Universität Bremen

IGMR
Institut für Informations-,
Gesundheits- und Medizinrecht

Universität Bremen | Postfach 33 04 40, 28334 Bremen
IGMR | **FB06**

Fachbereich 06
Rechtswissenschaft

Prof. Dr. Dennis-Kenji Kipker

GW 1, Raum A 2010
Universitätsallee
28359 Bremen

Tel. 0421 5905 5465
Fax 0421 218 66052
kipker@uni-bremen.de

www.igmr.uni-bremen.de
igmr@uni-bremen.de

Bremen 2. November 2022

EncroChat and the "Chain of Custody".

Digital Investigations as a Test for a Right to a Fair Trial?

Dennis-Kenji Kipker/Hauke Bruns

IGMR
Institut für Informations-, Gesundheits- und Medizinrecht

Facts and content of the study:

Criminal proceedings are currently being pursued in numerous German cities on the basis of an analysis of EncroChat datasets from France. Although the legality of obtaining the data records and their usability have been discussed for quite some time and are partly questioned, the EncroChat information has so far been taken over by courts and public prosecutors largely unchecked. This study presents the technical background of the EncroChat hack and explains, on the basis of the so-called "chain of custody," the considerable constitutional weaknesses of the current investigation procedures and what must change in the future, also in terms of legal policy beyond EncroChat, if digital investigation procedures are to be operated in conformity with the constitution.

Key Findings:

- Crime courts are required to satisfy themselves of the admissibility of data processing in encro-chat procedures. This includes all processing steps and also the raw data sets that are currently kept secret.

- The right to a fair trial under the rule of law requires that the defense be granted comprehensive access. This also includes those documents that were created for the purpose of the investigation but were not taken into the file. A blanket refusal to allow access on the grounds of "jeopardizing ongoing investigations" is not a permissible argument. This is the only way to ensure transparency of information between the state and its citizens. The current investigations therefore do not represent such a fair and constitutional procedure.

- In terms of legal policy, it is necessary to demand that the standards for constitutional proceedings in the case of evidence collected by government agencies be set higher than they have been to date, especially for the use of digital investigative tools. Preventive protection of fundamental rights requires that investigating authorities make it possible to exercise the rights of the defense at a later stage, even in the case of infiltration of technical systems or other targeted data collection for the purposes of criminal prosecution. This necessarily means that the entire chain of custody must be transparently logged and accessible.

I. The EncroChat system and the hack

EncroChat is an encrypted communication technology provider founded in 2015. The provider provided technically modified smartphones (hardware) as well as a communication application (software). The product aimed to be able to communicate as securely as possible in encrypted form via text messages. To this end, the hardware was modified to the extent that components not necessary for this purpose, such as GPS sensors, microphones, cameras and the like, were removed, i.e. all device components that are not necessary for pure communication but enable or facilitate the tracking or monitoring - e.g. eavesdropping - of users. The software for sending text messages, EncroChat, is based on signal protocols and thus has end-to-end encryption. The devices also had a so-called "wipe function", with which all content could be deleted shortly after entering a PIN.

After French investigative authorities said they had encountered EncroChat devices on several occasions during investigations since 2017, they applied to the investigating judge in Lille, France, to authorize a hack of the EncroChat provider's servers. The authorization was granted by a decision dated March 20, 2020. The technical background to the hack itself is largely unknown and is being kept under wraps by the French authorities as a "military secret." However, it seems certain that the communication data was intercepted by malware disguised as an update that found its way onto the end devices before encryption and redirected to servers belonging to the authorities. In this way, communication data of tens of thousands of users could be siphoned off.

From the raw data obtained in France by French authorities, the information was mainly transferred to Excel spreadsheets. Already in France, the data was probably also filtered for the first time. Since the end devices only contained one-sided communication content, complete "conversations" were also reconstructed from the data obtained for the first time. Via Europol, the compiled data then reached the competent authorities in the respective countries in which the users were suspected; in Germany, the data was made available to the BKA. The General Public Prosecutor's Office in Frankfurt a.M., in cooperation with the BKA, first opened an investigation file against unknown persons that included all the data. It then successively separated individual excerpts of the communication and transferred the data records to the relevant public prosecutor's offices with the request to open an investigation.

