NJECL

*Bridging the Regulatory Disconnection Between Data Collection and Data Analysis in Criminal Investigation*

# The future of data driven investigations in light of the Sky ECC operation

New Journal of European Criminal Law
2023, Vol. 0(0) 1–25

DOI: 10.1177/20322844231212661
journals.sagepub.com/home/nje
Sage

**Jan-Jaap Oerlemans**
Utrecht University, The Netherlands

**Sofie Royer**
KU Leuven, Belgium

## Abstract

The Sky elliptic-curve cryptography (Sky ECC) operation is a prime example of a data driven investigation. The collection of approximately 1 billion messages from 70,000 phones paved the way for hundreds of criminal investigations, resulting in numerous convictions in the Netherlands and Belgium alone. This article addresses how the Sky ECC operation interferes with the right to privacy and the right to a fair trial. We examine whether or not, and on what terms, there is a future for data driven criminal investigations. Our main research question is therefore how data driven criminal investigations can be (better) regulated in order to be in line with case law of the European Court of Human Rights. To answer the research question, the main characteristics and legal criteria for data driven investigation are identified. These criteria derived from the right to privacy and the right to a fair trial. Finally, we examine the impact of a violation of these criteria for the use of evidence in criminal proceedings. The research uncovers a disconnection between data protection regulations and criminal procedural law. It highlights that practitioners concentrate primarily on the collection phase, governed by criminal procedural law, whereas the most urgent questions relate to the respect of data protection law and the right to a fair trial. This finding suggests an ongoing discourse relating to the transparency of data driven criminal operations like Sky ECC and the need to address concerns regarding the reliability of evidence.

## Keywords

data driven criminal investigation, Sky ECC, fair trial, right to privacy, grey infrastructure, reliability, exclustion of evidence

**Corresponding author:**
Jan-Jaap Oerlemans, Utrecht University, Newtonlaan 231, Utrecht 3584 CS, The Netherlands.
Email: j.j.oerlemans@uu.nl

## Introduction

Sky ECC was a subscription-based messaging application that ran on modified Nokia, Google, Apple, and BlackBerry phones. The phones were supplied by Sky Global, the company behind Sky ECC.[1,2] Like other cryptophones, Sky ECC's primary purpose was to facilitate secure communication between subscribers by use of applications that utilise strong encryption. The cameras, microphones, and GPS were disabled, making it impossible to make regular phone calls with a Sky ECC phone.

Worldwide, approximately 170,000 individuals used the tool, which had its own infrastructure and applications and was operated from the United States and Canada, using computer servers based in France. On a global scale, around three million messages were exchanged each day via Sky ECC. Over 20 percent of the users were based in Belgium and the Netherlands.[3]

In mid-February 2021, law enforcement authorities were able to monitor the information flow of approximately 70,000 users of Sky ECC. On 9 March 2021, the service was shut down after a joint operation by French, Belgian, and Dutch law enforcement authorities, known as 'Operation Argus'. The operation led to the interception of approximately 1 billion messages, which were later used as evidence in criminal investigations and for intelligence purposes.[4]

While the operation received much media attention, it was not the first operation targeting cryptophone companies and their users. Other examples are the investigations into Ennetcom, PGP Safe, IronChat, EncroChat, and ANOM cryptophones.[5] We refer to these operations as 'data-driven criminal investigations'. A data-driven criminal investigation involves the processing of data that has been collected by law enforcement authorities in an earlier phase, which is then enriched, and linked with other data for future investigations.[6]

In other words, the Sky ECC operation was not the first data-driven criminal investigation and it will most certainly not be the last one. We expect similar operations to be carried out in the future,

1. Prof. dr. Jan-Jaap Oerlemans is an endowed professor of Intelligence and Law, affiliated to the Willem Pompe Institute for Criminal Law and Criminology, Utrecht University, The Netherlands. He is also a senior researcher at the Dutch Review Committee for Intelligence and Security Services (CTIVD).
2. Dr. Sofie Royer is a research expert at the Centre for IT and IP Law, affiliated to the Institute of Criminal Law, both KU Leuven, and a guest professor at UAntwerpen and ULiège.
3. Europol, 'New major interventions to block encrypted communications of criminal networks' (*Europol*, 10 March 2021), <www.europol.europa.eu> accessed 1 October 2023.
4. This number is mentioned by Belgian law enforcement officials. See, e.g., Leon van Poppel, 'Waarom criminelen een berichtendienst gebruiken zoals Sky ECC' (*RTL Nieuws*, 10 March 2021) < https://www.rtlnieuws.nl/nieuws/nederland/artikel/5219062/sky-ecc-berichten-criminelen-encryptie> accessed 1 October 2023; H Lyons, 'Cracking of encrypted messaging service dealt major blow to organised crime' (*The Brussels Times,* 9 March 2021) < https://www.brusselstimes.com/159039/cracking-of-encrypted-text-messaging-service-sky-ecc-app-dealt-major-blow-to-organised-crime> accessed 1 October 2023; S Drommen and D Hiroux, 'Politie na "grootste actie ooit" in ons land: "Tonnen cocaïne, corruptie tot in alle lagen van de maatschappij"' (*vrt nws*, 9 March 2021) < https://www.vrt.be/vrtnws/nl/2021/03/09/huiszoekingen-200-1500-agenten/> accessed 1 October 2023.
5. See, for an overview of these operations in which Dutch law enforcement authorities were involved: J J Oerlemans, 'Overzicht cryptophone-operaties' (*jjoerlemans.com*, 14 November 2022) <https://jjoerlemans.com/2022/11/14/overzicht-cryptophone-operaties/> accessed 1 October 2023.
6. We derive this concept from the following paper: E van de Sandt, A van Bunningen, J van Lenthe, and 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 M F H Hirsch Ballin and J J Oerlemans, 'Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden' (2003) DD 18-38.

focusing on communication service providers such as VPN services, cryptocurrency-mixing platforms, and hosting providers. As these types of operations are a fairly new phenomenon, specific legal safeguards are often not yet in place. The bulk collection of communication data, however, tends to significantly interfere with several human rights, most notably the right to privacy (Article 8 of the European Convention on Human Rights (ECHR)). Furthermore, it is not yet clear what degree of transparency and access should be provided to the defence to ensure the right to a fair trial in criminal proceedings (Article 6 ECHR) and what consequences this may have for the use of data as evidence in criminal cases. These questions are relevant due to the hundreds of cases that have arisen and that are still expected to arise as a result of the Sky ECC operation and future similar investigations.

Our main research question is, therefore, *how data-driven criminal investigations can be (better) regulated in order to be in line with case law of the European Court of Human Rights (ECtHR)*. We will address this main research question by way of four sub-questions. The Sky ECC operation serves as a case study throughout the article. As far as it is available, we will incorporate references to the relevant case law in Belgium and in the Netherlands.

1. What are the facts of the Sky ECC operation, insofar as they are relevant for the right to privacy and the right to a fair trial?
2. What are the main characteristics of data-driven investigations, how should they be delineated from the activities of intelligence services and how do they relate to grey infrastructures?
3. What criteria for data-driven investigations can be derived from the right to privacy and the right to a fair trial?
4. What is the impact of a violation of these rights for the use of evidence in criminal proceedings?

In most countries, the collection of data is largely regulated as an investigative power, although the applicable rules are not always tailored to the characteristics of data-driven criminal investigations. The subsequent analysis of data has not received much attention in case law or elsewhere, despite the existence of European data protection rules and rules on the right to a fair trial. In this article, we will therefore highlight this disconnection between the collection of data and analysis of data, with regard to data protection regulations and the right to a fair trial.

## The Sky ECC operation

Sky ECC phones offered functionalities for encrypted e-mail, instant chats, instant group chats, notes, voicemail, images, and messages that were automatically destroyed after a certain period of time. The phones also had several features, including a 'distress password' and a 'kill switch', that allowed users to (remotely) wipe all data on the device. Making phone calls was not possible with a 'Sky phone'. To further promote anonymity, the phone did not use regular phone numbers to send messages to other phones. Instead, every user was assigned a user identifier (called 'Sky-ID'), which consisted of a unique combination of six characters (numbers and letters). In order to communicate with other Sky ECC phone users, they had to store these Sky-IDs as contacts. The phones were sold completely anonymously and only for cash. A subscription to use the Sky ECC applications was expensive compared to regular mobile phones. It would cost clients up to € 2,200 a year or € 600 every three months.

In the next three sub-sections, we discuss the start of the operation into Sky ECC, how the messages were collected by law enforcement authorities and how they are analysed for criminal investigations.[7] Understanding these intricacies is crucial, as they shed light on their impact on fundamental rights, particularly the right to privacy and the right to a fair trial.

## *Start of the investigation*

Already in 2015, Dutch and French law enforcement authorities found in multiple criminal investigations that individuals engaged in plotting and committing serious crime were using Sky ECC phones. After some years, they decided to start a criminal investigation to gain more insight in criminal organisations in which individuals used these cryptophones.

In 2018, Belgian law enforcement authorities started an investigation into the Sky ECC phones they increasingly encountered during drug investigations. An investigation was initially launched against Sky ECC for their membership of a criminal organisation because their services were actively aimed at thwarting law enforcement authorities.[8] Later, it became clear that probably the actual goal, and most certainly the result, of the operation was not to prosecute the individuals behind Sky ECC itself, but to obtain insight in the criminal activities carried out in Belgium and beyond and to prosecute individuals operating from Belgium and neighbouring countries.[9]

Around the same time, Dutch and French law enforcement officials also found that servers facilitating these encrypted communications were located at the hosting service provider 'OVH' in Roubaix, France. Subsequently, Dutch law enforcement authorities issued European Investigation Orders (EIOs) to France on 6 December 2018. They requested French law enforcement authorities to create an image of the Sky ECC servers. The goal of the EIOs was to reveal the technical setup of the servers and prepare for further investigation by use of wiretapping and the decryption of data. Belgium independently sent a similar EIO to France on 21 November 2018.

