THE CAMBRIDGE HANDBOOK OF DIGITAL EVIDENCE IN CRIMINAL INVESTIGATIONS

Authored by leading scholars in the field, this handbook delves into the intricate matter of digital evidence collection, adopting a comparative and intradisciplinary approach. It focuses specifically on the increasingly important role of online service providers in criminal investigations, which marks a new paradigm in the field of criminal law and criminal procedure, raising particular challenges and fundamental questions. This scholarly work facilitates a nuanced understanding of the multifaceted and cross-cutting challenges inherent in the collection of digital evidence, as it navigates the contours of current and future solutions against the backdrop of ongoing European and international policy-making. As such, it constitutes an indispensable resource for scholars and practitioners alike, offering invaluable insights into the evolving landscape of digital evidence gathering.

Vanessa Franssen is a professor at the University of Liège where she teaches criminal law, national and comparative criminal procedure, as well as cybercrime. Her current research centers on the impact of new technologies on criminal justice, at both national and European levels. Furthermore, she has extensive research experience in the field of European Union and comparative criminal law and procedure, economic criminal law as well as the interplay between criminal law and punitive administrative law.

Stanisław Tosza is Associate Professor in Compliance and Law Enforcement at the University of Luxembourg, where he researches and teaches comparative and European criminal law and criminal procedure, white-collar crime, cybercrime and cyberlaw. In his research he focuses in particular on the role of private actors in enforcement as well as the challenges of new technologies for criminal justice. He is the Secretary General of the International Association of Penal Law (AIDP).

The Cambridge Handbook of Digital Evidence in Criminal Investigations

Edited by

VANESSA FRANSSEN

University of Liège

STANISŁAW TOSZA

University of Luxembourg

CAMBRIDGE
UNIVERSITY PRESS

Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of Cambridge University Press & Assessment,
a department of the University of Cambridge.

We share the University's mission to contribute to society through the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781316511275

DOI: 10.1017/9781009049771

When citing this work, please include a reference to the DOI 10.1017/9781009049771

First published 2025

A catalogue record for this publication is available from the British Library

Library of Congress Cataloging-in-Publication Data
NAMES: Franssen, Vanessa editor | Tosza, Stanislaw editor
TITLE: The Cambridge handbook of digital evidence in criminal investigations / edited by Vanessa Franssen, University of Liège, Stanislaw Tosza, University of Luxembourg.
DESCRIPTION: Cambridge, United Kingdom ; New York, NY, USA : Cambridge University Press, 2024. | Series: Cambridge law handbooks | Includes bibliographical references and index.
IDENTIFIERS: LCCN 2024019915 | ISBN 9781009049771 ebook | ISBN 9781316511275 hardback
SUBJECTS: LCSH: Digital forensic science | Criminal justice, Administration of | Evidence, Criminal | Electronic evidence
CLASSIFICATION: LCC HV8078.7 .C36 2024 | DDC 363.250285–dc23/eng/20241007
LC record available at https://lccn.loc.gov/2024019915

ISBN 978-1-316-51127-5 Hardback

Contents

Tables

Contributors

Ma. Angela Leonor Aguinaldo, Associate Professorial Lecturer, De La Salle University, Philippines.

Tatiana Alekseeva, PhD student, Law Faculty, Moscow State University and lawyer at the Analytical Center of Criminal Law and Criminology, LLC, Russia.

Seçil Bilgiç, LLM Harvard Law School (Fulbright Scholar); technology transactions lawyer at Cohesity; admitted to the New York State Bar and the Istanbul Bar Association; formerly mergers and acquisitions/corporate lawyer at White & Case LLP.

Dominik Brodowski, Professor of Europeanization, Internationalization and Digital Transformation of Criminal Law and Criminal Procedure, Saarland University, Germany.

Sem Careel, FWO PhD researcher, Institute of Criminal Law, KU Leuven, Belgium.

Theodore Christakis, Professor of International, European and Digital Law at Grenoble Alps University, France and Director of Research for Europe with the Cross-Border Data Forum.

Marine Corhay, PhD candidate (FRESH grantee) FRS-FNRS, University of Liège, Belgium.

Carmen Cuadrado Salinas, Senior Lecturer in Criminal Procedure Law, Fellow at Faculty of Law, University of Alicante, Spain.

Paul de Hert, Professor of Law, Faculty of Law and Criminology, Free University of Brussels, Belgium and Associate Professor of Law and Technology, Tilburg Institute for Law and Technology (TILT), The Netherlands.

Cyprien Delpech de Saint Guilhem, FWO Postdoctoral Fellow, Computer Security and Industrial Cryptography (COSIC), KU Leuven, Belgium.

