

Legal aspects of the EncroChat- and SkyECC operation

Prof. dr. J.J. Oerlemans

Endowed professor of Intelligence and Law – Utrecht University

About me

- Endowed professor of Intelligence and Law at Utrecht University
- Obtained my PhD in 2017. Dissertation 'Investigating Cybercrime'. Also: five years experience at the IT security company Fox IT, Dutch Defence Academy and WODC.
- Now: senior researcher at the Dutch Review Committee for Intelligence and Security Services and a member of the Cybercrime expert group for the Court of Appeals in The Hague.



BRILL
NIJHOFF

EUROPEAN JOURNAL OF CRIME, CRIMINAL LAW AND
CRIMINAL JUSTICE 30 (2022) 309–328

European Journal of
Crime, Criminal Law
and Criminal Justice
brill.com/eccl

Agenda

1. Background of the cryptophone operations
2. Legal aspects of the EncroChat operation
3. Legal aspects of the SkyECC operation
4. Human rights aspects of these cryptophone operations
5. Discussion!

Legal Aspects of the EncroChat Operation: A Human Rights Perspective

J.J. Oerlemans

Endowed professor of Intelligence and Law, Willem Pompe Institute
for Criminal Law and Criminology, Utrecht University, The Netherlands
jj.oerlemans@uu.nl

D.A.G. van Toor

Assistant professor, Willem Pompe Institute for Criminal Law and
Criminology, Utrecht University, The Netherlands
d.a.g.vantoor@uu.nl

Abstract

In the EncroChat operation, French law enforcement authorities collected over 120 million messages from 60.000 EncroChat users. They cooperated with Dutch law enforcement authorities and Europol in a Joint Investigation Team. In the Netherlands, EncroChat data has already been used in over 200 criminal cases.

This article examines what lessons can be learned from the Dutch experience with the EncroChat operation from a human rights perspective, in particular the right to a fair trial.

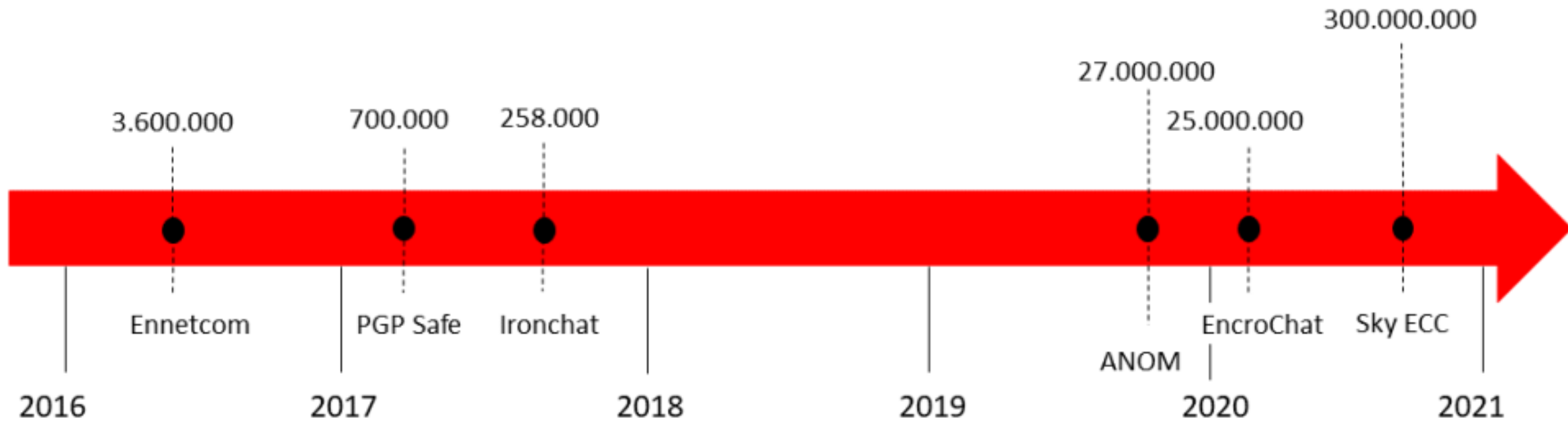
Data driven criminal investigations & the EncroChat- and SkyECC operation