The French authorities executed the EIO's and gained access to the IT infrastructure of the Sky ECC servers, allowing them to conduct a preliminary investigation. As a result of this investigation, on 13 February 2019, the French prosecutor at the Lille court initiated a formal investigation into Sky ECC. As part of this investigation, on 14 June 2019, the prosecutor sought and obtained permission from the French court to intercept, record, and transcribe communications passing through the Sky ECC servers.

On 24-26 June 2019, the IP traffic at two servers at OVH was wiretapped by French law enforcement authorities (the main server and a back-up server). Dutch law enforcement authorities

7. The reconstruction of the Sky ECC operation in this section is based on the description of facts in the following cases: Court of Amsterdam 21 November 2022, ECLI:NL:RBAMS:2022:6816, and Court of Gelderland 20 December 2022, ECLI:NL:RBGEL:2022:7425, ECLI:NL:RBGEL:2022:7440 and 11 April 2023, ECLI:NL:RBGEL:2023:2011. See also, J J Oerlemans, 'Meer details bekend over SkyECC-operatie' (2022) Computerrecht 384-385. In this case law, courts often cite from "letters" – dated 30 April 2022 and 2 June 2022 – from the Public Prosecution Service sent to the defence about the events of the operation. These "letters" contained appendixes listing police reports and other information. For example, the letter of 2 June 2022 had 42 appendixes (see Court of Amsterdam 23 December 2022, ECLI:NL:RBAMS:2022:7693).
8. Court of Antwerp (appeal) 14 June 2023, no. 2022/CO/418, unpublished; Court of Antwerp (first instance) 25 October 2022, no. 2022/4901, unpublished.
9. Team Justitie, 'Press release, "2 jaar SKY ECC: Bijna 3.000 verdachten en reeds 1.125 jaar celstraf uitgesproken" (*Teamjustitie.be*, 9 March 2023) <https://verlinden.belgium.be/nl/2-jaar-sky-ecc-bijna-3000-verdachten-en-reeds-1125-jaar-celstraf-uitgesproken> accessed 1 October 2023.

obtained access to the intercepted data on 11 July 2019. This was later formalised in a second EIO and a "notice of transfer" was issued on 20 August 2019, showing that the data collected by the IP taps had been transferred to two public prosecutors of the Rotterdam Public Prosecution Service and to the Belgian authorities under Article 26 of the Cybercrime Convention and Article 7 of the European Convention on Mutual Assistance in Criminal Matters. The magistrate judge of the Lille District Court initiated the transfer of data, requesting the findings to be fed back to France.

Most of the 'IP wiretap data' from this brief interception period in June 2019 was encrypted. Some data, however, was not encrypted. Notably, in July 2019, law enforcement officials were able to identify subject lines of some group calls and the Sky ECC IDs of the participants in these group calls.

## *Interception of Sky ECC messages*

On 1 November 2019, Dutch, Belgian, and French law enforcement authorities formally agreed to create a 'Joint Investigation Team' (hereinafter: JIT). The agreement was signed on 13 December 2019. The goal of the JIT was twofold: gathering evidence about the criminal activities of Sky Global and its users, and sharing technical knowhow and resources among participating authorities.

The signing law enforcement authorities agreed to share the intercepted data at OVH in France with all JIT partners in order to identify those responsible, get an idea of the IT infrastructure behind Sky ECC, take it down, and prove whether or not Sky ECC is a criminal product, consisting of the facilitating of criminal offences. Moreover, the partners agreed on the use of the intercepted data. It was explicitly mentioned that they could analyse the raw data that could contain information in order to support ongoing or launch new criminal investigations into other criminals or criminal groups. The JIT agreement was initially concluded for a term of one year, but was later extended until 13 December 2021.[10]

Dutch technicians then developed a technique to copy the random access memory (RAM) of one of the Sky ECC servers without causing them to go offline. Subsequently, the Netherlands developed a so-called 'Man In The Middle technique' (MITM technique), which enabled the decryption of message traffic. According to Dutch case law, this technique was jointly developed and refined by the JIT partners.[11] The aim was to obtain encryption keys and/or passwords to decrypt the connection between devices and Sky ECC servers and to forensically analyse the Sky ECC servers later. This decryption technique was then shared with French law enforcement authorities, who needed a special permit to use it. The permit was granted by a committee established to consider the right to privacy and confidentiality of postal correspondence in accordance with article R.226-2 of the French Code Pénal.

A French judge then authorised the interception from 18 December 2020 until presumably approximately 9 March 2021, the date law enforcement authorities made the Sky ECC operation public. On this 'action day', a large number of arrests were made, and numerous house searches and seizures were conducted, in Belgium and the Netherlands.[12] According to Belgian law enforcement

10. Court of Antwerp (appeal) 14 June 2023, no. 2022/CO/418, unpublished; court of Antwerp (first instance) 25 October 2022, no. 2022/4901, unpublished.
11. See Court of Gelderland 20 December 2022, ECLI:NL:RBGEL:2022:7439 and ECLI:NL:RBGEL:2022:7425; and Court of Gelderland 11 April 2022, ECLI:NL:RBGEL:2023:2011.
12. Europol (n 3).

officials, 1 billion (!) messages were intercepted and shared with the JIT partners.[13] At least 500 million messages of this 'bulk interception' were decrypted within the first month.[14] We believe that these messages represent a treasure trove or "jackpot" for law enforcement authorities, due to the potential evidence of crimes and intelligence that can be derived from them. Law enforcement officials have made similar statements in interviews.[15]

Belgian authorities stated on 9 March 2023, that the Sky ECC operation led to a total of 526 cases against 2,961 suspects. Sentences have already been imposed in 344 individual cases and almost €110 million in criminal money has been seized.[16] The Sky ECC operation also led to over 250 judgements in the Netherlands, and a sentence was imposed in 170 individual cases.[17]

## *Analysing Sky ECC messages*

After the interception, the collected data must be analysed and then actually used as evidence in criminal investigations. To this end, law enforcement authorities have a system in place to store and analyse the intercepted data. The system, called 'Hansken', is a forensic platform developed by the Dutch National Forensic Institute (NFI).

Hansken can store, extract, and process data using 'dozens' of forensic tools. The system is designed to process large volumes of structured and unstructured data from various sources, searching for data and correlations that can provide insights to make informed decisions.[18] The Hansken system has been used in over 1,000 criminal cases in the Netherlands.[19]

In Dutch case law, court judgments frequently cite the content of messages linked to suspects' Sky-IDs.[20] These messages often refer to particular drugs. Analysts utilising the Hansken system employ "topic lists" to effectively search for pertinent messages using specialised keywords, including slang terms related to drug trafficking and homicide.[21]

13. Drommen and Hiroux (n 4).
14. D Hiroux, 'Na advocatuur, parket en politie nu ook arrestaties bij fiscus en stad Antwerpen na "operatie Sky": Wat weten we nu al?' (*vrt nws*, 6 April 2021) <https://www.vrt.be/vrtnws/nl/2021/04/06/opgepakt-nasleep-sky/> accessed 1 October 2023.
15. See, e.g., L Verhagen, 'Met deze eigen zoekmachine spit de politie schatten aan digitaal bewijs door' (*De Volkskrant*, 12 October 2018), <https://www.volkskrant.nl/wetenschap/met-deze-eigen-zoekmachine-spit-de-politie-schatten-aan-digitaal-bewijs-door~be00b20a/> accessed 1 October 2023; E Stoker, 'Politie kon wekenlang meelezen met geheime berichten van duizenden zware criminelen' (*De Volkskrant*, 2 July 2020) <https://www.volkskrant.nl/wetenschap/met-deze-eigen-zoekmachine-spit-de-politie-schatten-aan-digitaal-bewijs-door> accessed 1 October 2023.
16. See, e.g., L Walker, 'Crime of the century: Two years on from Belgium's biggest bust' (*The Brussels Times*, 9 March 2023) <https://www.brusselstimes.com/399469/crime-of-the-century-two-years-on-from-belgiums-biggest-bust> accessed 1 October 2023; C Van den Berghe, G Paelinck, and D Leestmans, '1.000 jaar aan celstraffen, maar ook oplaaiend geweld: 2 jaar geleden kraakten Belgische speurders versleutelde berichten van drugscriminelen' (*vrt nws,* 9 March 2023) <https://vrt.be/vrtnws/nl/2023/03/08/sky-ecc-twee-jaar/> accessed 1 October 2023.
17. As of 19 September 2023, over 252 judgements were available in the Dutch public case-law database Rechtspraak.nl.
18. Data Protection Impact Assessment (DPIA) of 'Hansken Variant 1A "inzet als forensisch onderzoeker", 19 September 2019, The Hague: Ministry of Justice and Security, The Netherlands, p. 12.
19. H M A van Beek, J van den Bos, A Boztas, E J van Eijk, R Schramp and M Ugen 'Digital forensics as a service: Stepping up the game' (2020) FSIDI 1-13.
20. See, e.g., Court of Amsterdam 15 November 2022, ECLI:NL:RBAMS:2022:6620, Court of Amsterdam 24 November 2022, ECLI:NL:RBAMS:2022:7082, Court of Limburg 22 November 2022, ECLI:NL:RBLIM:2022:9411, Court of Gelderland 20 December 2022, ECLI:NL:RBGEL:2022:7440, Court of Gelderland 11 April 2023, ECLI:NL:RBGEL:2023:2011.
21. Verhagen (n 15). See also Court of Rotterdam, 21 September 2021, ECLI:NL:RBROT:2021:9085, para 91-92.

A judgment from the Lower Court of The Hague' provides a compelling illustration of how messages were identified and connected to the suspect.[22] The court highlights the automated analysis and classification of chats among Sky ECC users. Specifically, within the "cocaine" category, keywords such as 'cocaine',' 'port', the name of a specific place (such as Rotterdam), 'airco' (referring to an air conditioner), 'get out' (to get drugs out), and 'eye' produced relevant matches. These matches revealed messages originating from distinct users of Sky ECC phones. After public prosecutors approved the investigation, the dataset of messages and metadata was made available to the investigation of the suspect in the present investigation. These messages were then used as evidence that contributed to the conviction of these suspects. In the present case, the judges were convinced that these messages could be attributed to the suspect, based on location data, testimonials of the suspect and family, and linking specific dates and times to activities of the suspect. They were punished for drug trafficking and other crimes and sentenced to five years of imprisonment.

