Rethinking Procedural Safeguards in the Digital Age

Bulk Surveillance, Artificial Intelligence, and the Need for Responses at the EU Level

Lorena Bachmaier *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

ABSTRACT

This article examines the impact of digitalisation, mass surveillance, and artificial intelligence (AI) on procedural safeguards in criminal proceedings in the context of the developments in the EU's Area of Freedoms, Security and Justice. The author argues that contemporary surveillance capacities are changing the way in which prevention, intelligence, and criminal investigation are related to one another. Prior to the commencement of formal proceedings, individuals may be classified as "persons of interest" or "pre-suspects" via bulk data processing, algorithmic risk assessments, and communications interception, usually without the safeguards attached to suspect status. The article begins with an overview of ECtHR case law regarding secret and bulk surveillance, as well as the interception of communications for security purposes. Next, the focus is put on the CJEU ruling in EncroChat and its implications for transnational electronic evidence, access to communications of non-suspects, and the defence's ability to challenge the lawfulness, authenticity, and integrity of data obtained from encrypted platforms.

The author draws attention to the fact that the analysis of bulk data, coupled with AI capacities, may weaken the requirement of prior suspicion and undermine adversarial guarantees when data gathered outside of criminal proceedings is later used as incriminating evidence. She concludes that European legal systems must rethink procedural safeguards for the digital age, strengthening controls over reasonable suspicion and regulating algorithmic suspicion and mass data analysis. They must also address the role of private technology companies in criminal investigations. This would best be achieved at the EU level, as the bloc continues to develop its Area of Freedom, Security and Justice, always seeking to strike the right balance between fighting crime efficiently and ensuring procedural safeguards.

AUTHOR

Lorena Bachmaier

Full Professor of Law
Universidad Complutense Madrid

CITATION SUGGESTION

L. Bachmaier, "Rethinking Procedural Safeguards in the Digital Age", 2026, Vol. 21(1), eucrim. DOI: https://doi.org/10.30709/eucrim-2026-008

Preprint eucrim 2026, Vol. 21(1)
ISSN: 1862-6947
https://eucrim.eu

CC BY ND

I. Introduction

The digitalisation of every aspect of our lives is a driving force for change in contemporary society, impacting all areas. This article examines the extent to which digitalisation is being properly "steered" by our legal systems. This is done from the perspective of procedural safeguards in criminal proceedings, which must revolve around human dignity and the protection of fundamental rights. The issue is becoming increasingly relevant – and urgent – in light of the populist and autocratic tendencies in many legal orders previously considered to be firmly committed to the principles of the rule of law.

The following sections will analyse some of the problems and tensions that contemporary criminal proceedings face in the digital era. This analysis will help us rethink the future of criminal procedure in a "digitalised" world and explore how we can continue to safeguard individuals against the State's increasingly all-embracing power. I will not address the – albeit highly relevant – topics of the use of technology in general and the rules on electronic evidence or videoconferencing. The aim of this article is rather to draw attention to the ways in which information and communication technologies – particularly the State's capacity for mass surveillance, which is set in motion long before criminal proceedings formally commence – are already transforming the structure and functions of criminal proceedings.[1]

Two factors require us to reconsider the safeguards of the criminal justice system. The first factor concerns "persons of interest" who are subject to certain surveillance measures that may affect their right to privacy and their right to data protection. As they are not suspects in a criminal investigation and no criminal proceedings have been formally initiated, however, the corresponding safeguards do not apply. Still, it is evident that their situation is not comparable to that of an ordinary citizen who is outside the attention of security systems. Finding the appropriate balance between protecting individuals from the State and allowing the identification of risks that may significantly impact their liberty and privacy is difficult.[2] In parallel, data acquired through surveillance measures may be used in the criminal proceedings to trigger suspicion and investigative measures or even as evidence.

The second factor is the enormous expansion of surveillance possibilities through digital technologies and sophisticated software using artificial intelligence and, in the near future, quantum computing. These developments are changing the scope of preventive and predictive surveillance, as the information gathering of the "pre-digital age" – through informants, police surveillance, or the interception of communications by intelligence services – becomes less relevant.[3]

In this context, the role of large tech companies cannot be overlooked — not only because of their capacity to interfere with our right to privacy, but also because, they are becoming necessary "partners" of law enforcement authorities in criminal investigations through their management of our data.[4]

Without aspiring to find answers to all emerging questions of this digital revolution, in the following sections, I will highlight the need to redefine procedural safeguards in a digitalised context, namely where the fields of prevention and prosecution have become increasingly blurred. As it stands, AI tools are enabling the processing of vast amounts of data, which could affect both the initiation and the outcome of a criminal proceeding. To set the scene, I will first outline the current approaches of the European Court of Human Rights (ECtHR) and the Court of Justice of the EU (CJEU) regarding mass surveillance and access to bulk data without prior suspicion of an individual (Section II). Second, I will identify the main challenges for the criminal proceedings in the digital environment(Section III). Finally, I will draw conclusions for the future of procedural safeguards in the European Union (Section IV).