Anže Erbežnik, Professor of Criminal Law and Criminal Procedure, European Law Faculty, Slovenia and Advisor in the Secretariat of the European Parliament's Legal Affairs Committee and before of its Justice, Home Affairs and Fundamental Rights Committee.

Maria Filatova, PhD, Head of the Analytical Center of Criminal Law and Criminology, Russia.

Vanessa Franssen, Professor of Criminal Law and Criminal Procedure, University of Liège and Affiliated Senior Researcher, Institute of Criminal Law, KU Leuven, Belgium.

Agnes Kasper, PhD, Senior Lecturer of Technology Law, Tallinn University of Technology, Estonia.

Olga Kostyleva, Assistant Professor, Law Faculty, Moscow State University, Russia.

Elif Mendos Kuşkonmaz, Lecturer in Law, University of Essex, United Kingdom.

Giulia Lasagni, Senior Assistant Professor in Criminal Procedure, University of Bologna, Italy.

Eneli Laurits, State Prosecutor dealing with corruption-related crimes, Estonia.

Katalin Ligeti, Professor of European and International Criminal Law and Dean of the Faculty of Law, Economics and Finance, University of Luxembourg; President of the International Association of Penal Law.

T. J. McIntyre, Associate Professor, University College Dublin Sutherland School of Law and Chairperson of Digital Rights Ireland.

Maria Helen Murphy, Associate Professor, Maynooth University School of Law and Criminology, Ireland.

Juan Carlos Ortiz Pradillo, Professor of Civil and Criminal Procedure, Complutense University of Madrid, Spain.

Anna-Maria Osula, Senior Researcher, Tallinn University of Technology, Estonia and Research Fellow, Masaryk University, Czech Republic.

Gavin Robinson, Assistant Professor, eLaw – Center for Law and Digital Technologies, Leiden University, Netherlands.

Maciej Rogalski, Professor, Department of Criminal Law, Lazarski University and Rector of that university, Poland.

Melita Sogomonjan, Lecturer, Tallinn University of Technology, Estonia.

Dan Svantesson, Professor, Faculty of Law, Co-director for the Centre for Space, Cyberspace and Data Law, Bond University, Australia; Senior Fellow, Social Cyber Institute; Research Fellow, Masaryk University, Czech Republic; and Associated Researcher, Swedish Law and Informatics Research Institute, Stockholm University, Sweden.

Stanisław Tosza, Associate Professor in Compliance and Law Enforcement, University of Luxembourg and Secretary General of the International Association of Penal Law.

Tatiana Tropina, former Assistant Professor in Cybersecurity Governance, Institute of Security and Global Affairs at Leiden University, Netherlands.

Frank Verbruggen, Professor of Belgian, European and International Criminal Law, Institute of Criminal Law, KU Leuven, Belgium.

Ian Walden, Professor of Information and Communications Law, Centre for Commercial Law Studies, Queen Mary University of London, United Kingdom.

Li Zhe, Associate Professor, Faculty of Law, University of Macau.

Jin Zhenan, PhD candidate, Faculty of Law, University of Macau.

Foreword

Our digital information society comes with many advantages that will further increase with artificial intelligence (AI) applications. The digitalized world, be it in the area of communications, the Internet of Things or platform economies, not only produces and processes an enormous amount of data but also creates, through interconnectivity, new data knowledge and related applications. This bright side of innovative technologies, however, also comes with a dark side. Our daily digital fingerprint, based on location data and other, meta data, creates the possibility to construct a full personal digital identity. Data knowledge can be abused for preventive surveillance by states and companies, and undermine fundamental rights and democratic values.

The digital society is also an environment in which crime patterns change. New digital crimes are emerging and digital tools are meanwhile being used for committing common offenses of all types. The result is that access to electronic data for evidence purposes, commonly called digital or electronic evidence, has become indispensable in the large majority of criminal investigations. In the 2022 Sirius EU Digital Evidence Situation Report by Eurojust and Europol, we can read to what extent the request from law enforcement and judicial authorities to internet service providers (ISPs) has exploded and become a decisive tool in criminal investigations (Europol, "SIRIUS EU Digital Evidence Situation Report," 4th Annual Report, 2022, p. 16). With the rapid advancement of AI technologies, the need for direct enforcement cooperation with ISPs and other private partners in the digital markets will only increase.