Furthermore, the Dutch NFI confirms they make use of algorithms and artificial intelligence (AI) to analyse large volumes of data. For example, object recognition techniques are used to identify items such as ship containers, banking cards, weapons, and drugs. Additionally, the NFI is able to automatically extract text from images for subsequent examination.[23] It is worth noting that the NFI explicitly acknowledges that outcomes following the application of algorithms or AI are not 100% reliable.[24] For example, a false positive may occur when object or text recognition techniques are used.

In Belgium, there is no case law available with considerations about the way data from the Sky ECC operation is analysed. However, the Belgian minister of Justice is quoted in a press release, explaining that

> "[i]n order to mine the hundreds of millions of messages, we used artificial intelligence and machine learning to filter word combinations with criminal content. With this technique, we are currently moving to a second phase, which is to parse English and Albanian communications. Both languages are frequently used in the intercepted messages. Next, we will develop an algorithm that traces dubious money flows, for example with crypto coins. This new form of data-driven investigation is a powerful tool for our investigators. We want to exploit this to the maximum."[25]

## Data-driven criminal investigations

Sky ECC is an example of a data-driven investigation, i.e., an investigation in which the collected data drives new criminal investigations. As demonstrated in the preceding section, law

22. Court of The Hague 22 February 2023, ECLI:NL:RBDHA:2023:1960.
23. C van der Meer and M Willebrands, 'Duizenden foto's sneller doorzoeken dankzij slim algoritme' (*Magazines Forensisch Instituut,* 27 January 2021) <https://magazines.forensischinstituut.nl/atnfi/2021/35/duizenden-foto%E2%80%99s-sneller-doorzoeken-dankzij-slim-algoritme> accessed 1 October 2023. See also Forensichinstituut.nl, 'NFI leert computers om berichten met doodsbedreiging uit grote hoeveelheden data te filteren' (5 May 2021) <https://www.forensischinstituut.nl/actueel/nieuws/2021/05/05/nfi-leert-computers-om-berichten-met-doodsbedreiging-uit-grote-hoeveelheden-data-te-filteren> accessed 1 October 2023, and 'Demo Hansken' <https://www.hansken.nl/an-introduction-to-hansken/hansken-demo> (accessed 1 October 2023).
24. See Forensichinstituut.nl (n 23).
25. Translated by the authors with use of the tool 'Deepl'. Team Justitie, '1 jaar SKY ECC: Een ongezien succes in de strijd tegen de georganiseerde criminaliteit' (*teamjustitie*.be, 9 March 2022) <https://www.teamjustitie.be/2022/03/09/1-jaar-sky-ecc-een-ongezien-succes-in-de-strijd-tegen-de-georganiseerde-criminaliteit/> accessed 1 October 2023. See also N Vanhecke, 'Algoritmes jagen op Albanese maffia: wat is er veranderd na twee jaar Sky ECC?' (*De Standaard,* 9 March 2023) <https://www.standaard.be/cnt/dmf20230308_97761862> accessed 1 October 2023.

enforcement authorities can prioritise and look for messages using key words containing clues about particularly serious crimes, such as drug trafficking or homicide. Additionally, network analysis techniques could lead to the identification of organised crime groups. As stated earlier, the Sky ECC operation already led to hundreds of convictions of individuals in both the Netherlands and Belgium.

In the upcoming sub-sections, we will expand upon the concept of data-driven investigations and examine its relationship with the concept of 'grey infrastructures'. These infrastructures refer to services that are used for both legal and illegal purposes. Furthermore, we will highlight several legal challenges that may arise from this approach.

## *The concept of data-driven investigations*

The concept of data-driven investigations was developed by Dutch law enforcement officials involved in combatting cybercrime.[26] The work process for law enforcement authorities originated from a need to build a better information position by pooling digital traces and structuring data. In this way, information gathered in criminal investigations can also be used in other investigations. The data – typically called 'intelligence' – can also be used to gain insight into cybercrime phenomena and contribute to the development of new methods and means in tackling and stopping cybercrime.[27]

Data-driven investigations consist of four steps:

1. 'Collect', in which not only evidence from previous operations is used, but also newly acquired 'strategic data sets' are acquired in a criminal investigation;
2. 'Store', in which these multiple data inputs are warehoused and converted into information;
3. 'Analyse', in which related information points are combined with knowledge and become intelligence; and
4. 'Engage', in which intelligence is refined into facts that are used for lawful actions against crime.[28]

The first step of data collection typically involves the exercise of investigative powers, such as wiretapping, akin to the Sky ECC operation. A notable instance where substantial datasets were acquired is the Silk Road operation, where law enforcement obtained an image of a server. The copy was then shared by the Federal Bureau of Investigation (FBI) and Europol with other law enforcement authorities.[29] Another example is the EncroChat operation, which resulted in the collection of approximately 300 million messages.[30] And

26. van de Sandt, van Bunningen, van Lenthe, and Fokker (n 3). The concept of data-driven investigations and how it impacts the Dutch criminal law system is examined in Ballin and Oerlemans (n 6).
27. A J van Eeden, J J van Berkel, C C Lankhaar, and C J de Poot, 'Opsporen, vervolgen en tegenhouden van cybercriminaliteit', (*WODC, Cahiers 2021-2023*, 18 October 2021) <http://hdl.handle.net/20.500.12832/3114> accessed 1 October 2023.
28. van de Sandt, van Bunningen, van Lenthe, and Fokker (n 3) 2.
29. According to a judgement of the Court of Appeal of The Hague 26 June 2019, ECLI:NL:GHDHA:2019:1725, Europol provided data about Dutch vendors of Silk Road to Dutch law enforcement authorities. In several convictions the data was used as evidence. See, e.g., also the judgments of the Court of North Holland 10 March 2017, ECLI:NL:RBNHO:2017:1938, ECLI:NL:RBNHO:2017:1939, ECLI:NL:RBNHO:2017:1940.
30. See J J Oerlemans and D A G van Toor, 'Legal Aspects of the EncroChat Operation: A Human Rights Perspective' (2002) EJCCLCJ 309-328; van Eeden, van Berkel, Lankhaar, and de Poot (n 27).

recently, in May 2023, Europol revealed 'Operation SpecTor', following the seizure of servers of the marketplace Monopoly Market in December 2021, essentially describing a data-driven operation:

> "Europol has been compiling intelligence packages based on troves of evidence provided by German authorities, who successfully seized the marketplace's criminal infrastructure in December 2021. These target packages, created by cross-matching and analysing the collected data and evidence, served as the basis for hundreds of national investigations. (…) As law enforcement authorities gained access to the vendors' extensive buyer lists, thousands of customers across the globe are now at risk of prosecution as well."[31]

The second step of storage and third step of Analysis were already described earlier, using the Hansken platform as an example.

The fourth step of engagement is the step in which law enforcement authorities take specific interventions based on intelligence. The intervention may be a criminal investigation. For example, Europol states in another press release: "An intelligence packaged produced by Europol based on information from the SKY ECC operation allowed the identification of the structure, activities and international connections of the criminal network. This intelligence report triggered the current investigation."[32]

Note that these interventions do not necessarily involve launching a criminal investigation or prosecuting a specific suspect. For example, law enforcement authorities could decide to warn (mostly young) offenders by knocking on their doors ('knock-and-talks') or publishing nicknames of suspects to send them a message and attempt to halt their illegal activities.[33]

## *Grey infrastructures*

The fact that law enforcement authorities increasingly carry out data-driven investigations is closely linked to the emergence of 'grey infrastructures', such as Sky ECC, that render the use of traditional investigative methods more difficult.

A grey infrastructure is a service that is often located in a country with strong privacy laws or a history of not cooperating with law enforcement authorities, and thus often used by (cyber) criminals. Examples are bulletproof hosting providers, cryptocurrency exchanges, and Virtual Private Network Services.[34] These companies offer services that are used both for legal purposes and for committing and shielding crime.[35]

In its "Internet Organised Crime Threat Report 2021", Europol mentions for the first time that EncroChat cryptophones are an example of a service that offers a grey infrastructure. It also states

31. Europol, '288 dark web vendors arrested in major marketplace seizure' (*europol.eu*, 2 May 2023) <https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure> accessed 1 October 2023.
32. Europol, 'Cocaine cartel uncovered on SKY ECC busted in Bosnia and Herzegovina' (*europol.eu,* 15 May 2023) <https://www.europol.europa.eu/media-press/newsroom/news/cocaine-cartel-uncovered-sky-ecc-busted-in-bosnia-and-herzegovina> accessed 1 October 2023.
33. See J J Oerlemans and R S van Wegberg, 'Opsporing en bestrijding van online drugsmarkten' (2019) *Strafblad* 29; van Eeden, van Berkel, Lankhaar, and de Poot (n 27) 98.
34. Europol (2021), *Internet Organised Crime Threat Assessment (iOCTA) 2021* (*European Union* 2021).
35. van Eeden, van Berkel, Lankhaar, and de Poot (n 27) 42.

that "[a]lthough not all users of such services are necessarily criminals, the level of criminality associated with such services is often so high that national law enforcement agencies, after finding enough evidence of criminal abuse, could consider them to be criminal enterprise".[36]

While some countries intend to criminalise the use of cryptophones,[37] developing secure and privacy-friendly software is currently not prohibited. On the contrary, Article 25(1) of the General Data Protection Regulation (GDPR) requires controllers[38] to incorporate appropriate technical and organisational measures from the software design stage onwards, to ensure and demonstrate compliance with data protection principles. By integrating privacy-friendly features into their messaging applications, cryptophone providers effectively fulfil this obligation.[39] Nevertheless, cryptophone networks and services could be considered as grey infrastructures due to their prevalent use by criminals and criminal organisations.