II. EncroChat data as legal evidence

The data obtained from the mass surveillance subsequently led to numerous criminal proceedings and served as the basis for initial judicial decisions. Arrest warrants were issued on the basis of this data, and the data was also used to assess whether there was sufficient suspicion of a crime in the first decisions to open proceedings. As a result, a dispute arose over the legal assessment of the hack and the subsequent data processing. The view expressed by defense attorneys in particular that the French authorities had investigated "out of the blue" and that the same thing would not be conceivable under the German Code of Criminal Procedure gave rise to the accusation of forum or authority shopping, which was also taken up in various media

reports. Some conclude from this that the use of evidence is prohibited, while others consider the data to be unusable upstream. While the former point to the principles of the rule of law and the individual-protecting provisions of international mutual legal assistance, the latter criticize the fact that a provision on the purposeful further use of data is necessary, but is not to be found in German criminal procedure law. Despite these dissenting voices in the literature and occasionally also in the case law, the higher regional courts nevertheless assume in their decisions that the data obtained can be used or that it can be used in advance.

However, assuming that the legal - and certainly not entirely unfounded - reservations in this regard are ignored, the question arises as to whether the skimming of data, often referred to as "data treasure," is at all suitable for use as evidence in criminal proceedings. After all, from the already legally and technically opaque acquisition of the data in France to its introduction into German criminal proceedings, the chain of evidence is long and can rightly be described as hardly traceable, especially in terms of data authenticity and data integrity.

III. Data as evidence in criminal proceedings

In order to gain more clarity on the question of the admissibility of the use of EncroChat data in criminal proceedings, the consideration has to start where the data is currently located and relevant: at the German criminal courts. In the individual proceedings, one relies here on the data concerning the respective defendant that reached Germany as an excerpt of the hack, often in the form of Excel tables.

It is obvious that the data material used has been processed many times in the meantime: First, the data was skimmed from the end devices with the help of programs, then stored, merged, sent several times, processed and compiled. The data then entered the official procedure and was further processed here, for example to delete "irrelevant" parts or to rearrange data for "better readability". Measured against the standards to be applied to data authenticity and data integrity, it therefore appears questionable whether the data are still capable of doing what they are actually supposed to do, namely to provide evidence of the commission of a crime.

1. The principle of the judicial duty to investigate

The court's duty to clarify the facts follows from Section 244 (2) of the Code of Criminal Procedure, according to which the facts must be clarified comprehensively on the one hand and ex officio on the other. This requires the collection of evidence. The chat messages are data that contain both text and photos. Such data is introduced into criminal proceedings by way of documentary evidence or visual evidence. However, digital data is at a much higher risk of (intentional) manipulation or (unintentional) alteration than ordinary evidence of this kind. Once the raw EncroChat data has been siphoned off, its integrity is continuously compromised during storage and especially during subsequent processing operations - especially if there is no continuous logging of changes made.

Data stored by the investigative authorities can be altered by third parties, i.e., by external intervention, as well as by the investigative authorities themselves. External interference can be countered by classic IT security measures, such as backup copies, defensive software, access authorizations, logs, etc. The risk of changes by investigative authorities can be reduced to a minimum. The risk of changes by investigating authorities themselves must also be minimized by technical and organizational measures during processing. To this end, IT forensics has been developed to ensure the integrity of processed data during evaluation and copying processes by introducing processing standards. Similarly, the German Code of Criminal Procedure (StPO) imposes special documentation requirements for technical investigative measures that interfere with the integrity of IT systems and the confidentiality of communication processes protected by fundamental rights, such as telecommunications surveillance and online searches, which contribute to the verifiability of the means used and the changes made, see Section 100a (6) of the German Code of Criminal Procedure (in conjunction with Section 100b (4) of the German Code of Criminal Procedure).

The records themselves can serve for the verifiability of integrity insofar as generally the (documented) changes made to the data stock can be traced. Furthermore, the system used and possible sources of errors in it can be checked, if necessary with the help of expert knowledge. In addition, the persons acting and involved in the supervision (four-eyes principle) can be questioned as witnesses to the processing operations carried out.

Data that has already been processed as such therefore has only very limited probative value. Accordingly, if data from a later processing stage, as in the case of EncroChat, is introduced as evidence in proceedings, the courts must, as a rule, also examine the (raw) data on which the further technical processing is based and, if necessary, have them examined by an expert.

2. The graduated requirements for standardized procedures

Case law lowers these requirements (only) for standardized data processing procedures and especially for those that precede fine proceedings. This is primarily the case for speeding violations that are determined with the help of standardized measurement procedures using calibrated measuring instruments. This is also approved by the Federal Constitutional Court, with reference to procedural economy. In this case, there is only a "reduced obligation on the part of the courts to clarify and explain the facts of the case".