II. Intelligence, Prevention, and the Bulk Interception of Communications — From *Big Brother Watch* to *EncroChat*

The scenario described in the introduction raises several questions concerning the definition of suspects' rights in national codes of criminal procedure, also considering that only a minimum level of harmonisation at the EU level has been achieved through the procedural rights directives. Should we consider defining and regulating rights of individuals who are classified as persons of interest or "pre-suspects"? Do the safeguards provided by the data protection and data retention rules adequately protect citizens' rights? Should a new level of safeguards be introduced for these individuals to ensure that data collected for security purposes is not used for criminal prosecution? Should additional safeguards beyond those foreseen in criminal proceedings be required for the processing of data obtained through bulk surveillance?

The case law of the ECtHR (1. below) provides some guidance to these questions, even though the ECtHR has generally left the neuralgic issue of the admissibility of evidence in cases of procedural rights violations up to the national laws. The CJEU has also established some building blocks (2. below) and, in contrast to the ECtHR, even introduced some relevant criteria on the admissibility of digital evidence.

1. The case law of the ECtHR

The ECtHR established in numerous judgments the minimum standards of rights that must be guaranteed to individuals in the context of the protection of national security. Since *Klass and Others v. Germany*,[5] the ECtHR's approach has focused on the safeguards that must accompany methods of secret surveillance (covert surveillance), as well as how each of those investigative activities is recorded. The requirements relating to the interception of communications involving mass surveillance were defined in *Szabó and Vissy v. Hungary*,[6] *Weber and Saravia v. Germany*,[7] and *Zakharov v. Russia*,[8] but the Court has rarely assessed whether a situation affects national security. It has, however, stated that the protection of national security must always be weighed against the seriousness of the intrusion into the individual right to respect for private life.

a) The *Big Brother Watch* case

The opportunity to analyse mass surveillance measures and the right to privacy was given in the *10 Human Rights Organizations v. United Kingdom* case,[9] better known as the *Big Brother Watch* case. The applicants specifically argued that Art. 8 of the UK Regulation of Investigatory Powers Act (RIPA) 2000, which allowed the surveillance of bulk interceptions (through programmes such as KARMA POLICE, Black Hole, TEMPORA, etc.), did not comply with the standards set out in the ECtHR's previous case law.[10]

In its analysis of the *Big Brother Watch* case, the Court reiterated: [11]

> (…) the lawfulness of the interference is closely related to the question whether the 'necessity' test has been complied with and it is therefore appropriate for the Court to address jointly the 'in accordance with the law' and 'necessity' requirements.

However, the Court did not merely invoke its earlier case law on bulk interceptions, but also assessed whether that case law from ten years earlier was still applicable to the present digital environment.[12] The Court concluded that a new approach was required, as not all the safeguards for interceptions directed against specific persons are applicable in the case of bulk interceptions, for example the requirement of probable cause.[13]

Before analysing the specific safeguards that must be adopted for the bulk interception of communications, the Court outlined the different stages of this measure: (1) the initial search for information, which takes place for the most part in an automated manner; (2) the application of selectors; (3) the analyst's initial examination of the material resulting from the search, following the application of the selectors; and (4) the use of the intercepted material. It then specified that control mechanisms and effective safeguards must be present at each stage.

According to the Court, "the process must be subject to 'end-to-end safeguards', meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken."[14] The Court paid particular attention to the aforementioned second stage, the "application of selectors," as this stage is especially sensitive, since the choice of selectors may trigger the interception against individual persons.[15] It confirmed that states can use measures for the bulk interception of communications and that each member state must delimit the scope of application, depending on their needs assessment in terms of national security.