Moreover, the way grey infrastructures operate renders the use of traditional investigative methods, such as wiretapping and data production orders, ineffective. This forces law enforcement to resort to more intrusive investigative methods. With regard to Sky ECC, the company made use of a private Access Point Name (which is the gateway between a smartphone and another network) that connected the Sky ECC phones directly to the Sky ECC network. As a result, private data sessions were established through regular transmission towers without, however, being susceptible to regular interception by law enforcement authorities.[40] Law enforcement authorities consequently proceeded to another way of intercepting the communications, notably in bulk and using sophisticated decryption techniques. The details of the decryption technique and interception used are not entirely known at the time of writing (September 2023).

## *A slippery slope for law enforcement activities?*

Data-driven criminal investigations targeting grey infrastructures such as Sky ECC can be a slippery slope for two reasons: the 'mixed bag' of law enforcement purposes and an unclear threshold to be considered a grey infrastructure.

First, operations such as Sky ECC often involve a 'mixed bag' of law enforcement purposes, because they pursue different objectives. Collecting evidence of crimes is often only of them. The Sky ECC operation, for instance, yielded valuable intelligence on the modus operandi of organised crime, particularly drug-related activities, and to some extent disrupted criminals' communication about their illicit activities, until they moved to a different communication service. It may also have created uncertainty among individuals as to whether they are under suspicion by law enforcement authorities.

Consequently, some authors have called for a broader discussion about the role of law enforcement authorities in today's fight against crime. Should the scope of their responsibilities be limited to investigation and prosecution, or could investigative resources be deployed for

36. Europol (n 34) 18.
37. "Making, modifying, supply, offering to supply and possession of articles for use in serious crime" would constitute a criminal offence in the United Kingdom. J Cox, 'UK Proposes Making the Sale and Possession of Encrypted Phones Illegal' (*vice.com*, 8 February 2023) <https://www.vice.com/en/article/z34p49/uk-proposes-making-sale-possession-of-encrypted-phones-illegal-encrochat-sky> accessed 1 October 2023.
38. And encourages producers of the products, services and applications. See Recital 78 GDPR.
39. S Royer and P Dewitte, 'Drawing the line between privacy by design and criminal liability' (*CiTiP Blog,* 16 March 2021) <https://www.law.kuleuven.be/citip/blog/drawing-the-line-between-privacy-by-design-and-criminal-liability/> accessed 1 October 2023.
40. Court of Antwerp (appeal) 14 June 2023, no. 2022/CO/418, unpublished.

countermeasures, when it is clear from the start of an investigation that an actual prosecution is less feasible?[41] For example, is it allowed to take down an entire darknet market without initiating any investigation into the crimes committed by administrators or vendors? While some authors argue that such takedowns can be secondary objectives, the permissibility depends on the specific national laws.[42] Additionally, we wonder whether the primary objective of the Sky ECC operation should be considered the acquisition of intelligence, which drives subsequent criminal investigations, instead of gathering evidence in a criminal investigation.[43] It goes without saying that the main objective cannot be a fishing expedition. This may be the case when the data secured during an investigation is not sufficiently related to the investigation at hand.

Second, the threshold for law enforcement authorities to consider a service provider a 'grey infrastructure' is unclear. It was argued by Belgian authorities that Sky ECC was almost exclusively used for criminal purposes, justifying the broad scope of the interception.[44] In the operation regarding Ennetcom phones, the Dutch Public Prosecution Service submitted that – out of 458 conversations analysed – 78.4% (359) were found to contain topics related to criminal activities. These were identified by keywords, such as slang use for drug trafficking.[45] From a human rights perspective, this is problematic because communication of non-criminals will be intercepted as well. As the threshold for considering an infrastructure 'grey' is lowered, there is a risk that data-driven operations slip into a fishing expedition, which is prohibited by the ECHR.

We could ask ourselves whether it is it possible that law enforcement authorities will one day hack or bulk intercept data from (parts of) the IT infrastructure of services like Signal or Telegram. Clearly, these applications host, for example, designated group chats or 'channels' focusing on drug trafficking.[46] Although cryptophones are very different in nature from regular smartphones with encrypted communication applications, we do not consider this an unthinkable scenario.

This leads us to the question how legitimate users of grey infrastructures are protected, when those infrastructures are targeted in data-driven criminal investigations. This topic has not yet received much attention.[47] It appears that legitimate users are offered no or only very limited legal protection so far. For instance, from a human rights perspective, it was rather worrying that all legitimate Sky ECC users were asked to come forward at some point during the investigation.[48] For

41. van Eeden, van Berkel, Lankhaar, and de Poot (n 27) 94. See also Ballin and Oerlemans (n 6).
42. Ballin and Oerlemans (n 6) 27-30.
43. See also R Stoykova, 'Encrochat: The Hacker with a Warrant and Fair Trials?' (2023) FSIDI 1-14.
44. Court of Antwerp (appeal) 14 June 2023, no. 2022/CO/418, unpublished; Court of Antwerp (first instance) 25 October 2022, no. 2022/4901, unpublished.
45. Court of Rotterdam 21 September 2021, ECLI:NL:RBROT:2021:9085, paras 88 and 165 (annotated in *TBS&H* 2022 by J.J. Oerlemans). Note that court in this case did not accept that all of these conversations were necessarily criminal in nature.
46. See, e.g., Court of Amsterdam 29 June 2022, ECLI:NL:RBAMS:2022:4825. On 25 April 2023, Dutch police forces also took over a Telegram Channel related to drug trafficking. They warned channel members their data was stored in police databases, drug trafficking is illegal, and it creates health issues. See Politie.nl, 'Politie verstoort drugshandel in de Achterhoek door in te grijpen in Telegramgroep' (*politie*.nl, 25 April 2023) <https://www.politie.nl/nieuws/2023/april/25/02-politie-verstoort-drugshandel-in-de-achterhoek-door-in-te-grijpen-in-telegramgroep.html> accessed 1 October 2023.
47. See S Royer and R Vanleeuw, 'Cryptofoons, privacyvriendelijke applicaties en het vermoeden van onschuld' (2022) TBSH 90-97.
48. H Decré, 'Politie vraagt iedereen met versleutelde Sky ECC-telefoon om zich te melden: "Belgische gebruikers werden afgeluisterd"' (*vrt nws*, 11 March 2021) <https://www.vrt.be/vrtnws/nl/2021/03/11/oproep-sky> accessed 1 October 2023.

them, it may have been unclear what law enforcement authorities would do with this knowledge. Would their data be first checked and then filtered out? Should lawyers be obliged to hand over their Sky-ID to filter out privileged communications? We do not answer these questions in this article, but they are in our view worth examining.

## The right to privacy and the Sky ECC operation

The Sky ECC operation undoubtedly represents a significant interference with the right to privacy for both the company and its clients involved. In this section, we further examine the privacy interference and identify which minimum safeguards the ECtHR would probably require in an operation such as Sky ECC. Furthermore, we explore potential areas of tension where the collection and analysis of Sky ECC data might conflict with these safeguards. We then identify which safeguards might conflict with the collection and analysis in the context of the Sky ECC operation.

### *Interferences*

The right to respect for correspondence within the meaning of Article 8 § 1 ECHR aims to protect the confidentiality of communications. This covers the contents of the actual messages sent, but also information relating to such messages (traffic data, such as the date, time, duration, and telecommunications numbers).[49] It is clear people could communicate with Sky ECC using different apps, such as apps for e-mail, chats, and voicemail. Intercepting this data therefore amounts to an interference with the right to privacy and more particularly the right to respect for correspondence. The ECtHR has consistently regarded the interception of communications as a serious interference with the right to respect for private life and the right to respect for correspondence.[50]

Certain public prosecutors assert that devices like Sky ECC phones are distinct from regular smartphones, because they are primarily used to facilitate criminal activities rather than for legitimate business and personal purposes. As a result, they argue that the interception of communications through a cryptophone should be considered a minor infringement.[51] We firmly disagree with this reasoning, as the extent to which communications are related to criminal matters should not dictate the severity of the interference. What truly matters is that law enforcement authorities covertly intercept private communications between individuals and that this amounts to a serious interference with the right to respect for private life and the right to respect for correspondence. This interference is serious in nature, even when it relates to a single cryptophone. Moreover, given the very large amount of collected communication data ('bulk') (in this case, approximately 500 million messages), the interference with Article 8 ECHR is evidently serious in nature.[52]

49. See, e.g., ECtHR 25 September 2001, appl. no. 44787/98, ECLI:CE:ECHR:2001:0925JUD004478798, para 42 (*P.G. and J.H./the United Kingdom*).
50. See e.g., See e.g., ECtHR 24 April 1990, appl. no. 11105/84, ECLI:CE:ECHR:1990:0424JUD001110584, para 32 (*Huvig/France*), ECtHR 24 April 1990, appl. no. 11801/85, ECLI:CE:ECHR:1990:0424JUD001180185, para 31 (*Kruslin/France*), ECtHR 25 March 1998, appl. no. 23224/94, ECLI:CE:ECHR:1998:0325JUD002322494, para 72 (*Kopp/ Switzerland*) and ECtHR 16 February 2000, appl. no. 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895, para 56 (*Amann/Switzerland*).
51. See also para 6.8.10 of the Dutch Attorney-General Paridaens' opinion on 9 May 2023, ECLI:NL:PHR:2023:477.
52. We point out the Dutch Advocate General mentioned above ultimately agrees the privacy interference is serious in nature due to large number of messages that were intercepted.

Previous case law of the ECtHR has also dealt with bulk interception of communications. Early case law concerned bulk interception ("secret surveillance") of landline phones.[53] Following technological developments, it then concerned bulk interception of mobile phones, including internet traffic.[54] Most recently, in the landmark cases of *Big Brother Watch v. The United Kingdom*[55] and *Centrum för Rättvisa v. Sweden*,[56] the ECtHR addressed modern-day bulk interception of communications carried out by intelligence services.