However, these considerations should not obscure the fact that there is no general presumption that supports the correctness of a data processing operation. Instead, the lowered requirements are based on two essential premises, taking into account constitutional jurisprudence .

a) Fine (mass) proceedings

First of all, the cases in which raw data should not be used are on the one hand (only) fine proceedings with much less drastic consequences for the persons concerned, and on the other hand these are regularly mass proceedings in which a full review will not be possible for organizational reasons. Neither is the case for the EncroChat investigation proceedings. First of all, these are predominantly cases of narcotics crime and, in addition, possible violations of weapons or weapons-of-war regulations and thus criminal proceedings with a correspondingly

high threat of punishment. However, the fact that misdemeanor proceedings are mass proceedings that also involve a lesser degree of injustice and whose punishment is associated with far less drastic consequences for the defendant also seems to support the Federal Constitutional Court's view that the restriction of the duty to provide information is permissible. In addition, although a large number of defendants are currently facing accusations, the event as such, namely the hacking of the EncroChat system and the data obtained as a result, is unique and clearly delimitable, so that it is by no means the comparable situation of a standardized mass procedure to which lower test requirements would have to be applied in this respect.

b) Standardized procedures

It should also be noted that the processing of EncroChat data cannot be considered standardized. However, speed measurements are standardized insofar as there are standardized technical requirements for the measuring instruments used to generate the raw data sets, they have to undergo an approval procedure, they have to be calibrated on a regular basis and, finally, the persons involved have to be trained accordingly and instructed by means of operating instructions.

With a view to the digital data sets that are now being used for investigative and law enforcement purposes, the case of EncroChat is "uncharted territory" in this respect. First of all, it is completely unclear which technical procedures were used to collect the data. The procedure for carrying out the hack is neither obvious nor standardized, nor are the authorities currently making any efforts to clarify this. As far as can be seen, the processing operations that followed the collection were carried out in ordinary data processing programs that are also used by private users and do not provide any protection against loss or modification. There are also no indications that particularly technically skilled or trained personnel were significantly involved in the subsequent further processing.

Thus, in the EncroChat case, there is ultimately already no upstream guarantee for the correctness, completeness and authenticity of the data, as exists in contrast to this in the case of speed measurement systems. The case law, on the other hand, bases the justifiability of the lowered requirements for proof precisely on the existence of these facts, however, when it assumes that the "approval by the German Physikalisch-Technische Bundesanstalt" with simultaneous "use [...] within the scope of the approval specifications" offers a sufficient guarantee that the processing "also provides an error-free result in the individual case". This result can hardly be assumed for the extraction and further processing of the EncroChat data based on the considerations made before.

c) Interim result

Already because of the lack of a corresponding technical-organizational standardization of the collection and further processing procedure of the EncroChat data, the courts cannot refer back to the secondary data and assume the correctness of the processing procedures without further ado.

3. Increased requirements in the event of concrete indications of data changes

Moreover, the German Federal Constitutional Court does not allow the presumed correctness of the further processing of the raw data to be relied upon, even in the case of data obtained in fine proceedings with the aid of standardized measurement technology, insofar as there are indications that errors actually occurred during processing.

This cannot be excluded without further ado for the data obtained in the course of the EncroChat investigations either. The data records provide concrete indications of inconsistencies in content, for example, because only 3,000 duplicate messages could be detected in a data record comprising 16,000 lines. This is surprising because the French authorities stated that live chats and archived messages were intercepted. However, the messages would then have to have been siphoned off twice each from the sender's terminal and the recipient's terminal. So why some messages are stored twice, but otherwise only once in the Excel file, does not seem comprehensible against this background. This is even more obvious with the time stamps to the messages. There the documented time of the receipt of the message would lie partly before that of the dispatch, which cannot be explained however in particular by deviating time zones, since the time stamps at other place of the discussions did not exhibit such inconsistency.

The objections cannot be conclusively clarified without further inspection of the procedural files. However, the mere fact that such allegations exist and cannot be easily dispelled reveals clear weaknesses in the investigations and the data processing on which they are based. The trial court is therefore required to satisfy itself of the reliability of the data processing in the EncroChat proceedings.

IV. Indispensability of the reconstruction

As a result of the above findings, it is essential to revert to data from earlier processing stages of the EncroChat process. In the following, it is therefore to be examined which legal requirements are to be applied to such a reconstruction of the data.