In contrast to the Grand Chamber majority, not all of the judges were convinced by the argument that information obtained through bulk interception would have no evidential impact. As expressed in the joint, partly concurring opinion:[16]

> It appears that on the basis of the information thus obtained, law enforcement agencies could act, for example, by proceeding to conduct investigative measures or even arrests, this in turn producing evidence for the purpose of prosecution. It is likely that in a not so distant future, by exploring this particular ground, crime investigation might move from targeted surveillance to bulk interception of data.

This statement can only be endorsed, as evidenced by the rapid development of AI tools since this judgment was issued.

b) Subsequent case law

The ECtHR has subsequently ruled in several cases on the extent to which systems for the interception of communications, whether preventive in nature or operated by intelligence services, comply with the ECHR, specifically the right to respect for private life recognised in Art. 8 ECHR. In the judgment in *Ekimdzhiev and Others v. Bulgaria*,[17] the Court held that there had been a violation of Art. 8 ECHR due to the lack of adequate legal provisions ensuring that secret surveillance — and the subsequent system for the retention of and access to the intercepted communications — was limited to what was strictly necessary.

In *Haščák v. Slovakia*,[18] the Court found a violation of Art. 8 ECHR due to the lack of safeguards against arbitrary interferences, as required by the principles of the rule of law, and the fact that the retention of the intercepted communications had not been subject to external supervision.

Similarly, in *Pietrzak and Bychawska-Siniarska v. Poland,*[19] involving surveillance measures adopted preventively under Poland's anti-terrorism legislation, the ECtHR confirmed a violation of Art. 8 ECHR, due to the lack of adequate supervision of communications monitoring carried out under anti-terrorism legislation.

c) The *ByLock* case

Another important case is the *Yüksel Yalçinkaya v. Turkey* case,[20] also known as the *ByLock* case or the "Turkish *EncroChat*". The case concerned the use of evidence that was obtained from access to an encrypted communication system, questioning the admissibility of evidence and its conformity with Arts. 6 and 8 ECHR. The applicant alleged that the lack of judicial control over the obtaining and processing of data from

the *ByLock* platform made it impossible to verify the authenticity and integrity of those electronic communications. Despite this evidence having been decisive and incriminating, the defence was unable to challenge its reliability, authenticity, and lawfulness.

The ECtHR first reiterated its general doctrine on the admissibility of evidence, i.e., that the assessment of evidence is essentially a matter for the national courts and that the Court's role is limited to reviewing whether that assessment is unreasonable or arbitrary, since the ECtHR is not a fourth instance. The reasoning of the national judgment should shed light on these matters. Regarding the use of the encrypted communication system, in this case, the ECtHR stated that the mere downloading or using such a system, or even the use of any other method to safeguard the private nature of the messages exchanged, neither constitutes a criminal offence in itself (in this case membership of a terrorist organisation), nor can it be considered an evidential element capable of convincing an objective observer that unlawful activity or even a criminal offence is being committed.[21]

Having analysed the manner in which the evidence had been obtained, the safeguards adopted in respect of the integrity and authenticity of the evidence, and the response to the accused's appeals, the ECtHR concluded that Art. 6(1) ECHR had been violated. The Strasbourg Court did not call into question the legitimacy of access to the *ByLock* platform. On the contrary, it stated: [22]

> The use of electronic evidence showing that an individual is using an encrypted messaging system that has been specifically designed and used exclusively by a criminal organisation in the internal communications of a criminal organisation may be very important in the fight against organised crime.

The Court recognised that the use and assessment of electronic evidence in criminal proceedings may entail specific difficulties for judges, due to its complexity, which may affect the ability of national courts to decide on its authenticity, accuracy and integrity. It also stated that, in criminal proceedings, national courts may increasingly rely on electronic data or other data gathered by intelligence services, whose activities in this respect may or may not be subject to the rules governing the obtaining of evidence within criminal proceedings.[23]

The ECtHR also held, however, that the right of access to the sources of evidence — and therefore the right to comment effectively on them — is not an absolute right and may be subject to limitations.[24] Therefore, it took into consideration whether the applicant's lack of access to the sources of evidence had been counterbalanced by adequate procedural safeguards and whether he had been given a proper opportunity to prepare his defence.[25] It is important to emphasise that the ECtHR does not call into question the use of intelligence information as evidence, leaving this matter to national legislation.

