



The Rise of Transnational Surveillance and the Future of Criminal Investigative Procedures

Written by Perrine Guilmain

Edited by Areesh Siddiqui, final editing by Josephina Trebing

Abstract:

The increasing reliance on digital evidence within criminal investigations has exposed the limits of territorially grounded legal systems of criminal procedure. The aim of this journal is to examine whether emerging frameworks that govern cross-border access to digital evidence sufficiently protect fundamental human rights; such as Art. 8 of the ECHR. Focusing on the EU e-Evidence Regulation¹ and the US CLOUD Act², it introduces the important question of whether efficiency-driven mechanisms undermine the legitimacy/fairness of a trial and privacy guarantees under human rights law. This suggests that, without harmonised safeguards and effective oversight, current approaches risk undermining procedural justice in transnational criminal investigations.

Key Words: Transnational Surveillance, EU e-Evidence Regulation, US CLOUD ACT, Mutual Legal Assistance Treaties, ECHR, Privacy Rights, Human Rights Law, Digital Criminal Investigations.

Introduction

Digital technology has fundamentally reshaped the nature of modern criminal investigations. Electronic communication, chat rooms, data storage in the ‘cloud’, and metadata now constitute the new norm, and key forms of evidence, yet are frequently stored outside of the territorial jurisdiction of the investigative authority. An example of this being Apple iCloud data, these data centres being located in the United States, Denmark and China.³ Though digitalisation has enhanced investigative capacities, it has simultaneously hindered criminal procedure frameworks that remain grounded in their territorial sovereignty.

¹Ilias Bantekas, Susan Nash and Mark Mackarel, *International Criminal Law* (Third, Routledge 2001)78–80.

²Jennifer Daskal, ‘Borders and Bits’ (*Scholarship@Vanderbilt Law*2018) <<https://scholarship.law.vanderbilt.edu/vlr/vol71/iss1/3/>>

³‘Apple Data Center and Servers FAQ’ (www.datacenterknowledge.com) <<https://www.datacenterknowledge.com/servers/apple-data-center-and-servers-faq>>.



This development of technology has raised an important question within the investigative procedures of international criminal law: Can cross-border access to digital evidence still remain in line with the procedural safeguards designed to protect human rights? As states are increasingly prioritising speed and efficiency in their investigations rather than ensuring that all rights are fulfilled, traditional mechanisms of judicial oversight are at high risk of being marginalised.

Territoriality and its Relationship with Mutual Legal Assistance in Criminal Law

Traditionally, Cross-border evidence has been governed by Mutual Legal Assistance Treaties (MLATs), which highlight the principles of territorial sovereignty and interstate cooperation. These mechanisms require consent in order to pass through designated authorities, ensuring that there is judicial oversight by both the requesting and requested states.⁴

MLATs have often been criticised for being slow and ill-suited to the ever changing nature of digital evidence, which can be rapidly altered or deleted⁵. However, it is important to recognise that the procedural safeguards embedded within the MLAT frameworks, such as judicial authorisation and respect for domestic legal standards, are what ensures human rights being protected within criminal investigations. Thus, the marginalisation of MLATs risks discarding protections that have long reinforced international criminal procedures.

New Legal Frameworks regarding Cross-Border Digital Evidence

In response to the ongoing criticism of MLATs, states have established new instruments which enable a more direct approach to accessing digital evidence. An example of this would be within the European Union, *Regulation 2023/1543 on European Production and Preservation Orders*. This regulation allows authorities in one member state (belonging to the EU) to demand the immediate release of digital data of service providers in another state.⁶ The scope of the Regulation includes various categories of electronic evidence, namely Subscriber data (names and addresses), Traffic data (metadata relating to communications) and Content data

⁴Ilias Bantekas, Susan Nash and Mark Mackarel, *International Criminal Law* (Third, Routledge 2001)78–80.

⁵Jennifer Daskal, 'Borders and Bits' (*Scholarship@Vanderbilt Law*2018) <<https://scholarship.law.vanderbilt.edu/vlr/vol71/iss1/3/>>

⁶Regulation - 2023/1543 - EN - EUR-Lex' (*Europa.eu*2023) <<https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng>>.



(emails, messages etc.) Most requests for traffic data require notification of the enforcing state, however, requests limited to basic subscriber information do not require such notification, permitting a more expedited access to information.