1. Domestic (further) processing

The chain of processing of EncroChat data records is to be clarified by the courts due to the identified inconsistencies from the official duty to clarify, at least until the resolution of inconsistencies along the individual processing steps. This could be done in particular by means of motions for evidence filed by the defense, and officials with authority could be heard as witnesses. However, it is questionable whether this is sufficient, since technical processes such as the sorting out of individual data for each specific case cannot be conclusively investigated without full logging. For this purpose, it would be necessary to also examine the data of earlier processing steps.

The defense could prepare this by means of a comprehensive inspection. The principles of the Federal Constitutional Court on the rights of the defense should be referred to in this regard.

In its case law on the inspection of trace files in criminal proceedings and raw measurement data in fine proceedings, the court concludes from the right to a fair trial under the rule of law the right of the defense to inspect, apart from requests for evidence, such documents that were created for the purpose of the investigation but were not taken into the file.

The EncroChat data most recently found its way to the courts via the locally responsible investigative authorities and, before that, via the BKA and the General Public Prosecutor's Office in Frankfurt a.M. The latter, however, refuses to hand over large parts of the file, citing the threat to ongoing investigations.

According to the case law of the German Federal Constitutional Court, however, the defense has a fundamental right to be provided upon request with - in principle all - information that has arisen in the course of the investigation, regardless of whether it has been added to the criminal or administrative fine file or is available elsewhere. The aim is to establish "information parity in relation to the administrative authority". Furthermore, the Federal Constitutional Court rightly states in its decision on raw measurement data: "The requirement for fair proceedings [...] must be observed [...] by all [...] state bodies that influence the course of criminal proceedings, and accordingly also by the executive, insofar as it considers itself legally obliged not to release certain evidence".

The General Public Prosecutor's Office in Frankfurt a.M. is therefore also obliged in principle to grant access to files. In its previously cited decision, the Federal Constitutional Court itself immediately cites "constitutionally guaranteed interests such as the proper functioning of the administration of justice" as possible conflicting aspects, which is likely to result in a weighing of individual cases. However, in the case of the serious criminal offenses at issue here, and thus the drastic consequences of high penalties for those affected, only very weighty reasons are likely to be sufficient to deny access to the files. The general reference to the possible endangerment of other proceedings is by no means sufficient to meet this strict standard.

2. Foreign data processing and inspection of raw data files

When granting access to files, however, it must be taken into account that only parts of the collection and processing procedures of the EncroChat procedures are nationally known anyway. This brings us to the further problem of the processing of raw data. These are located in France and are currently kept under lock with reference to military secrecy. For data stored with French authorities, there is no obligation on the part of the authorities and no enforceability of such a claim. From a national perspective, documents relating to earlier processing operations, as well as the original raw data themselves, are thus to be regarded as non-existent.

3. Court case SaarlVerfGH Lv 7/17

The Constitutional Court of the Saarland, in a decision that has received much attention, considered the mere absence of raw measurement data to be a violation of the right to a fair trial under the rule of law in its manifestation as the right to an effective defense, and therefore considers a conviction in such a case to be out of the question. It follows from the aforementioned right that the defense must also be able to verify the existence and validity of the factual

basis of the accusation made against the accused. Accordingly, "the fundamental possibility of verifying an accusation based on technical processes and algorithms is part of a procedure under the rule of law". Even though the decision was made under state constitutional law, it is also based in particular on Article 6 (3) of the ECHR, and the guarantees are reflected in Article 20 (3) in conjunction with Article 2 (1) of the German „Grundgesetz“ (constitution).

The Saarland Constitutional Court's ruling has been widely criticized. However, this criticism is itself subject to doubts, but as far as can be seen is predominantly based on the special features of fine proceedings and standardized processing procedures and, finally, on the presumption of correctness that is at issue for the measurement results. As seen, all this is in no way transferable to the EncroChat data.

Therefore, only a criticism of the derivation of the Saarland Constitutional Court from the required equality of arms seems to be valid. According to the convincing jurisprudence of the Federal Constitutional Court of Germany, it is only a matter of establishing "information transparency in the relationship with the administrative authority". However, if - as in the case decided - no raw measurement data is available, there is also no disparity to be compensated, since the authority is not in a better position in this respect. The considerations on equality of arms are therefore not able to support the decision. Their further explanations seem to make the reproach, however, with regard to the omission of the technically quite possible storage of the raw measurement data. The right to effective defense is prima facie torpedoed by the omitted storage (without technical justification). Even if one might still argue for an overall view in fine proceedings and be of the opinion that the accusation to be made against the authorities would not have weighed sufficiently heavily, at least at that time, the Constitutional Court's assessment is convincing, at least for criminal proceedings.

