Prosecuting communication services providers as crime facilitators: a cautionary tale

Oerlemans, J.; Royer, S.

Computer Law & Security Review 61 (2026) 106330

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

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

Prosecuting communication services providers as crime facilitators: A cautionary tale

Jan-Jaap Oerlemans [a,*], Sofie Royer [b]

[a] Institute for Criminal Law and Criminology, Leiden University, Steenschuur 25, 2311 ES, Leiden, the Netherlands
[b] KU Leuven, Centre for IT & IP Law (CiTiP), Sint-Michielsstraat 6, 3000 Leuven, Belgium

ARTICLE INFO

Keywords:
Crypto communication services
Bulletproof hosting
Privacy
Complicity
KYC
Criminal liability

SUMMARY

This article examines a novel trend in combating organised (cyber)crime: prosecuting communication service providers for complicity in offences committed by their users. Illustrative of this approach is the high-profile case involving Pavel Durov, CEO of Telegram, launched in 2024. The authors observe that, over the past decade, bulletproof hosting providers and providers of crypto communication services have also been prosecuted. They were prosecuted on the charges of complicity for computer crimes and organised crime, such as drug trafficking facilitated through their platforms. Drawing from Dutch judgments, the article examines this prosecution strategy and identifies its challenges and risks. Moreover, the authors identify key constraints for these operations from a fundamental rights perspective.

1. Introduction

Pavel Durov, founder and Chief Executive Officer (CEO) of the widely used communication platform Telegram, was arrested on 24 August 2024 as part of a French investigation into criminal activities allegedly facilitated through the platform. French law enforcement authorities charged Durov with multiple offenses, including criminal association with intent to commit a crime, the refusal to provide information for lawful interception, and complicity in the distribution of child sexual abuse material, drug trafficking, money laundering, computer crime, and fraud.[1]

Following his arrest, Durov was detained for several days before being released on bail set at approximately five million euros. Coincidentally, Durov said in September 2024 that the messaging app would tackle criticism of its content moderation and remove some features that had been abused for illegal activity.[2] In March 2025, an investigating judge relaxed his travel restrictions, permitting Durov to temporarily leave France. Consequently, Durov returned to Dubai, although he continues to face charges in France.[3]

The arrest of Pavel Durov is illustrative of a new trend in law enforcement strategy to combat cybercrime and organised crime. As demonstrated by the analysis of this strategy and case law in this article, law enforcement authorities and public prosecutors increasingly target communication service providers. In press releases, these providers are frequently characterised as "crime facilitators". With the intention of combating cybercrime more effectively and deterring future offending, law enforcement authorities cooperate internationally and employ a variety of interventions, such as issuing warning messages to suspects and informing victims of cybercrime. Public prosecutors also prosecute individuals with key positions within these companies for complicity in criminal offences committed by their clients.

This article explains why communication service providers are prosecuted and examines whether this approach is compatible with fundamental rights. The research question is therefore: *To what extent do*

* Corresponding author.
E-mail address: j.oerlemans@law.leidenuniv.nl (J.-J. Oerlemans).

[1] Parquet de Madame la Procureure de la République, Communiqué de press, 26 August 2024. https://www.tribunal-de-paris.justice.fr/sites/default/files/2024-08/2024-08-26%20-%20CP%20TELEGRAM%20.pdf (accessed 1 February 2026).

[2] M. Trevelyan, M. Coulter, Durov says Telegram will tackle criticism of how it moderates content, Reuters.com, 6 September 2024. https://www.reuters.com/technology/durov-says-telegram-will-tackle-criticism-how-it-moderates-content-2024-09-06/ (accessed 1 February 2026).

[3] Le Monde with AFP, Telegram founder Durov allowed to temporarily leave France, where he is charged, LeMonde.fr, 15 March 2025. https://www.lemonde.fr/en/international/article/2025/03/15/telegram-founder-durov-allowed-to-temporarily-leave-france-where-he-is-charged_1234567_4.html (accessed 1 February 2026). In November 2025, his travel ban was fully lifted: LeMonde with AFP, France fully lifts travel ban on Telegram founder Durov, lemonde.fr, 13 November 2025. https://www.lemonde.fr/en/france/article/2025/11/13/france-removes-travel-ban-for-telegram-founder-pavel-durov_6747429_7.html (accessed 1 February 2026).

https://doi.org/10.1016/j.clsr.2026.106330

Available online 20 April 2026

fundamental rights constrain the strategy of law enforcement authorities and public prosecutors to target communication service providers?

Existing scholarship on prosecutions involving communication service providers and their clients – notably concerning to the 'EncroChat' and 'SkyECC' cases - has primarily focused on the impact on the right to privacy and the right to a fair trial.[4] Cross-border evidence gathering and the use European Investigation Orders for data acquisition have also been widely discussed.[5] This article shifts the focus from criminal cases targeting users of these (encrypted) communication services to those involving individuals to those involving individuals holding positions of responsibility within these companies, including directors and staff with technical expertise. It contributes to current knowledge by systematically analysing for which offences these individuals are prosecuted, while considering the important role of communications service providers in enabling access to (encrypted) communication and the relevant fundamental rights constraints.

Most case law concerning the prosecution of communication service providers within the European Union (EU) originates from the Netherlands. As detailed in Section 2, this is a consequence of Dutch law enforcement's pioneering strategy to obtain large amounts of data from communication service providers and dismantle the infrastructure used by clients of these services. Because criminal laws governing complicity and participation in crime vary across EU member states, the fact that this research relies primarily on Dutch case law represents a significant limitation.[6] Consequently, this article's case law analysis does not aim to provide an extensive comparative exercise but relies heavily on Dutch judgments.

To answer the research question, this article is structured as follows. Section 2 explains the underlying reasons why law enforcement authorities and prosecutors increasingly target communication service providers. Section 3 examines the implications of this strategy for fundamental rights and the extent to which these fundamental rights impose restrains on it. Section 4 analyses the judgments relating to four communication service providers, highlighting the extent to which individuals with key positions within these companies can be prosecuted for complicity in crimes committed by their clients. Section 5 compares the case law analysis in Section 4 with the fundamental rights constraints identified in Section 3 and provides a reflection of the findings. The article concludes by answering the research question and providing recommendations for practitioners, alongside directions for future research.

2. The evolution of a law enforcement strategy

This section outlines the background to the strategy of targeting communication service providers by law enforcement authorities and public prosecution services; a strategy pioneered by Dutch law enforcement authorities. It begins by explaining how the inherent difficulties in investigating cybercrime have led to more strategic operations aimed at combating this type of offending more effectively and deterring future criminal activity. We then focus on international cybercrime operations with significant involvement of Dutch law enforcement authorities, where communication service providers are regarded as 'crime facilitators'. Finally, we explain how this strategy is increasingly adopted in the European Union to investigate and prosecute serious crime, such as offences involving criminal organisations engaged in drug trafficking.

2.1. *From reactive to pro-active investigations*

Cybercrime investigations present significant challenges due to the inherent difficulties in identifying suspects, overcoming encryption and navigating jurisdictional boundaries. These difficulties have been widely documented in literature and reports.[7] For instance, cybercriminals often use online handles (nicknames) to conceal their true identity and employ techniques to obscure their originating IP addresses. Traditional investigative methods, such as intercepting internet communications, are increasingly complicated by the widespread

[4] See J.J. Oerlemans, D.A.G. van Toor, Legal aspects of the EncroChat operation: A human rights perspective, Eur. J. Crime Crim. Law Crim. Justice 30 (2022) 309–328. https://doi.org/10.1163/15718174-bja10037; P. Sommer, Evidence from hacking: a few tiresome problems, Forensic Sci. Int. Digit. Invest. 40 (2022) 301333. https://doi.org/10.1016/j.fsidi.2022.301333; R. Stoykova, Encrochat: the hacker with a warrant and fair trials?, Forensic Sci. Int. Digit. Invest. 46 (2023) 301602. https://doi.org/10.1016/j.fsidi.2023.301602; J.J. Oerlemans, S. Royer, The future of data driven investigations in light of the Sky ECC operation, New J. Eur. Crim. Law 14 (2023) 434. https://doi.org/10.1177/20322844231212661; C. Ursing, M. Konopka, K. Moeller, OMEGA: studying Swedish court cases built on decrypted chat messages, Nord. Tidsskr. Kriminalvidenskab 111 (2024) 203. https://doi.org/10.7146/ntfk.v111i3.151392; S. Okunrobo Perez, Proliferation of e evidence: reliability standards and the right to a fair trial, Eur. J. Crime Crim. Law Crim. Justice 33 (2025) 187–200. https://doi.org/10.1163/15718174-bja10070.

[5] J. Lindeman, M. Luchtman, D.A.G. van Toor, Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair-Trial Rights in the Netherlands, in: L. Bachmaier, F. Salimi (Eds.), Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights, Hart, Oxford, 2024, pp. 103–126; A. Sachoulidou, The Court of Justice in Staatsanwaltschaft Berlin v M.N. (EncroChat): from cross border, data driven police investigations to evidence admissibility, Maastricht J. Eur. Comp. Law 31 (2024) 510–519. https://doi.org/10.1177/1023263X241290365; D. Bajović, D. Ćorić, Encrochat and Sky ECC Data as Evidence in Criminal Proceedings in Light of the CJEU Decision, Eur. J. Crime Crim. Law Crim. Justice 33 (2025) 235. doi:10.1163/15718174-bja10062; G. Lasagni, G. Contissa, Effective rights and remedies in the computable era: facing informative asymmetry when AI adds to transnational cooperation, in: G. Lasagni, G. Contissa, M. Caianiello (Eds.), Facilitating Judicial Cooperation in the EU: A Computable Approach to Mutual Recognition in Criminal Matters, Brill, Leiden, 2025, pp. 19–22; E. Cervellera, France: cooperation in criminal matters between mutual recognition and protection of fundamental rights – the contribution of France, in: G. Lasagni, G. Contissa, M. Caianiello (Eds.), Facilitating Judicial Cooperation in the EU: A Computable Approach to Mutual Recognition in Criminal Matters, Brill, Leiden, 2025, pp. 168–170.

[6] J. Keiler, Actus reus and participation in European criminal law (doctoral thesis), Maastricht University, Intersentia, Maastricht, 2013, p. pp. 295, 557. 295 and 557. See also J. Keiler, Forms of participation, in: J. Keiler, D. Roef (Eds.), Comparative Concepts of Criminal Law, Intersentia, Cambridge, Antwerp, Chicago, 2019, pp. 328.