In *Big Brother Watch* and *Centrum för Rättvisa*, the ECtHR considers that an interference with Article 8 ECHR takes place not only during the interception, but during each and every phase in which intercepted communications are processed, i.e., from the collection phase, through the analysis phase, to the actual use of the data in a criminal investigation and sharing the data with other law enforcement authorities. The Strasbourg Court finds the *analysis* of intercepted communications particularly infringing.[57]

## Minimum safeguards

An interference with the right to privacy can only be justified if the conditions set out in the second paragraph of Article 8 ECHR are satisfied. Thus, the interference must be "in accordance with the law", pursue one or more "legitimate aims" and be "necessary in a democratic society" to achieve those aims. As part of the legality requirement, the ECtHR often sets out criteria or "minimum safeguards" to which Member States must adhere to avoid abuses of power.

Before applying the safeguards from existing ECtHR case law to the situation of data-driven criminal investigations, we point out that bulk interception in the context of intelligence services is different from bulk interception in a law enforcement context as carried out in the Sky ECC operation.[58] There are two reasons for this. First, the aim to collect data is different. Intelligence and security services usually perform bulk interception for the purpose of foreign intelligence gathering, or the early detection and investigation of cyberattacks, counter-espionage, and counter-terrorism.[59] In the context of bulk interception in the Sky ECC operation, the purpose is to combat and investigate crime. Second, bulk interception in an intelligence context is generally directed at international communications focusing on monitoring communications of persons or organisations outside the State's territorial jurisdiction.[60] In the Sky ECC operation, network traffic was intercepted from specific servers used by Sky ECC Global at a single internet service provider in France. This interception is more targeted compared to bulk interception in an intelligence context.

53. ECtHR 6 September 1978, appl. no. 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971 (*Klass and other/Germany*).
54. See, e.g., ECtHR 29 June 2006, appl. no 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400, (*Weber and Saravia/Germany*), ECtHR 1 July 2008, appl. no. 58243/00, ECLI:CE:ECHR:2008:0701JUD005824300, (*Liberty and Others/the United Kingdom*) and ECtHR 4 December 2015, appl. no 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306 (*Roman Zakharov/Russia*).
55. ECtHR 25 May 2021, appl. nos. 58170/13, 62322/14 and 24960/15), ECLI:CE:ECHR:2021:0525JUD005817013, para 330 (*Big Brother Watch/The United Kingdom*).
56. ECtHR 25 May 2021, appl. no. 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208 (*Centrum för Rättvisa/Sweden*).
57. *Big Brother Watch* (n 55) para 330.
58. See also Georgios Sagittae, 'On the lawfulness of the EncroChat and Sky ECC-operations' (2023) NJECL 1–2.
59. *Big Brother Watch* (n 55) paras 345 and 348; *Centrum för Rättvisa* (n 56) paras 259 and 262.
60. *Big Brother Watch* (n 55) paras 236 and 344; *Centrum för Rättvisa* (n 56) para 258.

However, given the overall similarity to bulk interception, the ECtHR will probably require the same safeguards for Member States.[61] States and their institutions, such as the Public Prosecution Service and the judiciary, should also realise that in criminal cases, defence attorneys may refer to this case law and demand that States respect these minimum safeguards.

In *Big Brother Watch* and *Centrum för Rättvisa,* the ECtHR stated it will examine whether the domestic legal framework of the State in question clearly defined the following eight minimum safeguards:

1. the grounds on which bulk interception may be authorised;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure to be followed for granting authorisation;
4. the procedures to be followed for selecting, examining, and using intercepted material;
5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material, and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.[62]

We find it particularly noteworthy that the minimum safeguards do not only focus on the collection phase, but require safeguards during *all phases*, including the (further) processing of data.[63] Obviously, only a warrant provided by a judge or independent authority to justify bulk interception of communications is not enough. With these minimum safeguards, the ECtHR makes clear that throughout the phases of bulk data investigations, principles of data protection regulations apply, such as those mentioned in no. 6: the limits on the duration of interception, the storage of intercept material, and the circumstances in which such material must be erased and destroyed. Here, the ECtHR clearly establishes a connection between criminal procedural law and data protection law.

In order to minimise the risk of the bulk interception power being abused, the ECtHR emphasises the need for 'end-to-end safeguards'. This entails the following key elements: (a) a necessity and proportionality assessment should be made at each stage of the process; (b) bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and (c) the operation should be subject to supervision and independent *ex post facto* review.[64] The ECtHR references the report of the Venice Commission, which similarly highlighted the importance of authorisation and oversight in bulk interception regimes.[65]

61. See also paras 5.7.1-5.7.11 of Attorney-General Paridaens' opinion on May 2023, ECLI:NL:PHR:2023:477; M Galič, 'Bulkbevoegdheden en strafrechtelijk onderzoek: wat de jurisprudentie van het EHRM ons kan leren over de normering van grootschalige data-analyse' (2022) TBSH 130-137; M I Fedorova, R M te Molder, M J Dubelaar, S M A Lestrade and T F Walree, *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden* (Radboud University Press 2022).
62. See *Big Brother Watch* (n 55) para 361; *Centrum för Rättvisa* (n 56) para 275.
63. See *Big Brother Watch* (n 55) para 350; *Centrum för Rättvisa* (n 56) para 264.
64. See *Big Brother Watch* (n 55) paras 349-350 and 360; *Centrum för Rättvisa* (n 56) paras 263-264 and 274.
65. Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies 2015.

## Application to the interception of Sky ECC communications

In the Sky ECC operation, it is clear that an *ex ante* (judicial) authorisation from a French judge to intercept the communications in bulk was available. As explained earlier, Dutch, Belgian, and French law enforcement agencies cooperated and prepared the operation well, intercepting data from Sky ECC in steps. In the first stage, French law enforcement authorities obtained a warrant to intercept data for a limited amount of time and transfer data to other States in order to find a technical solution to decrypt the network traffic. A decryption technique developed by Dutch law enforcement authorities was then shared with French law enforcement authorities, who required a special permit to use it, which was granted by the appropriate committee.[66] A French judge then subsequently authorised the bulk interception for a much longer period of time. In sum, a test on necessity and proportionality took place in the collection phase of the Sky ECC operation and was approved by Belgian courts.[67]

In the Netherlands, the Dutch Supreme Court ruled that the principle of mutual trust between States applies in the Sky ECC operation. First, this means that decisions by French authorities that form the basis for investigations conducted in France, must be respected by the Dutch courts in Dutch criminal proceedings. It should, therefore, be assumed that the relevant investigations by French law enforcement authorities have been conducted lawfully.[68] Second, the Dutch criminal courts must assume that the investigation abroad was conducted in such a way that its results can be relied on. The Dutch courts are obliged to give further consideration to the reliability of the results only when there are specific indications to the contrary.[69] The same applies if the investigation was conducted by a JIT.[70]

## Application to the analysis of Sky ECC communications

Tension may arise in respecting the safeguards by law enforcement authorities that relate to processing data *after* the collection phase.[71] As explained earlier, the ECtHR finds the analysis of intercepted communications particularly infringing.[72] We question whether law enforcement authorities have proper procedures in place for selecting, examining, and using intercept material; whether they have clear limits on the duration of interception, the storage of intercepted material, and the circumstances in which such material must be erased and destroyed; and whether they have proper procedures for independent and effective *ex post facto* review.

First, when it comes to creating subsets in the initially obtained data set, one could argue that a judicial warrant or a warrant by an independent authority should be obtained to further investigate these subsets for law enforcement purposes. In a typical bulk interception regime, 'selectors', such as an e-mail address of a target, are utilised to identify and store relevant communications. The data

66. In the EncroChat operation, the French Supreme Court ruled on 11 October 2022 this certificate had to be provided. It did not declare the operation itself unlawful. See Cour de cassation 11 October 2022, ECLI:FR:CCASS:2022:CR01226 and Cour de cassation 25 October 2022, ECLI:FR:CCASS:2022:CR01216.
67. E.g. Court of Antwerp (appeal) 14 June 2023, no. 2022/CO/418, unpublished.
68. Dutch Supreme Court 13 June 2023, ECLI:NL:HR:2023:913, para 6.5.1.
69. Ibid, para 7.7.4.
70. Ibid, para 7.3.2.
71. See also B W Schermer and M Galič, 'Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen?', (2022) NTS 167-177.
72. *Big Brother Watch* (n 55) para 330.

can then be examined by an analyst.[73] To determine the necessity and proportionality to select the data, a warrant should indicate the categories of selectors to be employed that relate to a target, such as an individual or a group of individuals.[74] In our view, a judicial warrant each time a subset is created, would be an important safeguard, because it requires a test on the necessity and proportionality to further analyse the data.[75] A judge could also provide additional safeguards in a warrant, such as special obligations to filter out privileged communications. We point out this is certainly not the case in Belgium, where the investigative judge – in line with criminal procedural rules – has transferred all the obtained data to the public prosecutor's office that decides on launching new criminal files.

Second, the Law Enforcement Directive determines that data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which it is processed.[76] However, it remains unclear for how long the initial data set is kept, especially with regard to data that is not used as evidence in a specific criminal case. Therefore, we wonder whether these data protection regulations are respected by the authorities analysing the Sky ECC data.

Third, with respect to safeguards relating to data protection regulations by law enforcement authorities, we find it worrying that it is not clear to what extent these safeguards are effectively enforced by data protection authorities. In the Netherlands, the Dutch data protection authority did not investigate any of the cryptophone operations in the Netherlands (or at least so far not publicly). Many Dutch legal scholars are also critical about the effectiveness of oversight by the Dutch data protection authority on compliance with data protection law.[77]

In Belgium, an independent supervisory authority, the Supervisory Body for Police Information, is entrusted with monitoring the compliance of data protection rules by all Belgian law enforcement authorities.[78] As far as we know, no investigation into the Sky ECC data collection and further processing has been launched so far. This is not surprising, as despite its broad legal mandate, the Supervisory Body cannot possibly investigate all data processing by law enforcement authorities because of its limited staff of ten persons.