Data driven investigations

- The EncroChat and SkyECC operation can be explained from the concept of 'data driven investigations'. The investigation starts by analysing large datasets acquired in previous investigations.
- This concept is developed by researchers from Team High Tech Crime of the Dutch police. (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 Serving the Public Interest," in Third INTERPOL-UNICRI Global Meeting on AI for Law Enforcement. 2020).
- In their paper, they urge law enforcement authorities to 'strategically acquire datasets' during criminal investigations for analysis later. Think of a subscriber database and transactional database from darknet markets for example.
- The goals of these operations is not just the acquisition of data to produce evidence in court, but to 'fight crime', like disrupting online operations of organised (cyber)crime.



Cryptophone operations



EncroChat

- In 2020, French and Dutch law enforcement authorities started a JIT to investigate criminal activities of both EncroChat and its users. Europol was also part of the JIT.
- In April 2020, French law enforcement authorities gained remote access – using an implant (hacking tool) uploaded from servers located at the ISP ‘OVH’ in Roubaix, France – to tens of thousands of cryptophones. Stored data on these phones was then copied and send back to law enforcement authorities.
- Then, approximately 115 million messages were intercepted.
- Metadata and content data, as well as images (copies) from servers where shared with Dutch law enforcement authorities and Europol.



Legal aspects

- The French Gendarmerie led the investigation under the supervision of the magistrates of the 'juridiction interrégionale spécialisée' (jirs) of Lille.
- A French judge authorised the use of the interception tool on 30 January 2020.
- The hacking tool (implant) was developed and deployed by the 'Direction générale de la Sécurité extérieure' (DGSE). The interception tool was reportedly developed by the 'Service Technique National de Captation Judiciaire' (STNCJ) in France.
- Later, the French 'Conseil Constitutionnel' *did not* consider the interception in the EncroChat in violation of the French Constitution (Conseil Constitutionnel 8 april 2022, nr. 2022-987)

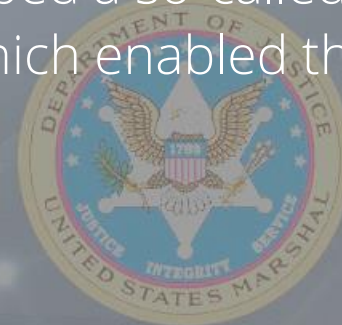
THIS WEBSITE HAS BEEN SEIZED

SkyECC

- In December 2019, French, Belgian and Dutch law enforcement authorities started a JIT to investigate SkyECC and its users.

- From 18 November 2020 until 8 March 2021 – after careful planning and brief interception and test to decrypt data – a total of **1 billion messages** were intercepted at the ISP 'OVH' in Roubaix, France.

- Dutch technicians developed a technique to copy 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.



Legal aspects

- A French judge then authorised the interception from 18 December 2020 until presumably until approximately 9 March 2021, the date law enforcement authorities made the Sky ECC operation public.
- The decryption technique was shared with French law enforcement authorities, who required 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 Code Pénal.
- The data is then actually processed/analysed and sometimes used as evidence in criminal investigations.

Data analysis and fundamental rights

Data analysis techniques used in Hansken

- Content is searched based on *key words* and filters (relating to drug trafficking or violent crimes, for example).
- Metadata is used to for network-analysis and create time lines.
- Incriminating messages are often cited in case law and used as evidence.

