OPEN LETTER OF CONCERN

We, the undersigned, are independent lawyers, advocates and litigators practising in criminal law across the continent of Europe and civil society. We have felt impelled to come together as never before, to send this letter of concern in respect of the use of evidence in each of our countries, obtained from the infiltration of the messaging platform 'EncroChat' by the French Gendarmerie.

EncroChat was a secure communications network. Participants obtained Encro-phones from agents; a subscription would be paid in order to receive a handset and the user would be assigned a unique 'handle' or username. The phone used a SIM card capable only of handling data, which was issued by the Dutch telecommunications company KPN. EncroChat devices could not connect to the telephone network; users could only communicate with other EncroChat users.

Since 2016, law enforcement agencies across Europe have suspected that EncroChat was used as a communications platform for organised criminal activity. It is understood that the French Gendarmerie managed to develop a way of obtaining EncroChat handle communications (and other data) by interception *and/ or* hacking. We are told that this began on 1st April 2020 and data was harvested and transmitted to a data hub controlled by the French Gendarmerie. The data was then transferred to Europol, which organised the processing and transfer of data to the relevant law enforcement agencies across Europe through EU police and judicial cooperation mechanisms. As a result, thousands of people across Europe have been arrested and prosecuted based on evidence obtained during the hack.

It is clear that law enforcement agencies in each of our countries should have the tools required to investigate serious organised crime, such as the type revealed by the EncroChat hack (with the use of sophisticated methods, in cooperation with agencies of fellow EU Member States and other international partners). However, investigative tools have serious implications on people's fundamental rights, and they must therefore be rightly framed in law, with adequate procedures and safeguards.

The EncroChat infiltration has revealed worrying trends that cause us deep concern.

1. **No right to a fair trial:** The manner of the infiltration has been suppressed under the shroud of a claim of national defence secrecy by the French authorities. This has made it impossible for those accused of crimes, to check the accuracy, authenticity, reliability and even the legality of the evidence used against them. Each of our countries' legal systems has specific, robust and world-leading procedures for dealing with sensitive information, and yet there has been a refusal by the French authorities to reveal its technique. This is unprecedented in our collective experience; it breaches EU standards on procedural safeguards; European Court of Human Rights caselaw; and international best practice guidance. It has generated a huge amount of otherwise avoidable litigation and driven a surge in prison populations through recourse to pre-trial detention. More troublingly, judges are forced to make decisions about complex technical matters based on inference as opposed to being provided with the complete, unadulterated evidence, to which they are entitled.

2. **Lack of transparency:** An emerging picture of inconsistent, even completely contradicting information has been provided by various law enforcement agencies across Europe, accompanied by an overall refusal by law enforcement agencies to liaise with each other in the ongoing disclosure process in current prosecutions. This raises serious concerns about the integrity and reliability of the evidence on which prosecutions across Europe are based.

3. **Extraterritorial effects:** The likelihood is that the hack involved an exercise by the French Gendarmerie of extraterritorial jurisdiction which breached the sovereignty of individual Member States.

4. **Privacy implications:** The likelihood is that the hack involved the fundamental rights of thousands of individual citizens of Member States, including at least the right to respect for private and family life, the right to freedom of expression and the right to protection of personal data, while an adequate review by an independent judicial authority is completely absent in this regard.

We wish to draw our concerns to the EU institutions, in view of the roles of two EU agencies, Europol and Eurojust, in this operation including by way of a joint investigation team (see e.g. here[1]). As the EU is set to further expand Europol's mandate pursuant to the European Commission's proposal of December 2020[2], we urge the EU to integrate safeguards and oversight mechanisms to help prevent fundamental rights violations.

Therefore, we call on the European Commission and the European Parliament to implement the following measures as a matter of urgency:

a. Ask all concerned Member States to impose a moratorium on (new) prosecutions until evidence is duly disclosed, as required to safeguard the right to a fair trial;

b. Require Europol to provide explanations in the related ongoing national proceedings on its role in processing and analysing the data; and in sharing the data (including which countries were involved and when), with a view to supporting the courts' oversight role;

c. Demand that the European Parliament to set up an inquiry committee pursuant to Article 226 of the Treaty on the Functioning of the EU to look into breached of EU law in the context of the EncroChat investigation;

d. As law makers, adopt appropriate safeguards to ensure that data processed and shared via EU police and judicial cooperation mechanisms cannot be subject to a blanket assertion of national defence secrecy as done by the French authorities, which undermines EU defence rights, starting with the proposal to revise Europol's mandate.

In the EU legal framework, it is recognised that the fundamental rights of all people, including suspects and accused persons, must be upheld and protected. We are very concerned that the current handling of the EncroChat issue threatens the Rule of Law and fundamental rights protected by EU law that, if it is allowed to pass unchecked, this sets a worrying precedent.

From Belgium: J. van Laer
From France: R. Binsard, G. Martine & A. Boret
From Germany: C. Lödden, L.M. Barczyk, O. Wallasch, M. Rakow & D. Scheibner

[1] https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0796.

From the Netherlands: J.C. Reisinger, R.D.A. van Boom, Y. Quint, R. Poppelaars & B. Janssen
From Norway: M.O. Dietrichson & A. Krasniqi
From Sweden: J. Grahn
From the United Kingdom: T. Schofield, I. Jinnah, O. Cook, S. Csoka QC, S. Choudhry & F. Hussain

For the Civil Society: Fair Trials