[7] See, e.g., E.J. Koops, The Internet and Its Opportunities for Cybercrime, in: P.C. van Duyne et al. (Eds.), Transnational Criminology Manual, Wolf Legal Publishers, Nijmegen, 2010, pp. 735–754; United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (Draft February 2013) UNODC CCPCJ EG.4/2013, p. 143.; J.J. Oerlemans, Investigating cybercrime (doctoral thesis), Amsterdam University Press, Amsterdam, pp. 37–58; Europol, Eurojust, Common Challenges in Combating Cybercrime, Europol, The Hague, 2019, pp. 10, 15–16; Europol, Internet Organised Crime Threat Assessment (iOCTA) 2021, Europol, The Hague, 2021, p. 18; Europol, Internet Organised Crime Threat Assessment (iOCTA) 2023, Europol, The Hague, 2023, p. 6; Europol, Internet Organised Crime Threat Assessment (iOCTA) 2024, Europol, The Hague, 2024, pp. 11, 33–34; Europol, European Police Chiefs Call for Industry and Governments to Take Action against End-to-End Encryption Roll-Out, 21 April 2024. https://www.europol.europa.eu/media-press/newsroom/news/european-police-chiefs-call-for-industry-and-governments-to-take-action-against-end-to-end-encryption-roll-out (accessed 1 February 2026); Europol, Eurojust, First, Second and Third report of the observatory function on encryption, 2019–2021. https://www.eurojust.europa.eu/ (accessed 1 February 2026); Europol, Eurojust, Common Challenges in Cybercrime, Europol, The Hague, 2025. https://doi.org/10.2813/3243780. https://www.europol.europa.eu/publications-events/publications/common-challenges-in-cybercrime (accessed 1 February 2026); J. Bonnes, O. Divendal, Innovatie in het Strafrecht: effectieve aanpak van cybercriminaliteit vergt brede bestrijding en verdient betere regulering, Ars Aequi 4 (2024) 320–330.

adoption of encryption technologies by search engines, webservers, and encrypted communication applications. Finally, jurisdiction often represents the greatest obstacle in cybercrime investigations. Both suspects and evidence may be located abroad. Due to the territorial restriction of enforcement jurisdiction, the collection of evidence or arrest of individuals cannot take place abroad without permission from the State involved (either *ad hoc* or on a treaty basis).[8] Advancements in EU instruments for judicial cooperation, such as the European Investigation Order, have facilitated cross-border evidence gathering. Nevertheless, jurisdictional issues continue to pose significant challenges in cybercrime investigations.[9]

Furthermore, the challenges of anonymity, encryption and jurisdiction are often intertwined. For example, in their 'internet Organised Threat Assessment' (iOCTA) of 2023, Europol states that: *"While VPN services are not illegal, some of them are designed for and advertised to criminals. Full anonymity offered by end-to-end encryption (E2EE) and a lack of cooperation with lawful requests for information from law enforcement are characteristic of these VPN services. Criminal VPN providers are aware of the needs of criminals and actively advertise their services on criminal markets VPN providers."*[10]

To address these challenges in cybercrime investigations, Dutch law enforcement officials of the Dutch 'Team High Tech Crime' developed a new strategy to combat cybercrime more effectively.[11] Rather than pursuing digital leads reactively, they adopted a proactive and well-planned approach. The strategy can be regarded as a refinement of 'intelligence-led' or 'data-driven' policing.[12] Law enforcement authorities 'Collect', 'Store', 'Analyse', and 'Engage' with data in a strategic manner. This so-called 'CSAE-model' is further explained in the following example.

Consider an online marketplace specialising in drug sales. Data about these marketplaces can be collected through the use of various investigative powers, including the seizure of servers, hacking, infiltration, and interception of internet traffic. The data is then stored in large amounts on a digital forensic platform and analysed using various forensic tools.[13] For example, a copy of a web server may reveal the platform's operational structure, administrative accounts, financial transactions, and details of vendors and buyers, providing both intelligence and potential evidence for criminal investigations.[14] The analysis may reveal a 'top-10 list' of vendors, allowing law enforcement officials to focus on these individuals in follow-up criminal investigations. After this collection, storage, and analysis of data, law enforcement authorities "Engage" with the data. This engagement is much broader than the collection of evidence for prosecution; it encompasses a wider range of activities aimed at disrupting criminal operations and protecting the public.

To combat cybercrime more effectively and deter future offending, law enforcement authorities can utilise a variety of "interventions". For example, Dutch law enforcement authorities also use the data as intelligence and employ tactics such as publicly 'naming and shaming' top sellers on online marketplaces, conducting 'cease-and-desist visits' with buyers of drugs or child sexual abuse materials (hereinafter: CSAM) from online marketplaces, and posting 'warning messages' on the splash page of a seized domain, internet forums, and channels or groups on messaging apps like Telegram.[15] In addition, victims of cybercrime are informed and enabled to check whether they are victimised of cybercrime via websites and provided with advice about how to prevent cybercrime.[16]

Combating cybercrime requires an international effort, and it is safe to state that this has now become a widely adopted strategy within the EU. Between 2015 and 2025, Dutch law enforcement authorities participated in dozens of international cybercrime operations, leading to the dismantling of IT infrastructures at communication service providers used for various types of cybercrime. The operations listed below demonstrate how this strategy is employed to combat different forms of cybercrime, ranging from online markets on the dark web and services utilised by cybercriminals, to dismantling botnets, ransomware attacks, and websites enabling CSAM.

- **'Operation Onymous'** (2014) focused on online markets on the dark web. The Head of the European Cybercrime Centre, Troels Oerting, stated: *"Today we have demonstrated that, together, we are able to*

[8] This strict territorial limitation of enforcement jurisdiction was made explicit by the Permanent Court of International Justice as early as 1927. PCIJ, SS Lotus, 1927, *PCIJ Reports*, Series A, No. 10 (France v. Turkey). See also M.N. Schmitt (Ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, Cambridge, 2017, pp. 145–146.

[9] See, e.g., Europol, Internet Organised Crime Threat Assessment (iOCTA) 2024, Europol, The Hague, 2024, p.13, 24 and 31; Europol and Eurojust 2025 (n 7). See also D. Bajović, D. Ćorić, Encrochat and Sky ECC Data as Evidence in Criminal Proceedings in Light of the CJEU Decision, Eur. J. Crime Crim. Law Crim. Justice 33 (2025) 235. doi:10.1163/15718174-bja10062, discussing the tension between national sovereignty, mutual recognition, and the admissibility of evidence obtained abroad.

[10] Europol, Internet Organised Crime Threat Assessment (iOCTA) 2023, Europol, The Hague, 2023, p. 6.

[11] E. van de Sandt, A. van Bunningen, J. van Lenthe, J. Fokker, Towards data scientific investigations: a comprehensive data science framework and case study for investigating organized crime and serving the public interest, Third INTERPOL UNICRI Global Meeting on AI for Law Enforcement, Bristol, 25 November 2020. See also A.J. van Eeden, J.J. van Berkel, C.C. Lankhaar, C.J. de Poot, Opsporen, vervolgen en tegenhouden van cybercriminaliteit, WODC Cahiers 2021, 18 October 2021, p. 40.

[12] J.H. Ratcliffe, Intelligence-Led Policing, Willan Publishing, Cullompton, 2008; M. den Hengst, O.L. Wijsman, Datagedreven politiewerk: Een organisatorisch en juridisch perspectief, in: T. Snaphaan et al. (Eds.), Big Data Policing, Gompel & Svacina, Antwerpen, 2023, pp. 71–90; W. Landman, Politiewerk aan de horizon. Technologie, criminaliteit en de toekomst van politiewerk, Politie & Wetenschap, Den Haag, 2023.

[13] R.B. Van Baar, H.M.A. van Beek, E.J. van Eijk, Digital Forensics as a Service: A game changer, Digit. Invest. (2014) 54-56; H.M.A. van Beek et al., Digital forensics as a service: Game on, Digit. Invest. (2015) 20-28; H.M.A. van Beek et al., Digital forensics as a service: Stepping up the game, Digit. Invest. (2020) 1-13.

[14] This data is also analysed for academic papers. See, e.g., R.S. van Wegberg et al., Plug and prey? measuring the commoditization of cybercrime via online anonymous markets, in: 27th USENIX Security Symposium (USENIX Security 18), USENIX, Berkeley, 2018, pp. 1009–1026 and F. Miedema et al., Mixed Signals: Analyzing Ground-Truth Data on the Users and Economics of a Bitcoin Mixing Service, in: 32nd USENIX Security Symposium (USENIX Security 23), USENIX, Berkeley, 2023, pp. 751–768.

[15] A.J. van Eeden, J.J. van Berkel, C.C. Lankhaar, C.J. de Poot, Opsporen, vervolgen en tegenhouden van cybercriminaliteit, WODC Cahiers 2021, 18 October 2021; B.W. Schermer, De gespannen relatie tussen privacy en cybercrime, inaugural lecture, Leiden University, Leiden, 2022; M.F.H. Hirsch Ballin, J.J. Oerlemans, Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden, Delikt en Delinkwent 2 (2023); J. Bonnes, O. Divendal, Innovatie in het Strafrecht: effectieve aanpak van cybercriminaliteit vergt brede bestrijding en verdient betere regulering, Ars Aequi 4 (2024), p. 320; M. Bada, A. Hutchings, Y. Papadodimitraki, R. Clayton, An evaluation of police interventions for cybercrime prevention, University of Cambridge Computer Laboratory Technical Report No. 983, July 2023. https://doi.org/10.48456/tr-983; E.G. van 't Zand, S. Matthijsse, T. Fischer, W. van der Wagen, Interventions for cyber offenders, in: W. van der Wagen, J.J. Oerlemans, M. Weulen Kranenbarg (Eds.), Essentials in Cybercrime: A Criminological Overview for Education and Practice, Eleven, The Hague, 2024, pp. 317–347.

[16] See, e.g., Politie.nl, Check je hack, https://www.politie.nl/informatie/checkjehack.html (accessed 1 February 2026). This service notifies individuals based on data seized in cybercrime operations and provides advice on preventing cybercrime.

efficiently remove vital criminal infrastructures that are supporting serious organised crime (…)".[17];

- **'Operation PowerOFF'** (2017, 2022 and 2024) focused on 'DDoS for hire-services'. Europol's press release noted: "*In response to the growing threat of these attacks, Operation PowerOFF not only focuses on dismantling the infrastructure supporting these attacks and holding those responsible accountable, but also takes proactive steps to prevent further incidents. These proactive steps include the creation of ads on Google search and YouTube aimed at deterring young people from engaging in these nefarious activities."*[18];
- **'Operation TOURNIQUET'** (2022) focused on online fraud markets. The Head of the European Cybercrime Centre, Edvardas Šileris, was quoted as follows: "*Disruption has always been a key technique in operating against threat actors online, so targeting forums that host huge amounts of stolen data keeps criminals on their toes. Europol will continue working with its international partners to make cybercrime harder – and riskier – to commit."*[19];
- **'Operation Endgame'** (2024 and 2025) focused on ransomware. Europol's press release noted: "*There were actions aimed at criminal services and their criminal users. These users were directly contacted by the police and asked to share relevant information regarding infostealers via the Operation Endgame Telegram channel. In addition, the failing criminal services are exposed via the Operation Endgame website*".[20]
- **'Operation Stream'** (2025) focusing on a child sexual exploitation platforms. Magnus Brunner, EU Commissioner for Internal Affairs and Migration, was quoted: "*The dismantling of this criminal network demonstrates the added value that EU agencies like Europol provide. This is precisely why the European Commission has presented a strategy for greater security in Europe. Criminals operate across borders, so we must also support investigators in doing the same."*.[21]

This law enforcement strategy is endorsed by the Dutch government.[22] However, it has not been without criticism and has prompted legal debate in the Netherlands. Scholars have questioned the extent to which investigatory powers can be used for purposes beyond prosecution, how the processing of large amounts of data – often referred to as 'bulk data' – should be regulated, and how effective oversight of these operations' lawfulness can be achieved.[23] This has led to the establishment of an evaluation committee tasked with addressing these issues and providing a report with recommendations by September 2026.[24]

In this article, we further focus on the question of criminal liability and complicity for communication service providers arising from criminal activities committed by their clients.