Taking into account the safeguards stemming from data protection regulations, we wonder whether, for example, maximum retention periods are available for the data acquired in the Sky ECC operation. When data protection authorities or independent supervisory bodies will look into whether States have clear limits on the duration, storage, and erasure of interception material, we are not confident that the further processing and use of data collected during data-driven investigations will pass this ECtHR test. We emphasise again that a warrant to collect the data is not enough to respect the standards set in ECHR case law: certain principles of data protection law must also be respected, such as procedures for selecting and examining the stored material, and independent and

73. See, e.g., *Big Brother Watch* (n 55) para 353.
74. See, e.g., *Big Brother Watch* (n 55) paras 353-355 and 382.
75. See also Oerlemans and van Toor (n 30).
76. Article 4 Directive 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
77. See L Stevens, M Hirsch Ballin, M Galič et al., 'Strafvorderlijke normering van preventief optreden op basis van datakoppeling' (2021) TBS&H 241-242 and Schermer & Galič 2022, p. 171; M I Fedorova, R M te Molder, M J Dubelaar, S M A Lestrade and T F Walree (n 61) 168; Ballin and Oerlemans (n 6) 34.
78. See Controleorgaan, 'National activities' <https://www.controleorgaan.be/en/monitoring-body/national-activities> accessed 1 October 2023.

effective oversight. In this respect, criminal procedural law and data protection law are connected with each other.

## Equality of arms and the Sky ECC operation

'Equality of arms' is the key principle of the right to a fair trial to consider in relation to the Sky ECC operation. As part of the right to a fair trial in Article 6 ECHR, the ECtHR has consistently judged that criminal procedure should be adversarial and that there should be 'equality of arms' between prosecution and defence.[79] We identify three main elements of the equality of arms in the context of the Sky ECC operation: (1) transparency; (2) reliability of evidence; and (3) access to datasets.[80] These elements are further examined below.

### *Transparency*

As part of the equality of arms and an adversarial trial, both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party.[81] Therefore, when the public prosecutor submits evidence in a criminal trial, the defence should have to opportunity to have knowledge and ask questions about the evidence obtained. This relates to the disclosure of prosecutorial evidence.

The question *how* evidence is obtained can be important for the defence to test the reliability of evidence and to test whether the right to privacy has been respected. The right to the full disclosure of prosecutorial evidence starts at the early stages of a criminal process, when the accused is to have adequate access to the investigation file.[82]

The ECtHR emphasises that the disclosure of all relevant evidence is not an absolute right.[83] In any criminal proceedings there may be competing interests against disclosure.[84] In some cases, it may be necessary to withhold certain evidence from the defence in order to preserve the fundamental rights of other individuals or to safeguard an important public interest, such as national security or the need to protect witnesses at risk of reprisals, or to keep police methods of criminal investigation a secret.[85] When the trial judge assesses the appropriateness of the non-disclosure of certain materials to the defence, the ECtHR has stressed the importance of (1) weighing the public

79. See, e.g., ECtHR 22 July 2004, nos 39647/98 and 40461/98, ECLI:CE:ECHR:2004:1027JUD003964798 (*Edwards and Lewis/The United Kingdom*) para 46.
80. Here we follow the categorisation made by Oerlemans and van Toor (n 30) in their analysis of the EncroChat operation in relation to a fair trial.
81. See, e.g., ECtHR 16 February 2000, appl. no. 28901/95, ECLI:CE:ECHR:2000:0216JUD002890195 para 60 (*Rowe and Dave/the United Kingdom*) and ECtHR 28 August 1991, appl. nos. 11170/84, 12876/87 and 13468/87, CLI:CE:ECHR:1991:0828JUD001117084, paras 66-67 (*Brandstetter/Austria*).
82. See M I Fedorova, 'The Principle of Equality of Arms in International Criminal Proceedings' (Master's thesis, University of Utrecht, 2012) 55.
83. ECtHR 26 March 1996, no. 20524/92, ECLI:CE:ECHR:1996:0326JUD002052492 (*Doorson/The Netherlands*), para 70.
84. ECtHR (GC) 16 February 2000, no. 28901/95, ECLI:CE:ECHR:2000:0216JUD002890195 (*Rowe and Davis/the United Kingdom*), para 61.
85. Ibid. See also ECtHR (GC) 16 February 2000, no. 27052/95, ECLI:CE:ECHR:2000:0216JUD002705295 (*Jasper/the United Kingdom*), para 52.

interest against the interest of the accused and (2) affording the defence an opportunity to participate in the decision-making process to the maximum extent possible.[86]

In the Sky ECC operation, it seems to be a recurring issue that public prosecutors are not willing to share all information that the defence requests. For example, the Italian Supreme Court declared in July 2022 that Italian prosecutors and police should disclose information on how they obtained intercepted messages from the Sky ECC cryptophone network.[87] In the Netherlands, some courts were critical that it took some time for the Public Prosecution Service to provide a sufficient amount of information about the investigation and evidence-gathering activities in the Sky ECC operation. More specifically, at first, the Dutch Public Prosecution Service did not mention the development of the decryption tool, and only provided the necessary details about the operation (in France) later.[88]

In Belgium, information on how the investigation has been carried out, has not been made public. Defendants, however, have access to their criminal files, which besides police reports on the specific case contain a report of the federal prosecutor on the operation. Yet, details on how the decryption of the messages in the initial investigation took place, are not shared with the defendants.[89] When it comes to the analysis of the intercepted data, only a press release of the minister of Justice is available, stating that artificial intelligence and machine learning were used to filter word combinations with criminal content and to parse English and Albanian communications, as both languages are frequently used in the intercepted messages.[90]

Notably, there is not much information available in case law about *how* the evidence is derived from the targeted bulk interception in the Sky ECC operation, in other words, about the analysis phase of bulk interception. The use of algorithms, key word indexes, or network analysis techniques is rarely mentioned in case law. It is possible that in relevant cases, the defence did not argue or explain why this information is relevant to the suspect and, therefore, courts did not deal with this aspect in their decisions. Yet, this information may be relevant when discussing the reliability of the evidence. In sum, while there is transparency about the collection phase of the Sky ECC operation in the Netherlands and Belgium, albeit not in all states, there is very little transparency about the analysis phase of the Sky ECC operation, even in the Netherlands and Belgium.

### *Reliability of evidence*

As explained above, there appears to be little transparency about the processing of data after the collection phase in the Sky ECC operation. This is relevant because the ECtHR pays attention to whether the defendant had the opportunity to challenge both the authenticity and the use of the contested evidence. However, national courts have a considerable margin of appreciation when assessing the reliability of evidence. Moreover, the ECtHR only considers obtained evidence as unreliable if there are 'manifest flaws' to be detected in its processing.[91] In the case *Khodorkovskiy and Lebedev v. Russia*, for instance, the defendants claimed that the authorities had presented more

86. Fedorova (n 82) 60 with reference to ECtHR 11 December 2008, appl. no. 6293/04, ECLI:CE:ECHR:2008:1211JUD000629304, para 205 (*Mirilashvili/Russia*).
87. Italian Supreme Court of 15 July 2022 (Cass., quarta sezione, n. 32915).
88. See, e.g., Court of Gelderland, 20 December 2022, ECLI:NL:RBGEL:2022:7425 and ECLI:NL:RBGEL:2022:7105.
89. Court of Antwerp (appeal) 14 June 2023, no. 2022/CO/418, unpublished; Court of Antwerp (first instance) 25 October 2022, no. 2022/4901, unpublished.
90. Team Justitie (n 25).
91. See also K Quezada-Tavárez, P Vogiatzoglou, and S Royer, 'Legal challenges in bringing AI evidence to the criminal courtroom' (2021) NJECL 531-551.

evidence to the court than had originally been seized, as the servers had not been properly locked up.[92] In this case, the ECtHR decided that the use of the evidence did not breach Article 6 ECHR, as the defendants had had the opportunity to interrogate witnesses that were present at the time of the search and seizure operation. In addition, the ECtHR could not detect any manifest flaw in the process of seizing and examining the hard drives that would make the information obtained unreliable. In other words, when the defence has sufficient opportunities to ask questions about the way the data is processed and request expert witnesses, a lack of transparency may be counterbalanced.

Reportedly, the Hansken system used to store and analyse Sky ECC data has an intricate system for logging, which results in a full trail of who did what with which data. This makes the processing of data – in theory – transparent to the investigation team, to the public prosecutor, to the court, and to the suspect's lawyers.[93] In practice, however, Dutch case law shows that requests of the defence for logging data or source code are always denied by Dutch judges. Instead, the defence are – to a certain extent – allowed to ask technical questions, access the data used against suspect themselves, and request a counter-expertise by an expert.[94] For the defence, it should be clear from evaluations how a system like Hansken works and to what extent the output is reliable.[95] The legal evaluation of the authenticity and reliability of digital evidence, and therefore the opportunity for the defence to challenge digital forensics expertise, depends on the selected digital forensic process, methods, and tools for each forensic task and its sufficient documentation in the chain of custody that can demonstrate data integrity preservation and reliability validation.[96]

In addition, Sagittae points out Dutch authorities took several steps to ascertain the reliability of collected data when selecting, examining, and using the data in Dutch criminal proceedings. First, the hash values of the data that were acquired in France were compared to the hash values of the data that were transmitted to the Netherlands. A hash value is a numeric value of a fixed length that uniquely identifies data. Corresponding hash values in both countries imply that both countries possess the exact same data.[97] With only very few exceptions, the Dutch hash values of Sky ECC data all matched the French hash values. Furthermore, the NFI examined the accuracy and reliability of the data obtained in the Sky ECC operation.[98] The report shows that the "Toolbox data" is a correct representation of the chat messages and their metadata, but that the data is sometimes