2. The bulk interception of communications and the *EncroChat* case at the CJEU

In the field of transnational evidence gathering and the admissibility of evidence obtained through the bulk interception of communications in the European Union (EU), perhaps no case has had greater resonance as the *EncroChat* case, on which the CJEU ruled on 30 April 2024.[26]

To briefly recall the facts of the case:[27] In the context of an investigation conducted by French law enforcement authorities, it emerged that some individuals under criminal investigation were using encrypted mobile phones operating under a licence called "EncroChat". The Lille magistrate authorised the use of a "Trojan horse" to access the entire messaging platform Specifically, the initial partial decryption of 3477 text files created as "notes" revealed that almost all of them were related to communications connected with criminal

activities perpetrated by criminal organisations. The intercepted material was then distributed among the Member States for use in their own criminal investigations.

I will consider the case as establishing certain principles to be observed with regard to procedural safeguards in criminal proceedings having a transnational dimension and involving electronic data and access to encrypted communication platforms in the Union.[28]

It may be argued that, strictly speaking, the case did not involve bulk surveillance, since access to the encrypted data was not carried out under a national security or intelligence scheme. Accessing the communications of users of the platform against whom no prior suspicion had been established, however, allows us to draw analogies with surveillance measures for preventive purposes and to approach the *Encrochat* case as if it were another bulk interception of communications. In this context, the CJEU had to deal with an unprecedented issue as to the use of non-targeted accessed communications as evidence in criminal proceedings and the rights of defence in cross-border digital environments.

Here, the Court in Luxembourg followed the criterion already adopted in the Strasbourg Court's case law[29] as well as in its own case law on data retention,[30] holding as follows:[31]

> As regards specifically the right to a fair trial, it must be noted in particular that if a court takes the view that a party is not in a position to comment effectively on a piece of evidence that is likely to have a preponderant influence on the findings of fact, that court must find an infringement of the right to a fair trial and exclude that evidence in order to avoid such an Infringement.

Interestingly, while the CJEU mentioned the lack of specific knowledge in digital matters on the part of the trial court as a factor to be taken into account when assessing defence rights in data retention case law, this was omitted in the ruling in the *EncroChat* judgment. Nevertheless, in defining the defence rights, the CJEU goes beyond the standards set out by the ECtHR in the *ByLock* case, in which the latter held that the right to comment effectively on digital evidence is not absolute. Furthermore, the CJEU ruled on the admissibility of evidence, by contrast to the ECtHR, which does not enter into establishing exclusionary rules of evidence, but analyses the case mainly from the fair trial rights' perspective (see also above 1.).

It remains to be seen how national courts interpret this rationale for inadmissibility of evidence, as defined by the CJEU. In the context of electronic evidence, the rights of the defence revolve around the ability to verify the lawfulness, authenticity, integrity, and proportionality of the evidence.

It follows that several questions arise: How can the integrity of the data be verified if access to the data in its entirety is not possible? Would the right to comment effectively imply a right of access to the raw data? How can the defence comment on bulk electronic data if sophisticated software is required to do so? Should data sifting always be done in the presence of the defence, as it is required for the cross-examination of witnesses? Does the state have to inform the defence about which AI tool was used to collect, process, and filter data?[32] Is there a need in the areas of freedom, security and justice for the EU Member States to always use a certified AI system? Should this be the same in all Member States?

3. Interim conclusion

As can be seen, both the ECtHR's case law and the CJEU's decision in *Encrochat* have already established a number of standards regarding bulk surveillance and bulk access to data. However, neither has defined which information gathered in this way can be used in criminal proceedings. While ECtHR and CJEU case law provide some guidance on the use of bulk surveillance and emphasise the need to ensure fair trial rights when encrypted messaging platforms are accessed, they do not prevent bulk data intercepted without prior identification of a suspect from flowing into criminal proceedings. On the one hand, the ECtHR expressly

refrains from setting any standards on the admissibility of evidence in this context; on the other hand, the CJEU only establishes the need to ensure the possibility of "effective comment" on evidence obtained from a "suspected" platform. The question is whether these general standards are sufficient to ensure, in a digital context, not only the protection of privacy rights, but also that information gathered for preventive purposes and/or without suspicion does not become incriminating evidence. Should procedural safeguards be activated earlier, given that the rules on evidence seem to offer only limited protection against state interference in individuals' privacy rights via bulk surveillance?