[17] Europol, Global action against dark markets on Tor network, 7 November 2014. https://www.europol.europa.eu/media-press/newsroom/news/global-action-against-dark-markets-on-tor-network (accessed 1 February 2026).

[18] See Europol, Operation PowerOFF. A global law enforcement effort targeting and dismantling Distributed Denial of Service (DDoS) for hire, 01 July 2017–15 July 2025. https://www.europol.europa.eu/media-press/newsroom/news/operation-poweroff-global-law-enforcement-effort-targeting-and-dismantling-distributed-denial-service-ddos-hire (accessed 1 February 2026).

[19] Europol, One of the world's biggest hacker forums taken down, 12 April 2022. https://www.europol.europa.eu/media-press/newsroom/news/one-worlds-biggest-hacker-forums-taken-down (accessed 1 February 2026).

[20] Europol, Largest ever operation against botnets hits dropper malware ecosystem. International operation shut down droppers including IcedID, SystemBC, Pikabot, Smokeloader and Bumblebee leading to four arrests and takedown of over 100 servers worldwide, 30 May 2024. https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem (accessed 1 February 2026); Europol, End of the game for cybercrime infrastructure: 1025 servers taken down. Operation Endgame's latest phase targeted the infostealer Rhadamanthys, Remote Access Trojan VenomRAT, and the botnet Elysium, 13 November 2025. https://www.europol.europa.eu/media-press/newsroom/news/end-game-cybercrime-infrastructure-1025-servers-taken-down (accessed 1 February 2026).

[21] Europol, Global crackdown on Kidflix, a major child sexual exploitation platform with almost two million users. The Europol-supported operation led to 79 arrests and 1,400 identifications, 2 April 2025. https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users (accessed 1 February 2026); Europol, Organised crime online: How Europol disrupts cybercrime, 11 November 2025. https://www.europol.europa.eu/media-press/newsroom/news/organised-crime-online-how-europol-disrupts-cybercrime (accessed 1 February 2026).

[22] See the Dutch Ministry of Justice and Security, Parliamentary letter of the Minister of Justice and Security, Parliamentary Series II 2024/25, 26643, nr. 1357, 27 June 2025, p. 4: *"Cybercrime therefore requires a comprehensive approach. Criminal enforcement remains essential but is supplemented with disruptive measures such as taking criminal infrastructures offline, disrupting the criminal revenue model, and deploying alternative interventions"*. See with regard to other countries: R. Borum, Scientific and Technological Advances in Law Enforcement Intelligence Analysis, in: B. Fox, J.A. Reid, A.J. Masys (Eds.), Science Informed Policing, Springer International Publishing, Cham, 2020, pp. 99–121.

[23] Commissie modernisering opsporingsonderzoek in het digitale tijdperk ('Commissie Koops I'), Regulering van opsporingsbevoegdheden in een digitale omgeving, Radboud University Press, Nijmegen, 2018; M.I. Fedorova et al., Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden, Radboud University Press, Nijmegen, 2022; M.F.H. Hirsch Ballin, J.J. Oerlemans, Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden, Delikt en Delinkwent 2 (2023); M. Galič, Bulkbevoegdheden en strafrechtelijk onderzoek: Lessen uit de jurisprudentie van het EHRM voor de normering van grootschalige data-analyse, Tijdschr. Bijz. Strafr. Handh. 2022(2) (2022) 130–137. https://doi.org/10.5553/TBSenH/229567002022008002007; B.W. Schermer, B.H.M. Custers, Modernisering strafvordering en de bescherming van persoonsgegevens in het opsporingsonderzoek, Delikt en Delinkwent 54(8) (2024) 659–673.

[24] In January 2025, the Dutch Minister of Justice and Security announced the establishment of a commission to advise on the legal framework for the further processing of criminal justice data. The commission, chaired by Prof. Bert-Jaap Koops, was tasked with proposing safeguards for the use of bulk data in policing. See Dutch Ministry of Justice and Security, Parliamentary letter on the establishment of the commission on criminal justice data processing, 29 January 2025. https://www.rijksoverheid.nl/documenten/kamerstukken/2025/01/29/tk-instellen-commissie-strafvorderlijke-gegevensverwerking (accessed 1 February 2026) and Dutch Ministry of Justice and Security, Decree establishing the Commission on the Regulation of Bulk Data Processing for Policing, Government Gazette (Staatscourant) 2025, no. 24983. https://zoek.officielebekendmakingen.nl/stcrt-2025-24983.html (accessed 1 February 2026).

2.2. Communication service providers as 'crime facilitators'

On numerous occasions, Dutch law enforcement authorities and Europol have referred to certain types of communication service providers as "crime facilitators".[25] These include hosting providers, VPN services, and cryptophone providers that offer services to criminals. They fail to respond to requests from law enforcement authorities and permit anonymous registrations and payments.

Europol stated this most clearly in its 2023 internet Organised Threat Assessment: "*Many Internet Service Providers (ISPs) frequently used by criminals do not engage in extensive customer monitoring practices such as Know-Your-Customer (KYC) procedures and storing of customer and metadata (e.g. IP address), facilitating criminal activities. Some of them do not provide customer information upon lawful requests except for an automated confirmation of an email address, leading to a limited availability of identifying information on a suspect*".[26]

These communication service providers allow their customers considerable leniency on the content they can upload and tend not to respond to requests for information from law enforcement authorities.[27] This type of hosting is referred to as bulletproof hosting, which has been notoriously difficult for law enforcement authorities to address for many years.[28] Hosting is a complex international business area where servers are often resold to other datacentres located in different regions, which can further complicate investigations.

An illustrative example is 'Cyberbunker', a bulletproof hosting provider notorious for hosting the file sharing platform 'The Pirate Bay' from a former NATO bunker in Traben-Trarbach in Germany. In 2015, the provider caught the attention of law enforcement authorities. Its clientele allegedly included dark web marketplaces, such as 'Wall Street Market' and 'Fraudsters', which facilitated the sale of drugs, counterfeit currency, prescription drugs, and stolen credit card data.[29] During the operation 886 servers – about two million gigabyte – were seized.[30]

On 6 September 2019, law enforcement authorities dismantled Cyberbunker. Ultimately, the principal defendant 'X.' and seven co-defendants were charged with and found guilty of membership in a criminal organisation.[31] The courts found that the defendants were aware of Cyberbunker's business model, which openly advertised hosting of all legal and illegal content - excluding child sexual abuse material and terrorist content - under the slogan "*stay online, no matter what!*".[32]

The defendants were informed about the general business model and were aware that the vast majority of their customers used their servers for criminal activities, particularly cybercrime. Their motivations included financial profit and, for some, an ideological commitment to enabling third parties to use the internet free from state control and surveillance. They lacked detailed knowledge of each individual offence, but were aware of the general criminal character of their clientele and the organisation's aim to facilitate such conduct.[33] Therefore, the German public prosecution office initially charged the defendants with complicity (*Beihilfe*) to numerous offenses committed by their clients, including drug trafficking, dealing in counterfeit currency, data theft, and the sale of prescription medication, hosting websites involved in the sale of synthetic drugs and psychotropic substances, and attempted computer sabotage through botnet hosting.

However, both courts acquitted the defendants of complicity (*Beihilfe*) in these specific offenses committed by their clients. The primary reason was the lack of the required intent to aid those specific crimes at the time the hosting services were provided. The courts found that, while the defendants knew that illegal activities were likely taking place, they generally did not have specific knowledge of the exact nature, type, or scope of these individual criminal acts (e.g., specific drug transactions) when providing server space and internet access. Under German law, general awareness or merely holding it possible "any criminal activities" were promoted, is insufficient to establish the required intent. The legal standard for complicity (*Beihilfe*) mandates that the participant's intent must encompass the essential characteristics of the principal offense, meaning that it must be related to a specific, concrete offense. Ultimately, the suspects were convicted of membership in a criminal organisation. Crucially, that offence only requires proof that the members knew the organisation aimed at these serious acts, rather than demanding knowledge of the exact details of specific underlying crimes, as is common in many countries.[34]

Dutch law enforcement authorities are particularly active in targeting communication service providers, such as bulletproof hosting providers and VPN-services. This is illustrated by the list of cybercrime operations between 2015–2025 below.

- **MaxiDed Bulletproof Hosting** (2018): Dutch law enforcement authorities seized ten servers from 'MaxiDed'. MaxiDed was

[25] See, e.g., FIOD, FIOD doet onderzoek naar bedrijf dat 'bulletproof' internetdiensten aanbiedt. https://www.om.nl/actueel/nieuws/2020/09/25/fiod-doet-onderzoek-naar-bedrijf-dat-%E2%80%98bulletproof%E2%80%99-internetdiensten-aanbiedt, 2020 (accessed 1 February 2026);Openbaar Ministerie, OM eist gevangenisstraf voor aanbieder Ennetcom PGP-telefoons. https://www.om.nl/actueel/nieuws/2021/05/27/om-eist-gevangenisstraf-voor-aanbieder-pgp-toestellen, 2021 (accessed 1 February 2026); Openbaar Ministerie, Politie leest opnieuw mee met criminelen: cryptocommunicatiedienst Exclu ontmanteld. https://www.om.nl/actueel/nieuws/2023/02/03/politie-leest-opnieuw-mee-met-criminelen-cryptocommunicatiedienst-exclu-ontmanteld, 2023 (accessed 1 February 2026). Europol, Internet Organised Crime Threat Assessment (iOCTA) 2021, Europol, The Hague, 2021, p. 19; Europol & Eurojust, 'Third report of the observatory function on encryption 2021, p. 18; Europol, Internet Organised Crime Threat Assessment (iOCTA) 2023, Europol, The Hague, 2023, p. 6; EU Serious and Organised Crime Threat Assessment (EU SOCTA), Europol, The Hague, 2025, p. 18.

[26] Europol, Internet Organised Crime Threat Assessment (iOCTA) 2023, Europol, The Hague, 2023, p. 6.

[27] Europol, Internet Organised Crime Threat Assessment (iOCTA) 2023, Europol, The Hague, 2023, p. 4. See also, e.g., A. Noroozian et al., Platforms in everything: Analyzing Ground-Truth data on the anatomy and economics of Bullet-Proof hosting, in: 28th USENIX Security Symposium (USENIX Security 19), USENIX, Berkeley, 2019, pp. 1341–1356.