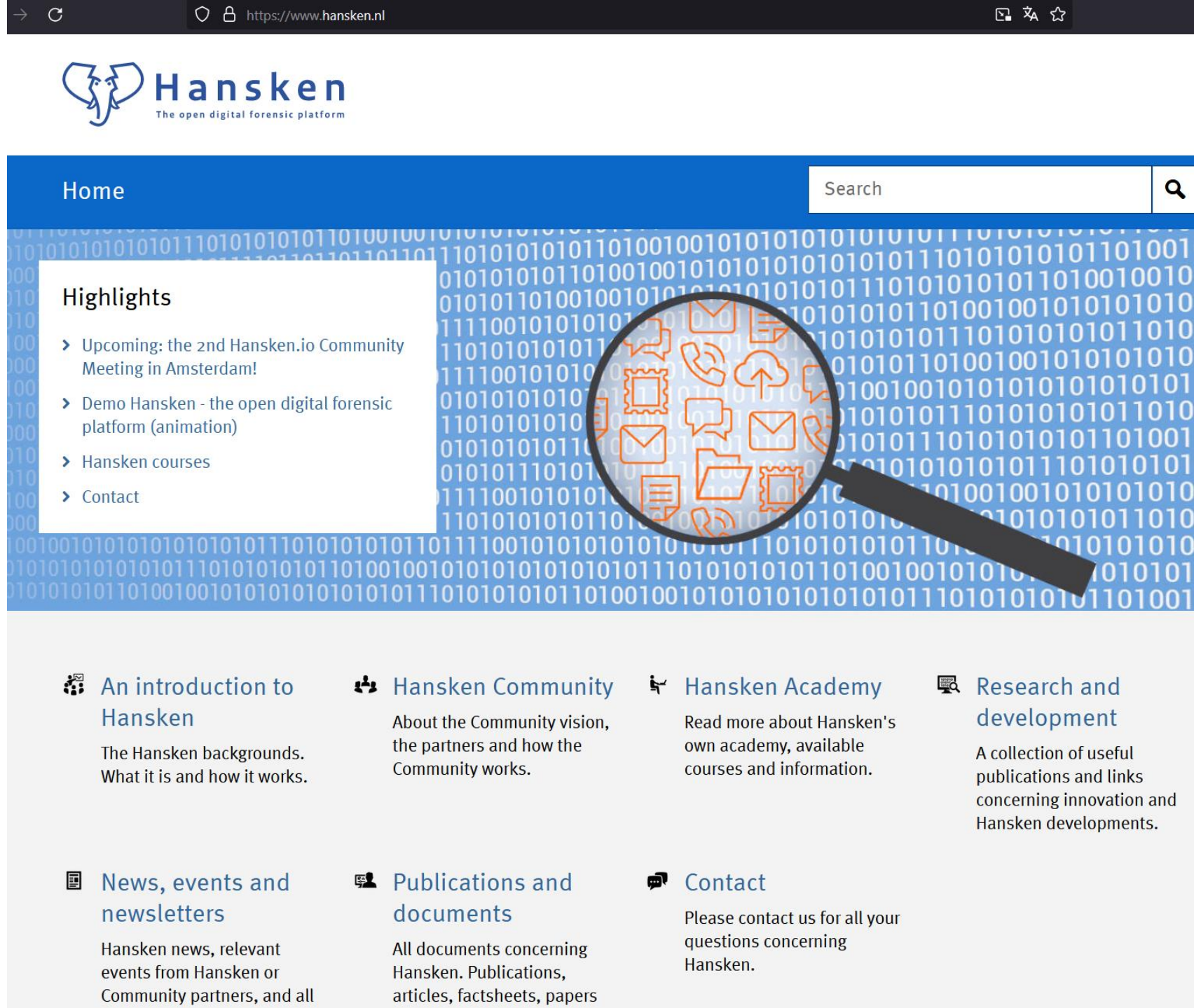


Tekst Christel van der Meer & Meike Willebrands

In onderzoeken naar zware criminaliteit neemt de politie vaak gegevensdragers zoals mobiele telefoons, computers en harde schijven in beslag om te speuren naar belastend bewijsmateriaal. Vaak gaat het om zoveel data dat het onmogelijk is om die

Processing of cryptophone data

- The Dutch National Forensic Institute developed a platform (called 'Hansken') to store, index and analyse the data (using "dozens of forensic tools" simultaneously).
- Europol created a 'Operational Task Force' (OTF) (codenames 'Emma') to analyse the 115 million messages. It was 1.3TB (terabytes) of data. They created 700 'intelligence packages' to 123 countries.