III. Prevention, Mass Surveillance, and Open Data Analysis: The Challenges for Criminal Proceedings

The gathering and processing of information for security purposes (what is usually understood as intelligence) is not only a necessary and useful task but also indispensable if action is to be taken effectively against criminal phenomena in general, and organised crime, terrorism, money laundering, and environmental crime in particular.[33] However, given the scale of information gathering and the technological possibilities of mass surveillance, we should question whether an alternative or additional system for the prevention and/or prosecution of crime is being introduced surreptitiously, permeating procedural structures without an adequate and transparent legal framework and effective procedural safeguards.1. "Persons of interest" and the changing rules of the game to open criminal proceedings

As has been widely pointed out, the boundaries between prevention and repression have become increasingly blurred in many areas, especially, but not only, in the fields of terrorism and organised crime. The reason for this is because criminal law has increasingly moved from repression to prevention[34] on the one hand and, on the other, measures of administrative law tend to acquire a punitive character.[35] This impacts not only fundamental rights, but also the very conception of criminal proceedings. The use of extensive preventive measures[36] has also led to the emergence of a new category of individuals who are not classified as suspects for the purposes of criminal proceedings, but who are identified as "persons of interest" or "pre-suspects" by algorithm-based mass surveillance systems.[37]

Classifying individuals as "persons of interest" based on their potential risk of committing criminal offences and subjecting them to continuous surveillance not only turns them into sources of information but also into objects of evidence, insofar as the data obtained from surveillance could acquire evidential value. Bulk data analysis can be initiated without the need to establish specific suspicions against particular individuals before a judge.[38] In many cases, a mere risk assessment is sufficient, and this assessment is regularly carried out by means of an algorithm.[39] In short, law enforcement authorities can access or purchase data analyses from companies that have the appropriate software to draw up not only profiles of potential risks, but, in particular, also profiles of those persons who represent a risk or who may directly be classified as criminal suspects. Thus, automated suspicion algorithms (ASAs) have come to increasingly replace informants and traditional police surveillance, while multiplying their reach exponentially. However, judges who must assess suspicions based on those ASAs within the criminal proceedings do not have clear criteria for determining their reliability.[40]

The consequence of all this is that the prerequisites for opening a criminal investigation may be completely altered by the new "rules of the game", because a thorough risk assessment can be carried out through the bulk analysis of data. This would then underpin the standard of probable cause required to open criminal proceedings. In short, it is worrying that an intrusive investigation can be initiated on the basis of the bulk processing of data for security purposes, without prior suspicion, since these surveillance measures only

concern "persons of interest."[41] The joint, concurring opinion on the ECtHR *Big Brother Watch* judgment (II.1.a above) indirectly pointed out this risk, which is dramatically increased by the development of AI tools.

I neither contend that this is generally the case, nor that law enforcement or intelligence services are acting outside the law. However, even if we accept this premise and that these activities are carried out within legal limits — and I am not aware of any data contradicting this —, the truth is that any surveillance system lacking transparency and not being public must be subject to a rigorous oversight. It must be borne in mind that the bulk interception of communications and the retention of the data thus obtained constitute a significant interference with the right to privacy, even when the data are in fact not analysed.[42] Naturally, the risks are even greater when certain persons become surveillance targets owing to the selectors applied and the content of their communications is monitored and analysed. In *Big Brother Watch,* the ECtHR underlined the importance of oversight at all stages of the "surveillance procedure" (end-to-end safeguards), specifically highlighting oversight in the application of selectors (see II.1.a above).

The usefulness of bulk interception for security operations is scarcely disputed, and a proactive approach towards identifying threats to national security is regarded as a legitimate and reasonable aim. There are, however, two basic elements that clearly differentiate the levels of safeguards in criminal proceedings and in the preventive system aimed at security: In the field of criminal proceedings, there exists the requirement of prior suspicion and, usually, of a judicial warrant before investigative measures entailing an intrusion into fundamental rights can be taken; this warrant includes prior checking of the necessity and proportionality of the interference. In the case of non-targeted surveillance, the approach differs from the aforementioned criminal procedure scheme, since there is no initial judicial decision based on prior suspicions against specific individuals, simply because there is no specific target or suspect.[43] The risk of circumventing the safeguards of criminal proceedings seems to be clear.

While the case law of the ECtHR stresses the importance of oversight at all stages, it does not prevent the information gathered for security purposes to flow into criminal proceedings. Yet, the CJEU does not ban access to large amounts of data without prior suspicion against an identified suspect, as seen in the *Encrochat* case. This shows that, even if we can already count on a number of standards from the ECtHR and CJEU, the issue of implementing procedural safeguards in a digitalised surveillance environment has not yet been addressed.