[28] Europol, Internet Organised Crime Threat Assessment (iOCTA) 2023, Europol, The Hague, 2023, p. 4.

[29] Der Spiegel, The German Bunker that Became a Hub of International Crime, 22 May 2020. https://www.spiegel.de/international/germany/the-german-bunker-that-became-a-hub-of-international-crime-a-0000000.html (accessed 1 February 2026); E. Caesar, The Takedown of a Dark-Web Marketplace, The New Yorker, 23 January 2021. https://www.newyorker.com/magazine/2021/01/23/the-takedown-of-a-dark-web-marketplace (accessed 1 February 2026).

[30] Berliner Kurier, Wie ein alter Bundeswehrbunker zum Darknet-Rechenzentrum werden konnte, 18 October 2020. https://www.berliner-kurier.de/000000 (accessed 1 February 2026).

[31] See §129 of the German Criminal Code (StGB).

[32] The main defendant received five years and nine months of prison sentence by the Court of Trier, while the others received sentences ranging from one to three years.

[33] See Landgericht Trier, Judgment of 13 December 2021, 2a KLs 5 Js 30/15; Bundesgerichtshof, Judgment of 12 September 2023, 3StR 306/22, ECLI:DE:BGH:2023:120923U3STR306.22.0, p. 30.

[34] See the judgment of the Bundesgerichtshof of 12 September 2023, 3StR 306/22, ECLI:DE:BGH:2023:120923U3STR306.22.0, p. 30. See also J. Keiler, Actus reus and participation in European criminal law (doctoral thesis), Maastricht University, Intersentia, Maastricht, 2013, p. 282. Interestingly, new legislation was adopted in Section 127 of the German Criminal Code (StGB) and criminalises whoever operates an internet trading platform whose purpose is to facilitate or promote 'unlawful acts'.

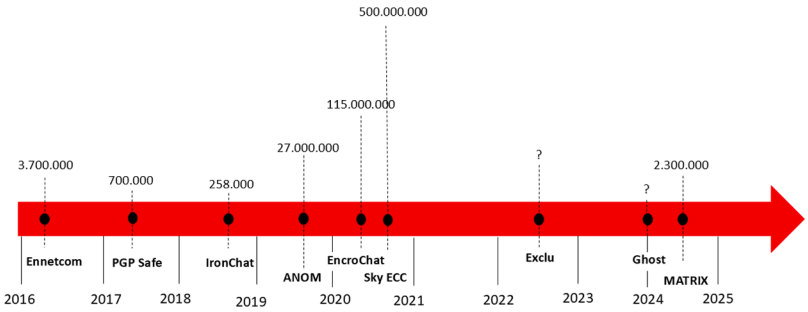

Fig. 1. A timeline of cryptophone operations from 2015–2025 and quantity of messages.[45].

characterised as a bulletproof hosting provider. The data was shared with Europol, and two suspects were arrested in Thailand and Bulgaria.[35] One suspect was subsequently prosecuted in the Netherlands (see Section 4.1).[36]

- **'X'** (2019): On 11 February 2021, the Dutch public prosecution service announced the prosecution of an unnamed company considered as a bulletproof hosting provider, along with two individuals, for hosting the Mirai botnet and facilitating hacking by third parties (see Section 4.2). Servers were seized and wiretapped in 2019.[37]
- **DoubleVPN Service** (2021): A Dutch-led operation dismantled DoubleVPN. After using the Dutch special investigatory 'hacking power', servers were seized worldwide and replaced with a law enforcement splash page. Europol reports that DoubleVPN was heavily advertised on Russian and English-speaking cybercrime forums as a means to mask the identities of ransomware operators and phishing fraudsters. Law enforcement obtained DoubleVPN's customer database, including personal information and logs. No arrests were reported.[38]
- **ZServers/XHost** (2025): Amsterdam's Cybercrime Team seized 127 servers belonging to ZServers/XHost, which allegedly offered bulletproof hosting in the Netherlands and openly advertised anonymity for criminal activity (payments were also accepted in crypto currency). No arrests were reported at the day of seizure.[39]
- **'X'** (2025): The Dutch Cybercrime Team of 'Oost-Nederland' seized 250 servers and thousands of virtual servers from a hosting company considered a bulletproof provider, offering services related to ransomware attacks, botnets, phishing, and child abuse materials. They reportedly advertised complete anonymity and non-cooperation with law enforcement.[40]

Despite the large amounts of data seized during these operations, relatively few suspects have been arrested, and only two Dutch judgments relating to hosting providers are available for further analysis (see Sections 4.1 and 4.2).

2.3. *Expansion from cybercrime to serious organised crime*

Investigations targeting crypto communication service providers began in 2015, when Dutch and French law enforcement authorities encountered cryptophones during arrests or searches. A crypto communication service refers to an 'ecosystem' of specific applications installed on a mobile phone (a 'cryptophone'). These apps facilitate encrypted communications, including audio calls, video calls, private messaging, note-taking, and anonymous browsing.[41]

Similar to cybercriminals, organised criminals seek to maintain anonymity using cryptophones. They typically purchase devices in cash, employ pseudonyms or random identifiers, and rely on encryption that prevents interception through conventional wiretapping orders. Law enforcement authorities cannot generally obtain client data or communications from cryptophone providers with production orders, as these companies operate through resellers and maintain infrastructures that do not facilitate interception.[42]

In the same period of 2015–2025, Dutch law enforcement authorities expanded their strategy from cybercrime to serious organised crime. Cryptophone operations, here understood as a law enforcement operation targeting both crypto communication services and their users, illustrate this transformation. As of November 2025, Dutch law

[35] C. Cimpanu, Police Seize Servers of Bulletproof Provider Known For Hosting Malware Ops, Bleepingcomputer.com, 16 May 2018. https://www.bleepingcomputer.com/news/security/police-seize-servers-of-bulletproof-provider-known-for-hosting-malware-ops/ (accessed 1 February 2026).

[36] Politie.nl, Jaarverantwoording. Midden in de samenleving, 2018, p. 39.

[37] Openbaar Ministerie, OM eist 15 maanden tegen host van agressief Mirai-botnet, 11 February 2021. https://www.om.nl/actueel/nieuws/2021/02/11/om-eist-15-maanden-tegen-host-van-agressief-mirai-botnet (accessed 1 February 2026). See also P. Vermaas, Who's bad? Samen met de branche wil het Landelijk Parket malafide hostingproviders weren, Magazine Openbaar Ministerie, nr. 5, 25 November 2025. https://www.om.nl/magazine-opportuun (accessed 1 February 2026).

[38] Europol, Coordinated action cuts off access to VPN service used by ransomware groups. Takedown of DoubleVPN makes it harder for criminal hackers to cover their tracks, 30 June 2021. https://www.europol.europa.eu/media-press/newsroom/news/coordinated-action-cuts-access-vpn-service-used-ransomware-groups (accessed 1 February 2026).

[39] Politie.nl, Politie Amsterdam ontmantelt digitaal crimineel netwerk; 127 servers offline gehaald, 13 February 2025. https://www.politie.nl/nieuws/2025/februari/13/politie-amsterdam-ontmantelt-digitaal-crimineel-netwerk.html (accessed 1 February 2026).

[40] Politie.nl, Duizenden servers in beslaggenomen in omvangrijk cybercrime onderzoek, 14 November 2025. https://www.politie.nl/nieuws/2025/november/14/duizenden-servers-in-beslaggenomen-in-omvangrijk-cybercrime-onderzoek.html (accessed 1 February 2026).

[41] This definition is based on the description of cryptophones in the Dutch press release following the dismantling of the Matrix crypto communication platform. Politie.nl, Opnieuw versleutelde communicatiedienst criminelen ontmanteld, 3 December 2024. https://www.politie.nl/nieuws/2024/december/3/opnieuw-versleutelde-communicatiedienst-criminelen-ontmanteld.html (accessed 1 February 2026). This description of the working of the Matrix crypto communication platform is also used in judgments, such as the Court of Overijssel decision of 16 July 2024 (ECLI:NL:RBOVE:2024:3797). Initially, these BlackBerry devices used Pretty Good Privacy (PGP) encryption, hence the term "PGP phones"

[42] Europol, Eurojust, Common Challenges in Combating Cybercrime, Europol, The Hague, 2024, p. 11; EU Serious and Organised Crime Threat Assessment (EU SOCTA), Europol, The Hague, 2025, p. 18.

enforcement has participated in investigations into nine crypto communication services.[43] Fig. 1 provides a timeline of these operations and illustrates the volume of data collected during cryptophone operations involving Dutch law enforcement authorities.[44]

In contrast to the cybercrime operations discussed in Section 2.1 and Section 2.2, data secured during cryptophone operations is often used as evidence in cases relating to serious organised crime. The Netherlands currently has over 1700 published judgments referencing evidence obtained from crypto communication services.[46] The contents of these messages often relate to serious crimes, such as murder and drug-related offences. These messages frequently serve as crucial evidence when linked to a suspect's cryptophone. Section 4.3 and Section 4.4 will further examine the available case law relating the prosecution of the crypto communication service providers Ennetcom and IronChat, specifically in relation to the supposed complicity of crime committed by their clients.

The substantial volume of judgments in cryptophone operations, including cases reaching the Supreme Court of the Netherlands, also enables judicial scrutiny of the lawfulness of these operations and the respect of fundamental rights of the suspects. In contrast, cybercrime operations appear to prioritise stopping crime, deterring future offending, and informing victims.[47] Cybercrime operations rarely result in the prosecution of those described as 'cybercrime facilitators'.

3. Fundamental right constraints

Investigating and prosecuting communication service providers seriously interferes with fundamental rights of both service providers and their clients, such as the right to liberty and security, the legality principle in criminal affaires, the protection of private life and correspondence, and even freedom of expression. In this section we examine what fundamental rights might be affected as a result of the law enforcement strategy described in Section 2, and what constraints the European Court of Human Rights (hereinafter: ECtHR) imposes. Our analysis focuses particularly on judgments the ECtHR, because it has had several opportunities to take a stance on the fundamental rights implications of prosecuting criminal offences committed while using encrypted communication applications.

The ECtHR has recognised encryption technologies are a means of protecting the right to private life and freedom of expression.[48] According to the Court, end-to-end encryption of private communications appear to help individuals and companies to defend themselves against abuses of information technologies, such as hacking, identity and personal data theft, fraud, and the misuse of confidential information. As a result, the Court exercises caution when assessing interferences with fundamental rights resulting from measures that weaken encryption technologies.