92. ECtHR 25 October 2013, appl. no. 11082/06 and 13772/05, ECLI:CE:ECHR:2013:0725JUD001108206, paras 72, 674-681, 700-702 (*Khodorkovskiy and Lebedev/Russia*).
93. H.M. van Beek, E.J. van Eijk, R.B. van Baar, M. Ugen, J.N.C. Bodde & A.J. Siemelink (2015). Digital forensics as a service: Game on. *Digital Investigation*, *15*, 27-28 (hereinafter: van Beek 2015).
94. See, e.g., Court of Oost-Brabant 7 July 2022, ECLI:NL:RBOBR:2022:2832, Court of Amsterdam 15 March 2022, ECLI:NL:RBAMS:2022:1227. See in this respect also the Dutch Supreme Court Case in relation to Ennetcom of 28 June 2022, ECLI:NL:HR:2022:900.
95. See also R.M. te Molder, 'Digitaal forensische zoekmachines, effectieve verdedigingsrechten en de modernisering van het Wetboek van Strafvordering: is aanpassing van het conceptwetsvoorstel gewenst?', *Bsb* 2022, nr. 5, p. 185 referring to T. Bollé, E. Casey & M. Jacquet, 'The role of evaluations in reaching decisions using automated systems supporting forensic analysis', *Forensic Science International: Digital Investigation* 2020, vol. 43, p. 1-13.
96. Stoykova (n 43) 5-8.
97. Sagittae (n 58) 16. See, for example, Court of Rotterdam 17 May 2023, ECLI:NL:RBROT:2023:4136, referring to such a report.
98. The report is called 'Volledigheid en correctheid van decodering van Sky ECC berichten met de toolboxmethode' in Dutch, which translates to a report on the 'Completeness and correctness of decoding SkyECC messages with Toolbox method" (this report is not publicly available, but mentioned in case law, such as Court of Oost-Brabant 23 March 2023, ECLI:NL:RBOBR:2023:1853.

incomplete. This incompleteness was deemed explainable by the NFI and not considered as a problem in case law.[99]

In a Belgian case, defendants have tried to challenge the reliability of the evidence, as law enforcement authorities did not disclose the decryption techniques that were used. Their arguments, however, were dismissed. The Antwerp Court of Appeal found that the disclosure of the decryption techniques is not relevant to assess the lawfulness of the evidence, as it does not concern the content of the messages. Moreover, the details of the used techniques were kept secret in order to be able to reuse the techniques in the future. According to the court, this did not constitute a violation of the right to a fair trial.[100] Nevertheless, since the law does not specify how to ensure the reliability of digital decrypted evidence and there is no supervision,[101] we believe it is necessary for the defence to know how the data was decrypted.[102]

Furthermore, case law shows that judges simply discuss the evidence at hand, for example, the content of messages about drugs trafficking linked to Sky ECC users by their Sky-ID, and then determine whether they find the evidence convincing.[103] The evidence is often supported by other materials. From case law, it visible how a variety of investigative methods are used to associate Sky ECC users with the messages. The additional investigative methods used include data production orders directed at telecommunication service providers to gather subscriber and location data, data production orders to gather passenger name records, seizing a suspect's cryptophone, correlating the nicknames of suspects from other sources of evidence to Sky ECC messages, and, of course, obtaining testimonials or even confessions from suspects.[104] In short, Sky ECC messages are rarely the only source of evidence used to convict individuals of crimes.

### *Access to datasets*

When a public prosecutor submits evidence in a criminal trial that is obtained during the Sky ECC operation, the defence should have the opportunity to acquire knowledge and ask questions about this evidence. In the Sky ECC operation, and also in many other modern-day criminal investigations, 'bulk data' is involved. The ECtHR developed a specific procedure for large datasets, which we will discuss below.

In order to analyse the data, law enforcement authorities filter the raw dataset (also known as a 'primary dataset') into a 'secondary dataset'. Where the raw dataset is unstructured and contains all seized data, the secondary dataset "only" contains all data relevant for criminal investigations. Still, this dataset is a large volume of information on all kinds of (potential) suspects and crimes. The next step is to compile the 'tertiary dataset' with all the relevant information for a specific

99. See, e.g., Court of Amsterdam 21 November 2022, ECLI:NL:RBAMS:2022:6800, para 5.1.8.
100. Court of Antwerp (appeal) 14 June 2023, no. 2022/CO/418, unpublished.
101. When special investigative powers are applied, the indictments chamber of the court has to supervise the secret methods used, as they are part of a secret file to which the defence does not have access.
102. On this topic, see the PhD research (2023) of Lisa Urban on Police-Hacking Techniques in Criminal Investigations – A Comparative and European Analysis, University of Luxemburg and KU Leuven (not published).
103. Stoykova (n 43) 7, points out the content of messages must at least be accompanied by digital forensic metadata and interpretation.
104. See, e.g., Court of Amsterdam 24 November 2022, ECLI:NL:RBAMS:2022:7082 and Court of Gelderland, 11 April 2023, ECLI:NL:RBGEL:2023:2011.

investigation. The question of whether a dataset should be disclosed, must be reviewed with regard to the three different datasets.[105]

As for the raw dataset, there is no obligation to disclose all information, especially not when law enforcement authorities did not review the relevance of the data themselves.[106] When the raw dataset is searched and thereafter filtered, using specific search terms to create a secondary dataset, it could be necessary to include the defence in this process.[107]

The ECtHR does not consider it necessary that the defence can use the search engine or any analytical software programs themselves: they can also provide law enforcement authorities with search terms. In that sense, a specific request to filter the raw dataset using specific search terms is also a safeguard against fishing expeditions.[108] In *Sigurðður Einarsson and others*, the Court found that a procedure whereby the prosecution itself attempts to assess the importance of undisclosed information to the defence and weigh this against the public interest in keeping the information secret – and does not involve the defence in this assessment – does not provide for a fair trial.[109] The defence needs to have the opportunity (a) to be involved in the definition of the criteria for determining what may be relevant and (b) to conduct further searches for exculpatory evidence.[110]

The tertiary dataset contains information that is relevant to a single case. For this type of dataset, the general rule is clear: this data can be used against the suspect, and should be disclosed.[111]

Lastly, the defence should have an 'effective opportunity' to access and analyse the data.[112] To make any discovery possible, it seems necessary to provide the defence with readable (i.e., not encrypted) data for review. Alternatively, the defence can be provided with access to the e-discovery program in which the data is made accessible on the premises of law enforcement authorities.[113]

In sum, all information that is deemed relevant in a particular case and that can be used against the suspect in a criminal case (the tertiary dataset), should be disclosed to the suspect. In addition, the defence should have sufficient facilities (an 'effective opportunity') to access and analyse the data. The defence can request and should motivate why they require further access to the secondary dataset. Then, when the Public Prosecution Service denies access to the data, they must motivate this, for example because of ongoing (other) criminal investigations or risk of reprisals for individuals who are also part of the dataset.

105. Oerlemans and van Toor (n 30) 323 with reference to Attorney-General Harteveld's opinion on the Ennetcom dataset, 8 March 2022, ECLI:NL:PHR:2022:219, para 6 and further; C. Van de Heyning, 'Not all that glitters is gold: een effectief recht op tegenspraak in tijden van bulkdata', *T.Strafr.* 2021 (4) p. 195-201. See, similarly, ECtHR 4 June 2019, no. 39757/15, ECLI:CE:ECHR:2019:0604JUD003975715 (*Sigurður Einarsson and Others/Iceland*). See also Attorney-General Paridaens' opinion about access to EncroChat and SkyECC data, 9 May 2023, ECLI:NL:PHR:2023:477, paras 5.7.16-5.7.21.
106. ECtHR 4 June 2019, no. 39757/15, ECLI:CE:ECHR:2019:0604JUD003975715 (*Sigurður Einarsson and Others/Iceland*), para 90.
107. Ibid.
108. Ibid.
109. Ibid, para 91.
110. Ibid, paras 90-91. ECtHR 25 July 2019, no. 1586/15, ECLI:CE:ECHR:2019:0725JUD000158615 (*Rook/Germany*), paras 67 and 72.
111. See ECtHR 25 July 2019, no. 1586/15, ECLI:CE:ECHR:2019:0725JUD000158615 (*Rook/Germany*), para 58.
112. See ECtHR 25 July 2019, no. 1586/15, ECLI:CE:ECHR:2019:0725JUD000158615 (*Rook/Germany*), paras 63, 67 and 70 and ECtHR 4 June 2019, no. 39757/15, ECLI:CE:ECHR:2019:0604JUD003975715 (*Sigurður Einarsson and Others/Iceland*), para 91. See further R. Stoykova (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, *49*, 105801.
113. Attorney-General Harteveld's opinion on the Ennetcom dataset, 8 March 2022, ECLI:NL:PHR:2022:219, para 6.15.

In practice, the raw dataset is not disclosed to the defence. In the Sky ECC operation, the dataset is too large to review the relevance of all messages for law enforcement authorities, and requests to obtain access to the full dataset are always denied.[114] In Belgium, the minister of Justice himself has been summoned to disclose the full criminal file of the Sky ECC investigation, but that claim has been declined.[115] Finally, the Antwerp Court of Appeal found that revealing the entire dataset containing all intercepted Sky ECC communications in a specific criminal case would lead to a serious and non-acceptable violation of the right to privacy of Sky ECC users who are not connected to the criminal case at hand. It would also violate the secret nature of a criminal investigation. Therefore, the request was declined.[116] In the Netherlands, the defence has access to the tertiary dataset used in the criminal case against a suspect. The defence can request and should motivate why they require further access to (part of) the secondary dataset, to which the Public Prosecution Service has to respond. The defence can even use the same Hansken platform as law enforcement authorities use.[117] At first, this was only possible on the premises of the NFI in the Hague, but this is now also possible remotely.

## Impact of human rights violations

From the analysis above, we can see that bulk data interceptions in criminal investigations can in principle be reconciled with the right to privacy and the right to a fair trial, on the condition that certain requirements, such as equality of arms, are met.

At the same time, it is possible that bulk interception, such as in the Sky ECC operation, leads to a violation of the right to privacy. For example, when a disproportionate amount of data of users of a grey infrastructure is targeted, when there are not enough safeguards in place for the further processing of the intercepted data during the investigation, or when data protection regulations are not respected. Violations of the right to a fair trial are not inconceivable either, e.g., when there is not sufficient transparency on how the evidence was obtained and handled, or when there are not sufficient means to mount a defence when it is suspected the data does not relate to the suspect or produces a false positive (i.e., that data is wrongly labelled as incriminating and relating to the suspect).