The United States has implemented a similar Act, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) which permits US authorities to compel companies (which are subject to US jurisdiction) to disclose data that is stored abroad— facilitating executive agreements with foreign states.⁷ Both frameworks have significantly increased the efficacy of investigative measures in criminal cases, however, this has reduced the involvement of the member state in which the data is located, leading to an increased risk of an unfair trial due to lack of monitoring and limited opportunities of judicial oversight/scrutiny.

Private Actors as De Facto Participants in Criminal Procedures

Though these new legal frameworks have allowed for efficacy, a notable consequence of these frameworks is the expanding role of private service providers in criminal investigations. Technology companies have become increasingly responsible for assessing the legality of cross-border data requests and determining their compliance.⁸

Unlike public authorities, private actors are not bound by constitutional obligations in the same manner. This structurally weakens judicial oversight in criminal procedures regarding accountability, transparency, and access to remedies. Individuals whose data is accessed may receive no information, undermining their ability to contest the legality of the investigative measures.

Implications for Privacy and Fair Trial Rights

Cross-border access to digital evidence has had significant implications for international human rights law. Article 8 of the European Convention on Human Rights (ECHR) focuses on the interest of individuals— protecting their right to privacy and requiring interference to be lawful, necessary and proportionate, reasonable suspicion having to be met.⁹ However, Article 8 is not

⁷ Clarifying Lawful Overseas Use of Data Act, 18 USC §§ 2713–2714.

⁸ ‘Opinion 23/2018 on Commission Proposals on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (Art. 70.1.b) | European Data Protection Board’ (*Europa.eu*2018) <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-232018-commission-proposals-european-production_en>

⁹ EHRC, ‘Article 8: Respect for Your Private and Family Life’ (*Equality and Human Rights Commission*24 June 2021) <<https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life>>.

an absolute right. Under Article 8(2) ECHR, any interference must satisfy a three part test: it must be (i) in accordance with the law, (ii) pursue a legitimate aim (such as the prevention of crime), and (iii) be necessary to a democratic society, meaning the interference must be proportionate to the aim pursued. The court, alongside the ECHR, has recognised that robust safeguards require not only a clear legal basis, but independent judicial oversight, strict necessity and proportionality assessments, and operative ex-post remedies to prevent any abuse of surveillance powers.¹⁰

The first case discussing this is *Big Brother Watch v. United Kingdom*.¹¹ The court stresses that ‘bulk interception regimes’ in the United Kingdom (the collection of private communication)¹² may be amassed only with the presence of robust safeguards. The court recognised the ever-changing nature of modern technology and surveillance yet stressed that invasive investigatory powers demand proportionally robust procedural guarantees to ensure there is no breach of Article 8 ECHR.

Similarly, the case of *Roman Zakhrov v. Russia* held that secret surveillance regimes that lack adequate safeguards constitute a breach of Article 8 ECHR, even when an individual cannot demonstrate that they were directly exposed to said surveillance. This judgement underlines the importance of legal certainty, transparency, and the prevention of arbitrary interferences with private life. The principles in the case aforementioned directly correlates to cross-border digital evidence gathering, due to investigative measures often being invasive, opaque and lacking effective remedies. Although Courts require vigorous safeguards, the margin of appreciation doctrine allows States a degree of discretion in the structuring of their national security and surveillance regimes. In a transnational context, this discretion may result in uneven standards of protection and complicate accountability in cases where digital evidence is obtained across jurisdictions.

Beyond privacy concerns, cross-border evidence regimes may also engage Article 6 ECHR, which guarantees the right to a fair trial. When digital evidence is obtained through muddled

¹⁰ *Szabó and Vissy v Hungary*’ (2016) 63 EHRR 3 [56]–[58]. <<https://hudoc.echr.coe.int/fre?i=001-160020>>

¹¹ ECHR, ‘*CASE OF BIG BROTHER WATCH AND OTHERS v. the UNITED KINGDOM*’ (Coe.int2026) <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-210077%22%5D%7D>

12 ‘Bulk Surveillance: Europe’s Recent Landmark Judgements – Digital Freedom Fund’ (*Digital Freedom Fund*2023) <<https://digitalfreedomfund.org/bulk-surveillance-europes-recent-landmark-judgements>>.



surveillance practices or without sufficient judicial oversight, questions arise regarding the legitimacy of this evidence, alongside the equality of arms. Enacting Article 6 of the ECHR allows for a strengthening in the procedural justice dimension of transnational surveillance debates.