Most of the relevant ECtHR cases relate to 'ByLock', an encrypted communication application that could be installed on smartphones, similar to WhatsApp. The application is not available anymore. In the aftermath of a failed but lethal coup d'état by members of the armed terrorist organisation FETÖ/PDY,[49] the Turkish government claimed that ByLock had been designed for the exclusive use of its members. According to the national courts, establishing of the use of ByLock was sufficient on its own to convict suspects as member of an armed terrorist group.[50] Several users of the application who were subsequently prosecuted, arrested and/or convicted, challenged their detention and/or conviction before the ECtHR.[51]

Below we first examine the extent to which a user of an encrypted communication application can be held criminally liable, with respect to fundamental rights case law. Establishing whether a user is legitimately subject to criminal prosecution is a necessary precursor to assessing any potential criminal liability - in terms of complicity - on the part of the provider of an encrypted communication service. We do not aim for an exhaustive discussion of the case law on the identified fundamental rights, but instead specifically discuss cases that are directly or indirectly related to the prosecution of communication service providers.

3.1. *(Exclusive) criminal use of an encrypted communication application*

In *Podchasov v. Russia*, the ECtHR acknowledged that criminals also use encryption technologies, which may complicate criminal investigations.[52] However, the Court has repeatedly held that this not imply that the mere use of an encrypted communication application – in this case Bylock - is a sufficient indication or evidence of criminal behaviour to justify pre-trial detention or a criminal conviction, even when a public prosecution service alleges that such an application is

[43] The operations focused on the following crypto communication platforms: Ennetcom (2016), PGP Safe (2017), Ironchat (2017), EncroChat (2020), Sky ECC (2020), ANOM (2021), Exclu (2022), Ghost (2024), and Matrix (2024). See for an overview: J.J. Oerlemans, Overzicht cryptophone-operaties, jjoerlemans.com, 13 December 2024. https://jjoerlemans.com/overzicht-cryptophone-operaties (accessed 1 February 2026).

[44] The volume of data is sometimes mentioned in Dutch press releases about these operations. It is not clear how this volume is calculated.

[45] See J.J. Oerlemans, Overzicht cryptophone-operaties, jjoerlemans.com, 13 December 2024. https://jjoerlemans.com/overzicht-cryptophone-operaties (accessed 1 February 2026).

[46] Judgments were identified as follows: On 1 February 2026, a search was conducted in the public database: https://uitspraken.rechtspraak.nl/. The search was filtered using the keywords Ennetcom (182), PGPSafe (98), IronChat (44), ANOM (85), EncroChat (648), Sky ECC (619), Exclu (37), Ghost (0), and MATRIX (10). The results were then restricted to verdicts rendered by criminal courts at first instance.

[47] At the same time, this statement can be nuanced. Law enforcement officials prioritised searches for 'threat-to-live situations' in cryptophone conversations to prevent murders and kidnappings. See, e.g., Openbaar Ministerie, Nieuwe klap voor georganiseerde misdaad, 9 March 2021. https://www.om.nl/actueel/nieuws/2021/03/09/nieuwe-klap-voor-georganiseerde-misdaad (accessed 1 February 2026). A Europol official stated 100 assassinations, kidnappings, and cases of torture were prevented in the EncroChat and Sky ECC operation alone. The Brussels Times, Dismantling of Encrochat prevented about 100 murders or kidnappings, says Europol, 21 June 2023. https://www.brusselstimes.com/encrochat-prevented-100-murders-or-kidnappings (accessed 1 February 2026).

[48] ECtHR 13 February 2024, no. 33696/19, Podchasov v. Russia, ECLI:CE:ECHR:2024:0213JUD003369619. See also J. Shurson, A European right to end-to-end encryption?, Comput. Law Secur. Rev. 2024, 106063. https://doi.org/10.1016/j.clsr.2024.106063 and O.L. van Daalen, The right to encryption: Privacy as preventing unlawful access, Comput. Law Secur. Rev. 49 (2023) 105804. https://doi.org/10.1016/j.clsr.2023.105804.

[49] FETÖ/PDY stands for "Fethullah Terrorist Organisation / Parallel State Structure". See, e.g., UK Home Office, Country policy and information note: Gülenist movement, Turkey, August 2025. https://www.gov.uk/government/publications/country-policy-and-information-note-gulenist-movement-turkey (accessed 1 February 2026).

[50] About the investigation and the data interception, see: Y. Gokce, The Bylock fallacy: An In-depth Analysis of the Bylock Investigations in Turkey, Digit. Investig. 26 (2018) 81–91. https://doi.org/10.1016/j.diin.2018.06.002.

[51] See ECtHR 22 July 2025, nos. 1595/20 and 238 others, Demirhan a.o. v. Türkiye, ECLI:CE:ECHR:2025:0722JUD000159520; ECtHR 27 August 2024, no 17389/20, Yasak v. Türkiye, ECLI:CE:ECHR:2024:0827JUD001738920 (referred to the Grand Chamber); ECtHR 19 March 2024, no. 66375/17, Parildak v. Türkiye, ECLI:CE:ECHR:2024:0319JUD006637517; ECtHR 26 September 2023, no. 15669/20, Yüksel Yalçinkaya v. Türkiye, ECLI:CE:ECHR:2023:0926JUD001566920; ECtHR 31 May 2022, 208/18, Taner Kiliç v. Türkiye, ECLI:CE:ECHR:2022:0531JUD0a00020818; ECtHR 22 November 2021, no. 19699/18, Akgün v. Türkiye, ECLI:CE:ECHR:2021:0720JUD001969918; ECtHR 7 September 2020, no. 66448/17, Baş v. Türkiye, ECLI:CE:ECHR:2020:0303JUD006644817; ECtHR 16 April 2019, no. 12778/17, Alparslan Altan v. Türkiye, ECLI:CE:ECHR:2019:0416JUD001277817.

[52] ECtHR 13 February 2024, no. 33696/19, Podchasov v. Russia, ECLI:CE:ECHR:2024:0213JUD003369619, par. 78.

exclusively used for criminal purposes.

In the case of *Akgün v. Türkiye*, the ECtHR assessed a pre-trial detention based solely on the applicant's use of ByLock. The Court found that this violated Article 5 ECHR, due to the absence of a reasonable suspicion that the applicant had committed a criminal offence at the time of his initial pre-trial detention.[53] Pre-trial detentions is lawful only if there is a reasonable suspicion that the suspect has committed a criminal offence.[54] A reasonable suspicion presupposes the existence of verifiable facts or information upon which an objective observer would be convinced that the suspect might have committed the alleged offence.[55] For example, vague references to unspecified documents cannot give rise to a reasonable suspicion justifying a pre-trial detention.[56] The mere fact that an encrypted means of communication is downloaded or used, cannot, in itself, constitute an element based on which an objective observer would conclude that criminal activity occurred. A reasonable suspicion should be supported by other evidence, such as the content of the messages or the context in which they are exchanged. The ECtHR noted that the public prosecution service had failed to substantiate the reasonable suspicion.[57]

In the case of *Yüksel Yalçinkaya v. Türkiye*, the government sought to substantiate the claim that ByLock was used exclusively for criminal purposes by referring to its technical features, including its encrypted nature, the special arrangements required to communicate with other users, the mandatory use of a VPN, and the automatic deletion of content. The applicant complained about the lack of equality of arms and argued that the application could have been used by individuals other than members of the terrorist organisation, as it was freely available via the Google Play Store for approximately two years without any control mechanisms.[58]

In its assessment of the government's contention that ByLock was used exclusively for criminal purposes, the ECtHR compares the number of downloads (100,000 times from Google Play store and 500,000 to 1 million times from APK download sites) with the number of users on the ByLock servers (215,092). The Court was also sensitive to the argument that several technical features of ByLock were found in many widely available applications. Furthermore, it referred to witness statements suggesting that ByLock may have been downloaded and used outside the strict organisational hierarchy of the terrorist organisation. Finally, the Court emphasised that the national courts should have established proof that a person had joined the network on the instructions of the terrorist organisation or, at the very least, explained why such an assessment was not considered necessary.[59] In the end, these circumstances contributed to the finding that, among other rights, the applicant's right to a fair trial had been violated.[60]

In the same case, the Grand Chamber of the ECtHR also found a violation of Article 7 ECHR.[61] The legality principle enshrined in Article 7 ECHR means that only the law can define a criminal offence and prescribe penalties. Consequently, individuals must be able to ascertain, from the wording of relevant legislation and, where necessary, with the assistance of judicial interpretation, what conduct will render them criminally liable.[62] The central question was whether the conviction of membership of an armed terrorist organisation was sufficiently foreseeable.[63] This criminal offence requires not only an organic link with the terrorist organisation (material element) but also knowledge of and intent to contribute to its activities (mental element).[64]

While the ECtHR recognises that the use of ByLock may indicate a connection with such an organisation, it stressed that intent must also be demonstrated. Although the use of ByLock is not itself a criminal offence, the national judges equated its use with knowingly and willingly being a member of a terrorist organisation, without considering the material and mental element of that offence in relation to the individual defendant. This amounted to attaching objective criminal liability to the mere use of ByLock. Such an expansive and unforeseeable interpretation of the law violated Article 7 ECHR.[65] The ECtHR confirmed this stance in a subsequent judgment involving no less than 239 applicants. In that case, the Court justified its decision by referring to the fact that some national judges explicitly indicated that it was unnecessary to wait for the submission of the decrypted ByLock content into the case file, as the establishment of the use of the application would suffice for a criminal conviction.[66] In the case of *Yasak v. Türkiye* the ECtHR reached a different conclusion, as the national court had established that the applicant had covertly engaged in activities within the terrorist organisation, used a codename, and was one of the main regional leaders of pupils within the organisation's secretive structure.[67]

3.2. Criminal liability of internet intermediaries for third party behaviour

The previously discussed cases mostly concern users of the encryption application Bylock. The ECtHR has had limited opportunities to assess the convictions of communication service providers for offences committed by their clients. In 2018, Telegram brought a case before the ECtHR challenging its conviction and the fine imposed by Russian authorities. They convicted Telegram because it refused to facilitate access

[53] ECtHR 22 November 2021, no. 19699/18, Akgün v. Türkiye, ECLI:CE:ECHR:2021:0720JUD001969918. See also the analysis in S. Royer, R. Vanleeuw, Cryptofoons, privacyvriendelijke applicaties en het vermoeden van onschuld, Tijdschr. Bijz. Strafr. Handh. 2022 (2) 90–97.

[54] Art. 5 ECHR. About the concept of reasonable suspicion in the context of post-coup state of emergency in Türkiye, see E. Turkut, S. Garahan, The 'reasonable suspicion' test of Turkey's post-coup emergency rule under the European Convention on Human Rights, Neth. Q. Hum. Rights 38 (4) (2020) 264–282. https://doi.org/10.1177/0924051920967182.

[55] ECtHR 10 December 2019, no. 28749/18, Kavala v. Türkiye, ECLI:CE:ECHR:2022:0711JUD002874918, par. 136-137.

[56] ECtHR 22 May 2014, no. 15172/13, Ilgar Mammadov v. Azerbaijan, ECLI:CE:ECHR:2019:0529JUD001517213, par. 97.