Therefore, even in cases of clandestine infiltration of technical systems, such as in the EncroChat cases, the investigating authorities must be required to store raw data and, if necessary, to obtain it from foreign investigating authorities. In the present case, however, the authorities are apparently unable to obtain this information because the French state invokes military secrecy.

V. Approaches to deal with missing raw data

This leaves the case that raw data are simply not available and the preservation of the integrity of the data, especially when processed abroad, can therefore not be assessed. Consequently, the question arises as to how to deal with this situation of missing raw data. In any case, the principle of mutual recognition, which is frequently invoked in the German proceedings and which at most justifies legal assessments to be adopted, but not a general presumption of the correctness - let alone the actual correctness - of the implementation of any measure, cannot be relied upon.

1. Question of assessment of evidence

Instead, one approach could be to leave it at a question of evaluating the evidence in constellations such as the present one. Thus, in the absence of the raw data, the secondary data sets would have to be evaluated and, if necessary, examined by an expert in order to determine their probative value. An expert opinion from one of the criminal proceedings on EncroChat states in this context that the authenticity and integrity of the data can only be reliably confirmed if the mode of operation of the Trojan used in France is known and the raw data is inspected. Accordingly, the probative value in these proceedings is likely to be low and a conviction (solely) on the basis of the EncroChat data would appear highly questionable.

2. Question of utilization of evidence

However, the requirements for proceedings in accordance with the rule of law should be more stringent than they have been up to now for evidence collected by government agencies, especially for the use of digital investigative tools. The state is bound by fundamental rights and other constitutional guarantees, including the right to a fair trial. Accordingly, the state has duties to protect these rights in all its actions. In the manner of anticipatory protection of fundamental rights, the state must therefore be obligated to make it possible for the rights of the defense to be claimed at a later date, even in the case of infiltration of technical systems or otherwise targeted data collection for the purposes of criminal prosecution. As a result of the right to safeguard the rule of law and in order to ensure the effectiveness of the subsequent exercise of the rights of the defense, it should be obligated to secure the collection and storage of raw data, particularly in terms of data integrity and data authenticity, to make data processing traceable and ultimately to make it accessible to the parties involved. This is in line with the principles of current IT forensics for digital investigation methods. However, if the state fails to do this, it torpedoes the rights of the defense. This in itself should be seen as a violation of the right to a procedure based on the rule of law and should accordingly rule out usability. Otherwise, these procedural requirements, which are so important for digital investigative measures, would become "toothless tigers".

This thesis is also supported by the fact that even in the case of data that can be determined to be identical to the raw data, the accused must be given the opportunity to at least present exculpatory circumstances. It must therefore be ensured that even the raw data that is irrelevant from the point of view of the investigating authorities, but which could contain precisely those exculpatory circumstances, is made available. This applies even if there is no prior indication of such exculpatory circumstances.

The special features of digital investigations, which make interventions across national borders possible, and the inherent danger of shifting responsibilities, should prompt a broader view overall. It is also incumbent on the state to ensure that the rights of the defense are also protected in proceedings for international legal assistance. Normative guarantees can be considered here, as well as influencing the foreign authorities after the data has been collected. If the state fails to do so, it is responsible for the lack of raw data. Accordingly, if access to the raw data fails, its usability should also fail. In this way, "forum shopping" could be counteracted, at least in principle.

VI. Final result

The EncroChat procedures currently underway in many places not only suffer from considerable technical and organizational deficiencies with regard to data security, but are also highly questionable in terms of criminal procedure and constitutional law. As precedents, they should prompt the state to rethink the way it handles digital evidence and call for legal reforms. In criminal proceedings, for example, it seems impossible to base a conviction on mere data that merely originates from the end of a processing chain that is opaque from the very beginning, without raw data and without knowledge of the individual processing steps and the software used in the process. Rather, it is contrary to the right to a fair trial if data collected by the state is not made available to the defense in the form of the raw data, regardless of whether this is denied for legal reasons or not possible for factual reasons. Whether these are domestic or foreign state measures should be irrelevant. Anticipating the dangers of globalized criminal prosecution under the rule of law, it should not be to the disadvantage of the accused that the state makes use of international powers and obtains incriminating data from foreign sources of information that are in doubtful cases non-transparent and do not operate on a comparable basis of authority. Unsolicited data are not exempt from this rule either, since it is the German state's very own task to include the safeguards of the Constitutional Law in international mutual legal assistance agreements as well.