Fragmentation and the Emphasis of Legal Uncertainty in Transnational Criminal Justice

When considering all the information given throughout this journal, it has been made clear that the coexistence of divergent national and regional frameworks that govern access to digital evidence, has led to a fragmented legal landscape. Conflicts within the law continue to arise due to multiple states attempting to assert jurisdiction over the same data, resulting in the affected individuals struggling to identify which legal standard they can apply and what remedies are available to them.¹³

This fragmentation poses a threat to the totality of human rights protection in criminal proceedings. Without a harmonised safeguard or common legal ground, all individuals are potentially subjected to investigative measures that would be deemed unlawful under their own legal system, diminishing their trust in transnational criminal cooperation, and the law as a whole entity.

Conclusion

It is important to recognise that these shortcomings of existing legal frameworks do not suggest that cross-border access to digital evidence should be abandoned. Technology continues to transcend everyday and it is important to implement new laws and strategies.

This journal aims to demonstrate the need for reform to be grounded within international human rights standards. Said reform should include minimal procedural safeguards, mandatory judicial authority/supervision, and more transparency regarding the law so that it remains comprehensive to citizens.

¹³Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' [2017] SSRN Electronic Journal.
<http://dx.doi.org/10.2139/ssrn.2732346>



Crucially, we emphasise that private service providers cannot be left to perform public law functions without a more scrutinous oversight. In order for efficiency to not come at the expense of procedural justice, it is essential to focus on a rights-centered transnational framework, focusing on individuals rather than regulations.

Digital evidence has rewritten borders and rights within criminal investigations. Criminal law's legitimacy is derived from its restraint, accountability, and respect for procedural safeguards. In a borderless environment such as the use of digital evidence in criminal procedures, it is quintessential to preserve these principles in order to ensure the legitimacy of transnational criminal justice.

***Perrine Guilmain** (2005, she/her) is a Belgian-Irish student at Vrije Universiteit Amsterdam, pursuing a Bachelor's degree in Law in Society (LL.B). Her academic interests include Criminal Law, Human Rights and Legal Philosophy. She intends on pursuing a Master's degree in Journalism to strengthen her analytical skills, with the aim of making complex legal issues more accessible and comprehensive throughout her career.*



Bibliography:

Ilias Bantekas, Nash S and Mackarel M, *International Criminal Law* (Third, Routledge 2001) 78-80

Daskal J, 'Borders and Bits' (*Scholarship@Vanderbilt Law*2018) <<https://scholarship.law.vanderbilt.edu/vlr/vol71/iss1/3/>>

'Apple Data Center and Servers FAQ' (*www.datacenterknowledge.com*) <<https://www.datacenterknowledge.com/servers/apple-data-center-and-servers-faq>>

'Regulation - 2023/1543 - EN - EUR-Lex' (*Europa.eu*2023) <<https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng>>

'Opinion 23/2018 on Commission Proposals on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (Art. 70.1.b) | European Data Protection Board' (*Europa.eu*2018) <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-232018-commission-proposals-european-production_en>

EHRC, 'Article 8: Respect for Your Private and Family Life' (*Equality and Human Rights Commission* (24 June 2021) <<https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life>>

'Szabó and Vissy v. Hungary' (*hudoc.echr.coe.int*) <<https://hudoc.echr.coe.int/fre?i=001-210077>>

ECHR, 'CASE of BIG BROTHER WATCH and OTHERS v. the UNITED KINGDOM' (*Coe.int* 2026) <<https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-210077%22%5D%7D>>

'Bulk Surveillance: Europe's Recent Landmark Judgements – Digital Freedom Fund' (*Digital Freedom Fund* 2023) <<https://digitalfreedomfund.org/bulk-surveillance-europes-recent-landmark-judgements/>>



Kuner, Christopher, Reality and Illusion in EU Data Transfer Regulation Post Schrems (July 7, 2017). 18 German Law Journal 881 (2017), Available at SSRN: <http://dx.doi.org/10.2139/ssrn.2732346>