[57] ECtHR 22 November 2021, no. 19699/18, Akgün v. Türkiye, ECLI:CE:ECHR:2021:0720JUD001969918, par. 180. See also: ECtHR 19 March 2024, no. 66375/17, Parildak v. Türkiye, ECLI:CE:ECHR:2024:0319JUD006637517, par. 80-82; ECtHR 31 May 2022, 208/18, Taner Kiliç v. Türkiye, ECLI:CE:ECHR:2022:0531JUD000020818, par. 106.

[58] ECtHR 26 September 2023, no. 15669/20, Yüksel Yalçinkaya v. Türkiye, ECLI:CE:ECHR:2023:0926JUD001566920, par. 338.

[59] ECtHR 26 September 2023, no. 15669/20, Yüksel Yalçinkaya v. Türkiye, ECLI:CE:ECHR:2023:0926JUD001566920, par. 339.

[60] The ECtHR has confirmed this judgment in a subsequent case: ECtHR 22 July 2025, nos. 1595/20 and 238 others, Demirhan a.o. v. Türkiye, ECLI:CE:ECHR:2025:0722JUD000159520, par. 45.

[61] ECtHR 26 September 2023, no. 15669/20, Yüksel Yalçinkaya v. Türkiye, ECLI:CE:ECHR:2023:0926JUD001566920, par. 404 This case is not isolated. At the time, the ECtHR had over 8,000 similar applications pending on its docket involving similar complaints.

[62] The legality principle in Article 7 ECHR means that only the law can define a criminal offence and prescribe penalties. Consequently, individuals must be able to ascertain, from the wording of relevant legislation and, where necessary, with the assistance of judicial interpretation, what conduct will render them criminally liable. ECtHR 26 September 2023, no. 15669/20, Yüksel Yalçinkaya v. Türkiye, ECLI:CE:ECHR:2023:0926JUD001566920, par. 237-239.

[63] See about the principle of legality, foreseeability, and the rule of law, e.g., Z. Erent Sunko, M. Dragičević Prtenjača, The interconnection of the rule of law, European Convention on Human Rights principle of legality, and Article 7 of the ECHR, EU Comp. Law Issues Chall. Ser. 8 (2024) 54–84.

[64] ECtHR 26 September 2023, no. 15669/20, Yüksel Yalçinkaya v. Türkiye, ECLI:CE:ECHR:2023:0926JUD001566920, par. 248.

[65] ECtHR 26 September 2023, no. 15669/20, Yüksel Yalçinkaya v. Türkiye, ECLI:CE:ECHR:2023:0926JUD001566920, par. 271.

[66] ECtHR 22 July 2025, nos. 1595/20 and 238 others, Demirhan a.o. v. Türkiye, ECLI:CE:ECHR:2025:0722JUD000159520, par. 40.

[67] ECtHR 27 August 2024, no 17389/20, Yasak v. Türkiye, ECLI:CE:ECHR:2024:0827JUD001738920. This case was referred to the Grand Chamber on 16 December 2024.

to confidential private information of Telegram users by the Russian Federal Security Service. Telegram argued that the conviction and fine had amounted to an interference with its freedom to impart information as protected by Article 10 ECHR. However, the case was struck out of the list, because of Russia ceased to be party to the ECHR in 2022.[68] Below we analyse the limited existing ECtHR case law concerning the liability of internet intermediaries for criminal offences committed by users of their platforms.

In *Eurofinacom v. France*, which took place in the pre-smartphone era, the applicant company offered a data communications service that was accessible via a terminal.[69] The service could be accessed by entering a code and provided a mailbox system enabling users to communicate with one another. Users could adopt a pseudonym and add a brief description. The service should be considered a communication service *avant la lettre*.

The public prosecutor suspected that Eurofinacom was being used by sex workers to contact potential clients, which was prohibited at the time in France.[70] As a result of the investigation, both the company and its manager were found guilty of acting as an intermediary between sex workers and their clients by making the communication service available. Their guilt was established by the fact that the intercepted messages related to sex work and that several sex workers had confirmed the use of the service.

According to the ECtHR there was no doubt that the applicant company provided technical assistance that facilitated contact between sex workers and their clients by making its service available to the general public, without necessarily pursuing such aim. Furthermore, the Court found that the company should have known that facilitating contact by passively providing a means of communication could amount to criminal liability.

Two elements of the ECtHR's reasoning appear crucial to reaching this conclusion. First, the Court finds that the applicant company, as a professional operating in the communications sector, could reasonably be expected to evaluate the risks of its activity. This applied even more strongly because, under its contract with the telecommunications provider, Eurofinacom was required to monitor the service to prevent the display of information contravening the provisions of the agreement, which specifically mentioned the criminal offence of living on immoral earnings. Second, the Court considered that the manager of the Eurofinacom was aware the service was being used by sex workers to contact potential clients. The applicant company must have known that its behaviour could amount to criminal liability. Therefore, the applicant's conviction did not breach Article 7 ECHR.[71]

As regards to interferences with the right to freedom of expression, the ECtHR has accepted (shared) liability of both internet intermediaries and actual perpetrators under certain circumstances. In 2015, the ECtHR appeared to limit intermediary liability to large, professionally managed commercial internet news portals that publish their own news articles and invite readers' comments.[72] However, this position appears to have been subsequently relaxed. In fact, in *Sanchez v. France*, the Grand Chamber of the ECtHR decided that the conviction of a French politician for failing to remove a post on his Facebook profile that triggered hateful and Islamophobic reactions, did not constitute a violation of his right to freedom of expression.[73] The Court considered various elements in its proportionality assessment, such as the nature of the posts. Although politicians generally benefit from a broad interpretation of their right to freedom of expression, the ECtHR found that his Facebook posts clearly incited hatred and violence. Furthermore, by making his profile accessible to everyone, the applicant had accepted a duty of care to monitor the reactions to his posts. As a politician, he therefore carried greater responsibility than an average Facebook user.[74] It is also essential to the Court's reasoning that the authors of the post were convicted for a distinct criminal offence.[75] The case *Sanchez v. France* concerns the liability of an individual for the actions of another person in the specific context of hate speech. While its analogical relevance may be limited, the judgment demonstrates that, in certain circumstances, the ECtHR does not rule out the possibility of imposing criminal liability on intermediaries.

3.3. Interim conclusion

With the above ECtHR case law in mind, we believe the following three conclusions can be drawn.

First, the ECtHR has ruled in favour of the protection of private communications by use of encryption technology, even though this may complicate the work of law enforcement authorities. Given the importance the ECtHR attaches to the protection afforded by end-to-end encryption in the case of *Podchasov v. Russia*, we can conclude that the *mere* offering of such a service could never, in itself, amount to (criminal) liability of a provider of such a service. This is corroborated by the fact that the ECtHR insists that users of those services cannot be detained or convicted solely on the basis of their use of the service, even if a government claims that it is exclusively used for criminal purposes. In the case of both pre-trial detention and conviction, the ECtHR requires additional evidence to substantiate the (exclusive) criminal use of a service. In other words, the Court adopts a critical stance towards governments that apply a uniform and global approach to users of encrypted communication services without individualising the evidence for specific suspects. We see no reason to apply a different approach to providers of other crypto communication services.

Second, the ECtHR has stressed – in relation to membership of a terrorist organisation – that imposing objective criminal liability for using an encrypted communication service is incompatible with the Convention. The mental element, namely at least the knowledge that one's participation will contribute to achieving the criminal aim of the organisation, must be demonstrated by the prosecution. This presumes that the accused has knowledge of the organisation's activities and that the prosecution establishes proof of intent. By analogy, this requirement should also apply to providers suspected of complicity in a specific crime committed by a user of an encrypted communication service, or of membership of a criminal organisation by offering such services. This does not, of course, preclude the possibility of prosecuting providers for distinct criminal behaviour, such as money laundering or tampering with evidence. When it comes to proving a provider's knowledge, it is

[68] ECtHR, no 13232/18, Telegram Messenger LLP and Telegram Messenger Inc. v. Russia. See also Council of Europe, Russia ceases to be party to the European Convention on Human Rights, Strasbourg, 16 September 2022. https://www.coe.int/en/web/portal/-/russia-ceases-to-be-party-to-the-european-convention-on-human-rights (accessed 1 February 2026).

[69] ECtHR 7 September 2004, no. 58753/00, Eurofinacom v. France, ECLI:CE:ECHR:2004:0907DEC005875300.

[70] Art. 225-6 of the French Criminal Code.

[71] See, cf., C. Ovey, Human rights: Article 6 – right to a fair trial – alleged entrapment by state official, Crim. L.R. (2005) 133–136.

[72] This case concerned civil, not criminal liability. ECtHR 16 June 2015, no. 64569/09, Delfi AS v. Estonia, ECLI:CE:ECHR:2015:0616JUD006456909; L. Brunner, The liability of an online intermediary for third party content: The watchdog becomes the monitor: Intermediary liability after Delfi v Estonia, Hum. Rights Law Rev. 16 (1) (2016) 163–174.

[73] ECtHR 15 May 2023, no. 45581/15, Sanchez v. France, ECLI:CE:ECHR:2023:0515JUD004558115; ECtHR 2 September 2021, no. 45581/15, Sanchez v. France, ECLI:CE:ECHR:2021:0902JUD004558115; K. Lemmens, Freedom of expression on the Internet after Sanchez v France: How the European Court of Human Rights accepts third-party 'censorship', Eur. Conv. Hum. Rights Law Rev. (2022).

[74] ECtHR 15 May 2023, no. 45581/15, Sanchez v. France, ECLI:CE:ECHR:2023:0515JUD004558115, par. 189.

[75] ECtHR 15 May 2023, no. 45581/15, Sanchez v. France, ECLI:CE:ECHR:2023:0515JUD004558115, par. 202-203.

important to note that contemporary communication service providers offering end-to-end encryption are technically unable to access the exchanged content. This contrasts with the provider in *Eurofinacom*, who was, or should have been, aware of message content because of its contractual obligation to monitor communications. Consequently, in the case of crypto communication service providers, knowledge of users' criminal behaviour must be inferred from other circumstances, which may complicate the prosecution's burden of proof.

Third, the ECtHR accepts that imposing criminal liability on intermediaries does not necessarily entail a violation of Article 10 ECHR. This was illustrated by the case of *Sanchez v. France*. Moreover, from the *Eurofinacom* case we can conclude that, to a certain extent, the ECtHR accepts stricter duties of care when assessing criminal liability of communication service providers in relation to their clients' behaviour. In its case law, the Court considers whether the intermediary was notified or aware of the criminal behaviour. When attributing criminal liability, the Court even takes into account the contractual obligations imposed on the provider. This can lead to a situation where, even if a provider had no actual knowledge of criminal behaviour, it should have had such knowledge. We observe that, since the ECtHR takes into account contractual obligations, the increasing number of legal obligations for communication service providers arising from both national and EU legal provisions could be relevant to questions of criminal liability.

