realistic, rather than perfect, route; as a way to uniformly address substantive law, while leaving procedural (due process-related) provisions to domestic laws and their particularities. Jonathan Allan Clough, "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation" (2014) 40(3) *Monash University Law Review* 698–736, p. 709 (with further references).

[9] For example, in the European context, Weyembergh has suggested approaching substantive criminal law through (the harmonising effect of) Directives. See Anne Weyembergh, "Approximation of Substantive Criminal Law: The New Institutional and Decision-Making Framework and New Types of Interaction Between EU Actors" in Francesca Galli and Anne Weyembergh (eds.), *Approximation of Substantive Criminal Law in the EU: The Way Forward* (Brussels: Editions de l'Université de Bruxelles, 2013), pp. 9–33 and 31–33.

initiatives to achieve the desired harmonising effect. This suggestion could very well be linked to or rely upon theoretical frameworks and, in particular, Swenson's legal pluralism archetypes that help better comprehend state-non-state interactions.[10] The prioritisation of cooperative and complementary perspectives over antagonistic (combative and competitive) approaches could be the way toward optimal harmonisation and bridging. The two reviewed books seem to let such cooperative and complementary perspectives in and welcome legal pluralism as a crucial element for the possibility of state and non-state authorities to successfully regulate cybercrime.[11]

[10] Geoffrey Swenson, "Legal Pluralism in Theory and Practice" (2018) 20(3) *International Studies Review* 438–462, pp. 442–446 and 456.

[11] See, for instance, Oerlemans' recommendations (at p. 383) referring to cooperation of states, as well as the role of international organisations; see also Wang's proposals (at pp. 277–282), some of which are more general, not expressly directed to legislators or expressly targeted at academics (e.g. to detect important features of cybercrime, instead of defining it).