The question should be raised what the impact of such violations can be on ongoing investigations, in particular whether they can lead to the exclusion of the obtained evidence. This is both important for the defence in their client's interest and for law enforcement authorities that seek a conviction.

In general, the ECtHR keeps aloof when it comes to the assessment of evidence, as this is rather a task for the national judges, especially assessing the admissibility or weight of specific pieces of evidence.[118] In other words, the ECtHR provides for a large margin of appreciation on this matter by national judges. Nevertheless, some overall observations should be made. To do so, we distinguish

114. See footnote 107.
115. M. Eeckhaut, 'Verdachten Sky ECC vangen bot in kort geding', *De Standaard,* 9 januari 2023.
116. Court of Antwerp (appeal) 14 June 2023, no. 2022/CO/418, unpublished.
117. See Van Beek et al. 2015.
118. E.g. ECtHR 26 June 2016, appl. no. 47911/15, ECLI:CE:ECHR:2018:0626JUD004791115, para 54 (*Telbis and Viziteu/Romania*), ECtHR 31 January 2017, appl. no. 40233/07, ECLI:CE:ECHR:2017:0131JUD004023307, para 47 (*Kalnéniené/Belgium*), ECtHR 12 May 2000, appl. no. 35394/97, ECLI:CE:ECHR:2000:0512JUD003539497, para 34 (*Khan/United Kingdom*).

between privacy violations and fair trial violations, because they can have different consequences during trial. We also identify the pending cases at the ECtHR and the EU Court of Justice (CJEU).

## Privacy violations

The ECtHR has repeatedly found that evidence obtained through a violation of the right to privacy does not necessarily amount to a violation of the right to a fair trial.[119] Hence, privacy violations should not lead to the exclusion of evidence and could have little to no impact on ongoing and future possible criminal cases. However, this view should perhaps be nuanced due to CJEU case law. The CJEU decided that national courts should exclude evidence if a defendant is not in a position to comment effectively on the evidence and if the evidence pertains to a field of which the judges have no knowledge and is likely to have a preponderant influence on the findings of fact.[120] The impact of this case law, however, is not entirely clear.[121]

In a Belgian Sky ECC case, the Antwerp Court of Appeal acknowledged that the right to privacy had been violated, as some of the collected data were retained under a data retention law that had been annulled in the meantime. In light of the above-mentioned case law of CJEU, the court found that the reliability of the data was not at stake and that the defendants had had the opportunity to challenge the data. It concerned data on several IMEI numbers that are not subject to interpretation and do not demand further scientific investigation. Moreover, the seriousness of the criminal offences at stake outweighed the privacy violation. Finally, the data was in no means decisive to the conviction. As a result, the evidence was not excluded.[122]

## Right to a fair trial violations

Violations of the right to a fair trial may have serious consequences for the outcome of an investigation. Not only can evidence be excluded from the procedure, e.g., when evidence is not reliable, but a violation of the right to a fair trial can also render the procedure as a whole inadmissible or lead to the acquittal of suspects, e.g., when the defendant has not had proper access to the evidence.[123]

## Pending cases

It remains to be seen whether these general principles on bulk interception will be upheld in future case law of the European courts. Whereas it may take years before those courts will decide on this matter, we highlight two pending cases that are particularly relevant in this context.

119. E.g. ECtHR 31 October 2017, appl. no. 22767/08, ECLI:CE:ECHR:2017:1031JUD002276708, para 50, (*Dragoş Ioan Rusu/Romania*) ECtHR 31 January 2017, appl. no. 40233/07, ECLI:CE:ECHR:2017:0131JUD004023307, para 50 (*Kalnénienė/Belgium*), ECtHR 12 May 2000, appl. no. 35394/97, ECLI:CE:ECHR:2000:0512JUD003539497, para 40 (*Khan/United Kingdom*).
120. CJEU 6 October 2020, appl. no. C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, para 227 (*La Quadrature du Net*).
121. For a more detailed analysis, see M. Panzavolta & E. Maes, 'Exclusion of evidence in times of mass surveillance. In search of a principled approach to exclusion of illegally obtained evidence in criminal cases in the European Union', *International Journal of Evidence & Proof* 26.3 (2022), p. 199-222.
122. Court of Antwerp (appeal) 14 June 2023, no. 2022/CO/418, unpublished.
123. Quezada-Tavárez, P Vogiatzoglou, and S Royer (n 91) 531-551.

First, there is a case pending at the ECtHR about ByLock. This smartphone application allowed users to communicate via a private, encrypted connection. The application had hundreds of thousands of users, until it was permanently shut down by Turkish authorities in 2016.[124] The applicant complains that the evidence, including information from his ByLock application, was collected, retained, and processed in violation of his right to respect for private life. Additionally, he complains that he was convicted on the basis of unlawfully obtained evidence, to which he did not have access, and which was not directly examined by the domestic courts, in violation of the principle of equality of arms and adversarial proceedings. The Grand Chamber has been invited to look into these issues in the near future.[125]

Second, the Landgericht Berlin requested a preliminary ruling to the CJEU on the EncroChat operation, which also involved the bulk interception and bulk collection of communications at a French internet service provider. Among other questions, the Landgericht asks the EU court whether the same German legal standards must apply when the evidence-gathering activities under an EIO took place in a different country (i.e., France) and what the consequences are when the integrity of the intercepted data cannot be verified by the authorities in the executing State by reason of blanket secrecy.[126]

## Regulating data-driven criminal investigations

In this article, we examined how data-driven criminal investigations can be (better) regulated with respect to the right to privacy and the right to a fair trial. The Sky ECC operation illustrates a law enforcement practice in which intelligence and criminal investigations have become intricately intertwined, potentially spawning hundreds, if not thousands, of criminal cases from a single activity involving bulk data collection.

We posit that Sky ECC may serve as a precursor to future operations in which law enforcement authorities target similar 'grey infrastructures', employing investigative techniques such as the seizure of servers, hacking, or the interception of communications, or all of these at the same time. However, law enforcement authorities must tread carefully on the fine line between intelligence gathering and criminal investigation. There is a danger that the main objective becomes a fishing expedition, because the sought-after data may be a treasure trove for other criminal investigations, but not sufficiently related to the investigation at hand. There is also the risk of a slippery slope, as it is unclear what proportion of criminal activity makes an infrastructure exactly 'grey' and thereby a potential target for law enforcement agencies.

When regulating data-driven investigations, the main take-away of our analysis should be that a warrant authorising acquisition of the data is not enough. The ECtHR requires that data protection regulations are also applied and overseen by independent and effective oversight bodies. Therefore, criminal procedural law, which regulates the collection of data, and data protection law, which regulates the processing of data, are connected and intertwined. When dealing with the lawfulness of data-driven investigations, States should take this into account and take steps to adequately protect

124. Reuters, 'Turkey coup plotters' use of 'amateur' app helped unveil their network' (*The Guardian,* 3 August 2016) <https://www.reuters.com/article/us-turkey-security-app-idUSKCN10E1UP> accessed 1 October 2023.
125. On 3 May 2022, a Chamber of the Court relinquished jurisdiction in favour of the Grand Chamber in the case no. 15669/20 (*Yalçınkaya/Turkey*).
126. See C-670/22, request for a preliminary ruling to the ECJ EU by the Landgericht Berlin (Germany) on 24 October 2022.

the right to privacy. Considering the substantial impact on the right to privacy in data-driven operations like the Sky ECC case, we expect data protection authorities to exercise vigilance on this emerging reality in law enforcement practice.

Our analysis of case law in Belgium and the Netherlands shows that there is limited case law available in which the use of algorithms, AI, key word indexes, or network analyses have been challenged by the defence. It is possible that the defence refrained from arguing about this or did not effectively articulate the relevance of an argument about this to the court. However, it is clear that digital evidence is not 100% reliable and mistakes can be made, also by use of software and data analytic techniques. Building upon the work of ourselves and others, we have demonstrated that the right to a fair trial imposes obligations for law enforcement authorities and public prosecutors with respect to (1) *transparency* regarding the collection and analysis of the data, (2) the *reliability* when this data is used as evidence in criminal proceedings, and (3) facilitating *access* to the data that is used against the suspect.

In the Sky ECC operation, state authorities seemed to be reluctant, especially at first, to disclose investigative methods that were used to collect the data, and there is limited information available about how the data is processed. Some national courts, e.g., in Belgium and in the Netherlands, have accepted this situation, relying on the principle of mutual trust and assuming the lawfulness of data collection in France. Clearly, the subsequent analysis of data after the collection by law enforcement authorities is fully subject to the principle of the equality of arms, as part of the right to a fair trial.

The defence should have the opportunity to have knowledge and pose inquiries regarding the means by which evidence is obtained. This may serve as a partial remedy for the lack of transparency. In practice, it is noteworthy that many courts do not only rely on the content of Sky ECC messages linked to the suspect, but also base their decision on other materials obtained through alternative investigative methods, such as location data, data from seized cryptophones, and testimonial evidence. Access to datasets is also an integral part of the principle of equality of arms. The practice in the Netherlands, in which the defence can access data related to their clients through the same forensic platform utilised by law enforcement authorities, merits attention of other states. This serves as a best practice for facilitating access to data to the defence, as part of the right to a fair trial.

Finally, we emphasise that violations of the right to a fair trial may have serious consequences for criminal proceedings, since they may lead to the exclusion of evidence. Therefore, we anticipate an ongoing discourse surrounding the transparency and reliability concerns in operations like Sky ECC. Dealing with these questions will require both technical and legal expertise to navigate these recurring issues in the evolving digital landscape. This endeavour is essential, because the Sky ECC operation will definitely not be the last of its kind.

## Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

## ORCID iD

Jan-Jaap Oerlemans https://orcid.org/0000-0002-7854-8047