On a European Union level, there is a noticeable trend of enhanced due diligence obligations for communication service providers. Communications service providers are often regulated under the Digital Services Act (DSA), which comes with its own enforcement mechanisms.[76] The DSA imposes stricter requirements on communications service providers to monitor and moderate illegal content, as well as to cooperate with data production orders and take-down requests from law enforcement authorities.[77] Regulations under the DSA bear notable similarities to KYC procedures in the financial sector, which also require identity verification. Anti-money laundering measures should be considered when communication service providers allow payments in cryptocurrencies such as Bitcoin, as this pseudo-anonymous cryptocurrency may pose heightened risks for money laundering.[78]

4. Case law analysis

This section examines the potential criminal liability of two (suspected) bulletproof hosting providers and two crypto communication service providers. As explained in Sections 1 and 2, our analysis focuses on Dutch judgments, as the law enforcement strategy to target these providers and collect large volumes of data originated in the Netherlands. Over the ten-year period of 2015–2025, only four cases resulting judgments are publicly available for further analysis. A broader analysis of these cases in light of the findings of the fundamental rights case law is discussed in Section 5.

4.1. Maxided

In 2019, the Court of Rotterdam convicted a 29-year-old Moldovon national for money laundering.[79] The court found that the defendant's salary - amounting to €537,494 - constituted illicit proceeds because it was paid by companies engaged in illegal activities, including copyright infringement and cybercrime.[80] The suspect had also admitted to these crimes. He was ultimately sentenced to five months' imprisonment for money laundering. Initially, however, the Dutch police had arrested him on suspicion of participating in criminal activities by providing infrastructure to offenders and hosting child sexual abuse material (CSAM) and malware.[81] These allegations formed the basis for charges of co-perpetration and complicity, but the court acquitted him of those offences.

The public prosecutor initially demanded a five-year prison sentence and also prosecuted the suspect for: (a) the distribution of CSAM, and (b) complicity in distributing CSAM by providing technical infrastructure (servers) for the company Maxided and failing to remove illegal content after being notified.[82] The public prosecutor argued that the defendant acted with intent, at least in the form of conditional intent, regarding the distribution of CSAM. According to the prosecutor, the defendant knew, or at least consciously accepted the substantial risk, that CSAM would be distributed through the companies' servers. The prosecutor also contended that the defendant made a profession and habit of hosting CSAM.

In the court's view, the files contained no direct evidence that the defendant knew CSAM was exchanged by users of Maxided, let alone that he actively engaged with them. The defendant claimed that whenever he encountered CSAM, he reported it to his employer, who was responsible for handling abuse reports. The court observes that conditional intent (*dolus eventualis*) requires (under Dutch law) that the defendant was aware of the substantial risk that the consequence would occur and consciously accepted that risk at the time of the act.[83] There is no evidence that the defendant consciously accepted that risk; his statement to the police that the company involved hosted illegal software and adult pornography does not support such a conclusion, nor is there evidence that he handled abuse reports concerning CSAM. Accordingly, conditional intent is also absent. The court therefore concludes that the defendant must be acquitted of both the primary charge (co-perpetration) and the subsidiary charge (complicity).

[76] See Art. 56 Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, OJ L, 2024/1385. These enforcement mechanisms are in the hands of individual member states or, for very large online platforms, the European Commission.

[77] See Art. 9 DSA and art. 10 DSA.

[78] See, cf., N. Vandezande, Virtual currencies under EU anti-money laundering law, Comput. Law Secur. Rev. 33 (3) (2017) 341–353. https://doi.org/10.1016/j.clsr.2017.03.011; C. Wronka, Money laundering through cryptocurrencies – analysis of the phenomenon and appropriate prevention measures, J. Money Laund. Control 25 (1) (2022) 79–94.

[79] Court of Rotterdam 29 April 2019, ECLI:NL:RBROT:2019:8067.

[80] Although the defendant did not control the companies' overall revenues, his receipt and use of salary payments via ePayments satisfied the elements of money laundering under Article 420bis of the Dutch Criminal Code. The habitual nature of these transactions over several years justified classification as habitual money laundering under Article 420ter).

[81] Politie.nl, Jaarverantwoording. Midden in de samenleving, 2018, p. 39. https://www.politie.nl/jaarverantwoording (accessed 7 December 2025). Interestingly, seized servers were analysed by academics who stated that Maxided was a 'major bulletproof hosting provider', because they allowed their clients host criminal activities in support of various type of cybercrime such as phishing, botnets, DDoS, spam, and counterfeit pharmaceutical websites. See A. Noroozian, et al., Platforms in everything: Analyzing ground-truth data on the anatomy and economics of bullet-proof hosting, in: Proc. 28th USENIX Security Symp. (USENIX Security 19), 2019, pp. 1341–1356).

[82] These acts were then criminalised under Art. 240b Dutch Criminal Code (currently under Art. 252 of the Dutch Criminal Code) and complicity is regulated in Art. 48 Dutch Criminal Code.

[83] See further about conditional intent within the Dutch criminal law system, J. de Hullu, P.H.P.H.M.C. van Kempen, Materieel strafrecht: Over algemene leerstukken van strafrechtelijke aansprakelijkheid naar Nederlands recht, ninth ed., Wolters Kluwer, 2024, pp. 260–269. See in comparison with other legal systems: J. Keiler, Actus reus and participation in European criminal law (doctoral thesis), Maastricht University, Intersentia, Maastricht, 2013, p. 281 and J.H. Blomsma, Mens rea and defences in European criminal law (doctoral thesis), Maastricht University, 2012. https://doi.org/10.26481/dis.20121011jb.

4.2. Bulletproof hosting provider 'X'

On 21 February 2025, the Court of Rotterdam convicted the director and shareholder of an undisclosed hosting provider for complicity in computer crimes.[84] In particular, the court determined that the defendant facilitated a botnet infrastructure for the Mirai malware. Mirai malware infects devices and incorporates them into a botnet, i.e., a network of compromised devices controlled by an individual via a command-and-control server. The court noted that botnets enable various forms of cybercrime, including hacking, malware distribution, and DDoS attacks.

The defence argued that the defendant should be acquitted because he did not act with intent, not even in the form of conditional intent, to assist in committing computer hacking or in offering and/or possessing a Mirai botnet. It was submitted he acted to the best of his ability. In August 2019, when the number of abuse reports became overwhelming, it was argued that the defendant and his co-defendant set up an automated system to respond to abuse reports and also attempted to address such reports directly to the best of their ability.

The court found that servers and IP addresses belonging to the hosting company 'X' hosted a Mirai botnet and facilitated computer intrusion. The court explains that - to establish complicity - it must be proven that the defendants' intent was directed not only at providing servers and IP addresses, but also at the underlying offences: computer hacking and hosting/distributing the Mirai botnet. To establish this, the court took into consideration that providers are expected to act on abuse reports under the Dutch 'Abuse Platform Code of Conduct', which requires proactive measures to prevent misuse. Despite being aware of this code, the defendants failed to comply. Evidence shows they knew their servers were misused, that a Mirai botnet and its servers operated within their network, and that their IP block was blacklisted. They received 8012 abuse emails in the period between 18 March 2019 and 1 October 2019, including 138 specifically mentioning Mirai.

Yet, the defendants sent only standard responses to abuse emails, and some reports could not be delivered because their inbox was full. Furthermore, investigation into the customers of the unnamed hosting provider revealed that they were able to purchase services without providing authentic contact details. For example, customers used email addresses whose composition was linked to services or activities commonly associated with cybercriminals, could pay pseudonymously via Bitcoin, and provided fictitious physical addresses such as "420 Hacktown".

Moreover, communications revealed that the defendants knowingly tolerated botnets when they were concealed, even providing instructions on how to obfuscate 'malware binaries' - executable malicious files - to evade detection by security systems. A Skype log shows a co-defendant stating he "doesn't care about abuse". Furthermore, when asked by an undercover officer whether they reviewed abuse reports, the company admitted they did not. A customer also recommended the company as a "bulletproof hoster" for Mirai.

Given these circumstances, the court concluded that the defendants consciously accepted the substantial risk (i.e., conditional intent) that their infrastructure would be used to host a Mirai botnet and facilitate computer hacking. Consequently, the court found the defendant guilty of co-perpetrating the aiding and abetting of computer trespass, as well as the aiding and abetting the co-perpetration of the possession and distribution of a Mirai botnet, by providing the necessary means to execute these crimes. The suspect was convicted of 174 h of community service and received a conditional sentence of four months' imprisonment, subject to a two-year probation period during which they must not commit further offences.[85]

4.3. Ennetcom

On 21 September 2021, the founder of the company that provided Ennetcom cryptophones was convicted of directing a criminal organisation, money laundering, forgery and illegal possession of weapons. The defendant was sentenced to 54 months' imprisonment.[86]

The court explained that the company supplied Ennetcom cryptophones, which allowed users to send encrypted text messages via BlackBerry devices. These messages were automatically deleted after 24 or 48 h, and a helpdesk could remotely erase the contents of a phone at the user's request ("wiping").[87]

The defendant argued that, similar to a general goods store that cannot be blamed for selling a knife later used in a murder, he should not be held responsible for selling a product that enabled others to keep their communications secret, even if a few customers misused it. The Court of Rotterdam emphasised that developing, offering, and selling such phones is *not*, in itself, an illegal activity. However, liability arises when such phones are used exclusively or predominantly by individuals seeking to obstruct the detection of crimes they have committed or intend to commit, provided that such a purpose was known within the organisation.

The court found that this purpose was known by the defendant, who directed the criminal organisation. The fact that he remotely erased data from phones upon request contributed to the conclusion that he knew the products and services were paid for by individuals engaged in criminal activities.

The court further noted that Ennetcom facilitated complete user anonymity (by not registering personal data, assigning anonymous usernames, and accepting cash payments) and implemented a modified retention policy (automatic deletion of messages after 24 or 48 h). It further found it relevant that the defendant attempted to discover the methods used by the Netherlands Forensic Institute (NFI) to decrypt phones. Taken together, these factors demonstrated that the company developed a product that was attractive to criminals and intended particularly for them. According to the court, offering such a product makes proper administrative recording of buyer details and non-cash payment - i.e., KYC policies - all the more necessary, yet these measures were not implemented.

4.4. IronChat

On 12 September 2024, the Court of Gelderland convicted a 52-year-old man of directing a criminal organisation whose objectives included providing a crypto communication service to other criminal organisations and laundering the proceeds generated through this activity. He

[84] Court of Rotterdam 21 February 2026, ECLI:NL:RBROT:2025:2488. A co-defendant, who was responsible for sales and customer contacts within the company was sentenced to 240 h of community service and a conditional prison sentence of six months (Court of Rotterdam 21 February 2026, ECLI:NL:RBROT:2025:2492).

[85] He was sentenced to four months of imprisonment (reduced due to the trial's length), a community service order of 180 h, and a probation period of two years.

[86] Court of Rotterdam 21 September 2021, ECLI:NL:RBROT:2021:9085 (annotated by J.J. Oerlemans). Co-defendants were also prosecuted and convicted by the Court of Rotterdam on 21 September 2021 (ECLI:NL:RBROT:2021:9086 and ECLI:NL:RBROT:2021:9087).