At the national level many states have adapted their criminal substantive law by introducing new cybercrimes and have revised their criminal procedural law by providing new tools for digital investigations, including production orders to ISPs located in their territory. The problem is, however, that the large majority of the ISPs are not established in the jurisdiction of the state of investigation or do not even offer services in that state, that the relevant data are located in multiple jurisdictions or that it is even unclear where they might be located. This globalization of digital criminal evidence leads to a disconnect with the territorial criminal jurisdiction of states and creates very significant obstacles for law enforcement agencies. As we all know, criminal law enforcement is strictly related to state sovereignty and territoriality, meaning that law enforcement agencies are not allowed to extend their operational investigative powers beyond their national borders. If they need transborder access to (digital) evidence, they have to rely on existing instruments of mutual legal assistance (MLA), which can be bilateral, multilateral or included in international repression conventions such as, for instance, the UN Convention on Transnational Crime (UNCTOC), the UN Convention on Corruption (UNCTAC) or the Council of Europe Convention on Cybercrime (Budapest Convention).

The problem with these conventions is that they rely on interstate cooperation and interstate requests between central authorities at the ministerial level. Most of these conventions have not been designed for digital evidence that is moreover mostly not in the hands of state authorities but held by the real gatekeepers in today's digital society: the ISPs. These conventions are also cumbersome, time-consuming and thus not really adapted to volatile digital information. However, these conventions contain standardized rules for cooperation and also provide for some minimum rights and remedies for the persons concerned.

In the light of this new reality and given the enforcement gap and the risk of impunity, national authorities have been experimenting with and attempting to regulate forms of cross-border access to data, outside of the existing MLA box. Legislators have come up with concepts such as the obligation for ISPs to locate data in the national jurisdiction or forms of extraterritorial investigative jurisdiction for serious crimes in exceptional circumstances, for instance when the digital evidence in point cannot be obtained on the basis of MLA. For their part, the law enforcement agencies have elaborated, based on national law, models of cooperation with ISPs on a voluntary basis, or have issued unilateral subpoenas for the production of data by foreign ISPs, or have used remote search and seizure (including so-called governmental hacking) in foreign jurisdictions or in cyberspace, in some cases in a legal limbo. This national unilateralism comes, of course, with tensions and clashes between states as well as between states and ISPs, but also triggers important questions in relation to sovereignty, international law standards, concepts of jurisdiction, the protection of fundamental rights and even data security. International law, unfortunately, also does not offer us any clear answers to the question whether these cross-border criminal investigative techniques could constitute a violation of sovereignty.

The demand for new regulatory standards is high and the international communities have been trying to come up with a new legal framework for the cross-border gathering of digital evidence in criminal matters. At the level of the Council of Europe, negotiations were launched in 2017 to elaborate a Second Additional Protocol to the Budapest Cybercrime Convention to enhance cooperation and the disclosure of electronic evidence. Although this is a regional Convention, it is the most important multilateral convention and the international standard in the field, as it has been ratified by important nonmember states of the Council of Europe and has also been a model for many national legislators, even in countries that have not joined the Convention. The negotiations on the Second Additional Protocol to the Cybercrime Convention were very difficult and intensive (more than ninety meetings), but were eventually concluded in 2022 and the Second Additional Protocol has been tabled for signature from May 12, 2022 onwards. Only parties to the main Convention are allowed to join. The Protocol contains, inter alia, an "emergency" MLA procedure in the case of a significant and imminent risk to the life or safety of any natural person and direct cooperation with ISPs, but this is limited to less intrusive data such as domain name registration or subscriber information. This means that content data, also very important for law enforcement, are excluded from direct cooperation with the ISPs. Clearly, the second Protocol did not bring about a convincing solution and is certainly not a game changer.

At EU level, the European Commission submitted, for its part, an e-evidence package in April 2018, as part of its broader regulatory Digital Agenda (Digital Markets Act, Digital Services Act, EU Data Act, Data Governance Act, AI Act, EU Media Freedom Act), its Security Strategy and its Priorities for the Area of Freedom, Security and Justice. The package contained a proposal for a directive and a proposal for a regulation. The directive provides for the obligation for ISPs active in the internal EU market to designate a legal representative in the EU. The regulation creates a European preservation order and a European production order, based on

mutual recognition, that a competent judicial authority can directly impose on foreign ISPs, thereby bypassing, to a large extent, the classic mutual recognition between the judicial authorities of the member states. Unlike the Second Additional Protocol to the Budapest Convention, this proposal consists of a real paradigm change as it invests the ISPs with a public role: it puts them in the position of an extended arm of the judicial authorities and also delegates the fundamental rights compliance check in the executing state largely to them. The negotiations on the EU e-evidence package were very intensive and difficult, as there were many disagreements between the member states and also between the European Commission, the Council of the EU and the European Parliament. The disagreements related, inter alia, to the bypassing of the judicial authorities of the executing state, the duties of the ISPs to check compliance with fundamental rights, the broad range of offenses, the types of data that should be covered, the grounds for refusal and the enforcement regime in the case of noncompliance by the ISPs.