The screenshot shows the Hansken website homepage. At the top, there is a navigation bar with 'Home' and a search box. Below the navigation bar is a large blue banner with a background of binary code (0s and 1s). In the center of the banner, there is a magnifying glass icon over a cluster of orange icons representing various digital forensic tools and concepts like envelopes, folders, and communication symbols. Below the banner, there is a 'Highlights' section with a list of items: 'Upcoming: the 2nd Hansken.io Community Meeting in Amsterdam!', 'Demo Hansken - the open digital forensic platform (animation)', 'Hansken courses', and 'Contact'. Below the highlights, there are four columns of content, each with an icon and a title: 'An introduction to Hansken' (with a document icon), 'Hansken Community' (with a group of people icon), 'Hansken Academy' (with a graduation cap icon), and 'Research and development' (with a magnifying glass icon). Below these are three more columns: 'News, events and newsletters' (with a newspaper icon), 'Publications and documents' (with a person icon), and 'Contact' (with a speech bubble icon).

Case law & first points of discussion

- Dutch Supreme Court ruled that the principle of mutual trust between states applies in the EncroChat and SkyECC operation (13 June 2023, ECLI:NL:HR:2023:913).
- This means that decisions by authorities abroad that form the basis for investigations conducted abroad must be respected by the Dutch courts in Dutch criminal proceedings. It should therefore be assumed that the relevant investigations by the authorities abroad have been conducted lawfully, in other words, in accordance with the laws of the foreign state concerned.
- *Is it comparable to the German approach?*
- Part of the discussion whether the Dutch warrant for the interception and/or hack was required. Answer is: not required, but ok.

The right to privacy

- Can we learn from case law relating to bulk interception?
(-> ECHR 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch et al./The United Kingdom*))
- Not entirely the same, but...

It may offer important insights for future case law.

Our conclusions

- (in: J.J. Oerlemans & S. Royer, 'The future of data driven criminal investigations in light of the Sky ECC operation', *New Journal of European Criminal Law* 2023 (forthcoming)).
- A warrant for bulk interception is not enough! There should be additional safeguards 'down the line', such as 'procedures to be followed for selecting, examining and using intercept material'.
- In the Netherlands, an additional warrant is requested when a subset of data is created for a new criminal investigation. (comparable to a selection mechanism and may be regarded as a best practice).
- *Open questions:* Are data protection authorities involved? Are there retention periods? What about data that is 'never touched'?

The right to a fair trial

1. The public prosecutor must provide (a degree of) **transparency** about the operation and collection of evidence. That way, defence attorneys can object to this. This relates to the principle of **equality of arms**.
2. The right to a fair trial also provides a legal basis to test the **reliability** of the evidence and the method of acquisition.
3. The right to a fair trial enables the defence – to a certain extent – to **access** the data that may be relevant in the trial against their client. (See also ECtHR 4 June 2019, ECLI:CE:ECHR:2019:0604JUD003975715, (*Sigurður Einarsson and Others/Iceland*))



Fair trial questions

- Dutch Supreme Court in their decision of 13 June 2023 that (ECLI:NL:HR:2023:913):
- Finally, the Dutch criminal courts must assume that the investigation abroad was conducted in such a way that its results can be relied on. Only further consideration when there are 'specific indications to the contrary'. The defence must argue why the data is not reliable.
- Prof. Bart Schermer and I argue the principle of mutual trust does not extend tot analysis phase of the data. Defence is in a Catch 22: they can't argue when the information is not there.
- In essence, it should be explained how LEA and the Public Prosecution Office came to the evidence (the result of data analysis). The reason is that digital evidence is – also – not 100% reliable. 'False positives' may occur.
- But how should it be explained and what detail? We are not sure yet...

2244

Wetenschap

Antwoorden op prejudiciële vragen in de EncroChat- en SkyECC-zaken

Jan-Jaap Oerlemans & Bart Schermer¹

Forthcoming..

Conclusions

- For the Dutch law enforcement authorities, the future is bright! The Dutch Supreme Court in a way legitimised these kind of 'data driven investigations' in which bulk datasets are obtained.
- However, I expect more court proceedings relating to the right to a fair trial and equality of arms.
- There may be upcoming cases in the ECtHR and EU Court of Justice. See C-670/22, request for a preliminary ruling to the ECJ EU by the Landgericht Berlin (Germany) on 24 October 2022.

Thank you!

j.j.oerlemans@uu.nl
jjoerlemans.com