[87] See for more background: H. Modderkolk & T. Kreling, Zorgen voor criminelen nu justitie versleutelde PGP-berichten kan lezen, *De Volkskrant*, 10 March 2017. https://www.volkskrant.nl/wetenschap/zorgen-voor-criminelen-nu-justitie-versleutelde-pgp-berichten-kan-lezen~b098bf7f/ (accessed 5 December 2025) and B.W. Schermer, J.J. Oerlemans, AI, strafrecht en het recht op een eerlijk proces, Comput. Recht 2020 (3) (2020) 14–21.

was sentenced to 4,5 years' imprisonment.[88]

IronChat was a crypto communication system designed to transmit encrypted messages utilising the Off-The-Record (OTR) messaging encryption protocol. The application, compatible with mobile devices and laptops, incorporated features that are now common, such as the ability to erase messages immediately upon receipt, a 'panic mode' for complete content deletion via a single command, and a function to crash the device and wipe all data through the command "CRASHME!".

The defence argued that the defendant should be acquitted because it could not be proven that the organisation had the intent to commit the offences listed in the indictment, and due to a lack of lawful and convincing evidence that he was aware of the criminal organisation's objectives.

The court determined that the communication method and application were created with the intention of maintaining communication confidentiality and providing maximum anonymity to clients. Consequently, when the devices and associated applications, subscriptions, and laptops were sold, no personal identification details were recorded beyond pseudonyms. Furthermore, the court noted that approximately 90% of all credit transfers were cash deposits. Even after the bank notified that such unusual transactions were unacceptable, they failed to take appropriate action. The defence was unable to substantiate claims of legitimate use by other parties, such as politicians and actors.

The court concluded that the evidence demonstrated that a substantial proportion of the company's clientele comprised individuals engaged in criminal activities, and that the defendant was aware of this fact. The court reached this conclusion based on intercepted communications from wiretapping, physical observations, and IronChat conversations. Furthermore, the court found that there was close and deliberate cooperation between the suspects regarding the deletion of accounts upon user request. Finally, the court determined that the accused maintained frequent contact with the leader of a criminal organisation involved in drug trafficking.

Consequently, the defendant was found guilty of participating in a criminal organisation by providing its members with the IronChat application, with full knowledge that the organisation's intent was to engage in criminal activities.

5. Reflection

When comparing the case law analysis in Section 4 with the fundamental rights constraints in Section 3, the following observations can be made.

The ECtHR ruled that the *mere* offering of an encrypted communication service does not, *in itself*, amount to criminal liability for the provider. As shown in the case law analysis, this principle is upheld in Dutch courts. However, in both cryptophone cases, directors of these cryptophone companies were sentenced for directing a criminal organisation. The courts took into account the fact that they facilitated complete user anonymity by not registering personal data, assigning anonymous usernames, and accepting cash payments. The public prosecutor had to prove that the defendants knew these phones were provided to criminals. This aligns with the ECtHR's requirement that the prosecution must establish proof that the accused had knowledge of the criminal organisation's activities. Imposing objective criminal liability for the use of an encrypted communication service is indeed incompatible with the ECHR.

As a result, the burden of proof extends beyond demonstrating the material elements of a criminal offence (*actus reus*) to establish intent in forms of participation of crime by providing the means to commit offences to third parties. It also requires proof of the perpetrator's criminal intent (or mental element of the crime (*mens rea*)).[89] In the context of a bulletproof hosting provider or crypto communication service provider, the *actus reus* typically relates to the physical act of providing the technical means to commit crime (e.g., servers and applications). Criminal intent can, for example, be demonstrated through communications with clients or advertisements on criminal marketplaces. As a Dutch public prosecutor explained in an interview: they must prove both that the hosting provider knew its client would commit a crime and that the provider actively aided the client in committing that crime.[90] The case law analysis demonstrates that public prosecution services should substantiate their claims with evidence demonstrating the provider's intent to facilitate crimes committed by their clients.

What is required to establish this type of intent can be different across EU countries, depending on the specifics of national criminal law. The cases of Maxided and hosting provider 'X' illustrate how Dutch courts approach this question. In Maxided, the public prosecutor failed to provide direct evidence that the defendant knew CSAM was exchanged by clients, let alone that he actively engaged with them. In contrast, in the case of hosting provider 'X', the prosecutor proved that the defendants' intent was directed not only at providing servers and IP addresses to cybercriminals but also at facilitating underlying offences: hosting the Mirai botnet and computer hacking. The evidence included activities such as: (a) systematically ignoring abuse reports, (b) permitting pseudonymous registrations, and (c) accepting Bitcoin payments without verifying customer identities. Based on these circumstances, the court concluded that the defendants consciously accepted the substantial risk that their infrastructure would be used for hosting a Mirai botnet and facilitating computer hacking.

Differences exist between national criminal laws regarding complicity and the required intent exist due to a lack of harmonisation at EU or international level. However, Article 5 of the UN Convention against Transnational Organised Crime provides a common legal definition of membership of a criminal organisation.[91] This provision allows for the prosecution of otherwise legal activities, such as providing crypto communication services, if the perpetrator knew that their actions would contribute to achieving the criminal aims of the organisation. In this respect, the burden of proof for membership of a criminal organisation is lower than that for complicity or aiding and abetting, which require proof of knowledge of a specific criminal offence. This was demonstrated in the German Cyberbunker judgment, where the defendants were found guilty of membership of a criminal organisation but were acquitted in the specific crimes committed by their clients (as discussed in Section 2.2).

Finally, the analysis of national case law highlights the growing relevance of KYC procedures and anti-money laundering measures in establishing criminal liability. Our analysis indicates that evidence of criminal intent can be inferred from a deliberate lack of due diligence by the provider, even even in the absence of strict legal obligations. This

[88] Court of Gelderland 12 September 2024, ECLI:NL:RBGEL:2024:6732. See also J.J. Oerlemans, Meer duidelijkheid over de Ironchat-operatie, https://jjoerlemans.com/meer-duidelijkheid-over-de-ironchat-operatie/, 20 February 2023 (accessed 1 February 2026).

[89] G.P. Fletcher, Basic concepts of criminal law, Oxford University Press, New York, 1998, pp. 43–58. See also, e.g., J. Keiler, Actus reus and participation in European criminal law (doctoral thesis), Maastricht University, Intersentia, Maastricht, 2013, p. 7. The actus reus is also classified as the objective or tangible side of a person's conduct. The mens rea is describes the intangible, subjective side of a person's conduct, such as their state of mind or criminal intent.

[90] P. Vermaas, Who's bad? Samen met de branche wil het Landelijk Parket malafide hostingproviders weren, Magazine Openbaar Ministerie, nr. 5, 25 November 2025. https://www.om.nl/actueel/nieuws/whos-bad-cybercrime-opportuun (accessed 5 December 2025). This is called 'double intention' by the public prosecutor. See J. Keiler, Forms of participation, in: J. Keiler, D. Roef (Eds.), Comparative Concepts of Criminal Law, Intersentia, Cambridge, Antwerp, Chicago, 2019, p. 315.

[91] Cf. Article 5 § 1 (a)(i)(ii), (b)(i)(ii) and § 2 of the United Nations Convention against Transnational Organized Crime 2004.

includes instances of inadequate customer administration (cf. KYC practices), a failure to implement anti-money laundering measures, and the systematic ignoring of abuse notifications and law enforcement requests.

In that respect, it remains to be seen how recent regulations for digital platforms interact with criminal law. A failure to comply with the stricter compliance obligations of the Digital Service Act could not only lead to sanctions based on the DSA, but also to criminal liability. We have already identified how (deliberate) compliancy failures are being taken into consideration to establish criminal intent.

6. Conclusion

In this article, we examined how fundamental rights constrain the law enforcement strategy that targets communications service providers as crime facilitators. In Section 2, we explained how the challenges of anonymity, encryption and jurisdiction in cybercrime investigations led to a shift from reactive to pro-active investigations. As a result of these challenges, law enforcement authorities adopted an intelligence-driven (also called 'data-driven') approach. This involves collecting large amounts of data with objectives broader than the mere prosecution of individuals, in an attempt to combat cybercrime more effectively. Stopping crime, deterring future offending, as well as notifying victims seems, now to be as important as the prosecution of crime.

We also showed how this law enforcement strategy, initially developed in the Netherlands as a response to cybercrime, has broadened its scope to include serious crime and is increasingly being adopted by other law enforcement authorities within the European Union and Europol. This expansion was illustrated by the analysis of cryptophone investigations. These operations targeting crypto communication providers led to a substantial volume of judgments, which enabled judicial scrutiny of the lawfulness of these operations and the protection of fundamental rights of suspects. In contrast, cybercrime operations appear to prioritise stopping crime, deterring future offending, and informing victims. Because these cybercrime operations rarely result in the prosecution of those identified as 'cybercrime facilitators', their lawfullness is seldom subject to meaningful judicial scrutiny.

This article focused on the challenges under criminal substantive law when prosecuting communications service providers as co-perpetrators of crime. The fundamental rights analysis in Section 3 demonstrated that mere provision of an encrypted communication service does not, in itself, establish criminal liability for the provider. To impose criminal liability, both the material elements of a criminal offence and the requisite criminal intent must be proven. This does not preclude the possibility of prosecuting providers for distinct criminal behaviour, such as money laundering or tampering with evidence.

Both public prosecutors and defence lawyers can draw lessons from the judgments examined in Section 4. Public prosecutors must present substantive evidence regarding both the material elements of the alleged offences and the requisite criminal intent. The case law demonstrates that proving complicity via aiding and abetting crimes committed by clients is not straightforward. Prosecutors must demonstrate not only the underlying offences but also that the provider intended to assist in their commission. Our analysis indicates that the criminal intent of hosting providers and crypto communication services may be partially inferred from a failure to act following notifications of illegal content, the inadequate administration of cash deposits or cryptocurrency transactions, and poor customer due diligence (cf. KYC practices). Consequently, this finding indicates that the failure to adhere to these compliance obligations can lead to criminal liability.

The relevance of these findings depend, however, on the specific offences and the applicable legal frameworks in jurisdictions. Further research exploring the intersection between due diligence obligations of communication service providers and substantive criminal law would be valuable. Accordingly, a doctrinal analysis of the various modes of criminal participation is recommended, specifically within the legal systems of those states that actively employ this prosecution strategy: namely the Netherlands, France, Germany and Belgium.

In this context, the ongoing proceedings against Pavel Durov in France warrant close attention. It is essential to distinguish Telegram from the significaly smaller bulletproof hosting providers and crypto communication service providers discussed in this article. The proportion of criminal activity on Telegram, relative to its user base, will likely differ from providers allegedly targeting criminals exclusively. Consequently, establishing the requisite mens rea for prosecution, specifically regarding co-perpetration and complicity, will present evidentiary hurdles.

Therefore, continued scrutiny of cases such as the one involving Pavel Durov is essential. This must be paired with doctrinal analysis of criminal participation within these jurisdictions to fully understand the scope and limitations of prosecuting communication service providers as facilitators of crime.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.