Both the Regulation and the Directive were adopted in July 2023 and it seems that the model of direct cooperation with the ISPs has survived. The ISPs will be embedded in an EU-wide platform to guarantee the authenticity of the orders and the security of communications. The rights of ISPs to refuse cooperation are limited and ISPs are in principle obliged to produce the required data. Enforcement procedures and potentially significant sanctions (going up to 2 percent of the total worldwide annual turnover) shall assure compliance with the orders. Contrary to the Second Protocol, the e-evidence package has greater chances to become a real game changer introducing a completely new paradigm of public–private cooperation in the cross-border gathering of digital evidence in criminal matters.

Relevant is also the United States' dimension where many important ISPs are established. In 2018, US Congress passed the CLOUD Act, under which ISPs can lift blocking provisions and produce data, including content data, related to non-US citizens and residents to foreign judicial authorities only if there is an executive agreement between the US and the country of the foreign judicial authority. Such agreement would allow for direct cooperation with the ISPs, even for content data, without channeling the judicial request through the MLA mechanisms. The first CLOUD Act executive agreement was concluded between the US and the UK in 2019, and entered into force on October 3, 2022. In the meantime, an agreement with Australia has been signed and negotiations with Canada have started. Negotiations between the US and the EU have also been launched, but have been stalled as they awaited the approval of the e-evidence package in the EU, and were revived once the agreement on the package was reached.

It is against the backdrop of all these challenges and legal developments that this Handbook comes in and is filling a real gap by giving us an insight into: (1) the phenomenon of digital evidence in criminal matters and the new challenges it creates, be they legal or technological; (2) the discussions at the scholarly and policy levels on relevant concepts and definitions; (3) the new legal instruments elaborated by the EU, the Council of Europe – including the issues that were discussed (heavily) around the negotiation table – and the US CLOUD Act; and (4) how national jurisdictions are (or will be) dealing with the challenges. As you will understand from these four dimensions, this Handbook offers a highly interesting and very valuable analysis of the state-of-the-art and the challenges to be overcome, from the point of view of both effective law enforcement and compliance with fundamental rights. The Handbook is based on an international and comparative research project directed by the two editors. They have in my opinion decided on a convincing structure for this Handbook, starting with Part I on "Collecting Digital Evidence: Transversal Challenges and Solutions." In this first part the contributions not only set

the scene (the phenomenon, the impact of digitalization on criminal justice and so on) but also deal with the problem of definitions of digital evidence and the types of data, with unsolved problems of jurisdiction, digital investigative measures, digital evidence law as well as encryption technology and criminal justice. The contributions have been written not only by criminal lawyers but also by international public lawyers and computer scientists. In this part we also get an in-depth analysis of the new European and international legal framework for direct cooperation with ISPs when it comes to the gathering of digital information for evidence purposes in criminal matters.

Even when new international and European standards are of the utmost importance for judicial cooperation, the national regulations on the gathering and use of digital evidence are and will to a large extent remain the backbone for the law enforcement agencies. Therefore, the editors have made a very wise choice to include in this Handbook a substantial part on comparative criminal justice both in Europe (Part II) and worldwide (Part III), based on a convincing set of jurisdictions for a functional comparison and making use of a modeled questionnaire for the exercise. The richness of the comparative approach is threefold. First, it shows to which extent the national legislator and the judiciary (including in many cases constitutional courts) have been struggling with giving content to the new challenges in this field. Second, it also demonstrates the regulatory gaps in many countries. Third, it shows very clearly that exercising enforcement jurisdiction, particularly investigative jurisdiction, outside the national territory, based on a unilateral approach encounters quite some difficulties in law and in practice, from the point of view of both effective enforcement as well as compliance with fundamental rights. And thus the need for international standards is also based on evidence that is delivered by this national comparative analysis.

The Handbook clearly underpins the need for new legislative solutions at the international level in order to provide for effective enforcement. However, it also stresses that the game changer, by including the ISPs in the cooperation mechanisms, cannot come with a substantial loss of procedural safeguards and fundamental rights. Outsourcing fundamental rights compliance to ISPs is also outsourcing a positive obligation of states toward a private party and entails the risk of the privatization of enforcement and of human rights compliance. Finally, both the Council of Europe and the EU are international communities in which the rule of law and fundamental rights are key values. If they want to be global trendsetters, they will have to find a convincing balance between the interest of effective criminal enforcement and the protection of fundamental rights. If the security approach were to become the leading factor in the new cooperation instruments, then these instruments would risk undermining the key values not only of the criminal justice systems but also of the international communities in which they are adopted.

Prof. Dr. John A. E. Vervaele
Professor at the College of Europe, Bruges; Emeritus Professor of Economic and European Criminal Law, Utrecht University, Honorary President of the International Association of Penal Law (AIDP-IAPL)