2. Mass surveillance and criminal evidence standard

It could be argued that mass surveillance is not intended to gather evidence for criminal investigation purposes, since its focus is on prevention. But does this mean that the principle of respect for privacy does not apply? If these data are the basis for obtaining evidence (having established a "reasonable suspicion" for a judicial warrant in order to initiate investigative measures), as outlined under 1. above, are we not caught in a vicious circle?

The fact that certain countries already use ASAs underpins these risks. As a result, criminal proceedings are no longer the place where facts and criminal liability are established, because, according to the algorithm used, data have already been collected against a "person of interest" and the next step is merely to present this data set as evidence. The evidence then secures the criminal conviction of an individual or, as a simpler solution, a plea agreement.[44] This phenomenon can be observed in criminal justice systems in which trials are slowly losing their previous importance and becoming the exception rather than the rule.[45]

This handling of evidence necessitates reconsideration of the system of procedural safeguards centered on the liberal model and, specifically, on the principle of a public and oral trial hearings, i.e., the moment at which adversarial proceedings reach their fullest expression in the taking of evidence. In order to solve the

problem of using data from bulk interceptions as criminal evidence, the correct approach should be to reinforce the safeguarding prerequisites that may give rise to the opening of a criminal investigation against a specific person in the first place. We should rethink the role of "rational indications," "well-grounded suspicions," or "probable cause" (the term used in the Fourth Amendment of the United States Constitution).[46] Indeed, the term "probable cause" is ambiguous and as yet undefined, referring to a calculation of probabilities/to a non-quantitative or statistical probability that moves within a variable range.

The requirement of probable cause should become the decisive criterion when authorising access to and seizure of electronic data. In this context, it should not be overlooked, however, that the activation of an algorithm to identify or compile data by means of bulk processing could generate indications or suspicion criteria in respect of practically any individual. This could mitigate the normative and conceptual uncertainty of the probable cause standard and serve as the basis for initiating criminal proceedings, as well as for adopting criminal investigative measures that restrict fundamental rights (though they must still be subject to the additional criteria of necessity, suitability and proportionality).

In other words, if we wish to continue maintaining the traditional safeguards of criminal proceedings, the standard for activating investigative measures based on the processing of big data or for indiscriminately accessing retained user data, must be strengthened. It is worth noting here that the standard of probable cause "may not ultimately address any one right specifically, but instead protect all of liberty generally,"[47] thus safeguarding the rule of law principle.

We could still hope that the exclusionary rule of evidence would apply to data obtained prior to criminal proceedings or that evidence obtained solely on the basis of "reasonable suspicion" arising from mass surveillance would be declared invalid. This would be the procedural safeguard that governs the use of bulk data as evidence in criminal proceedings. However, this approach cannot be taken for granted, because the risk entailed is that it would suffice to confront the accused with all the data available to the prosecution to persuade the defendant to accept the conviction upon a plea agreement, without validity of the evidence never being assessed at trial.

IV. Concluding Remarks

A number of conclusions can be drawn from the discussion of the above-mentioned challenges:

Firstly, and perhaps most importantly, there is a need to continue the struggle for procedural safeguards in a digitalised world. Secondly, the prerequisites that allow the state to access and process citizens' data for preventive purposes need to be redefined. Thirdly, stricter control is also required over the application of the probable cause or "reasonable suspicion" requirement, as it could become the only way to prevent a criminal investigation from being opened and, subsequently, from turning any data already obtained into incriminating evidence. In a system that is primarily focused on prevention and technology, the defence can only assert its right to "comment effectively" on the evidence thus obtained.[48]

As the ECtHR held in *ByLock,* the right to effectively respond to the evidence obtained does not, however, necessarily include the right to review the integrity of the intercepted data or to have knowledge of the software used to access the communications. Any effort to strengthen the rights of the defence must include effective access to digital tools (knowledge of how the data was processed) and appropriate software (ability to analyse the raw data) in order to ensure the equality of arms. Otherwise, it will be impossible to comply with the adversarial principle as means of establishing facts in criminal proceedings.[49]

In any event, requiring prior suspicion as a prerequisite for taking notably intrusive measures into the citizens' sphere of privacy does not appear to protect us against mass surveillance. This became readily

apparent in the *EncroChat* case, when national courts accepted the intercepted communications as evidence against individuals despite there being no prior grounds for suspicion. It might be considered to revisit the standard of probable cause against the new digital reality and the resorting to data brokers for establishing ASAs.

In the EU, some progress has been made in protecting the rights of individuals facing criminal proceedings. The procedural rights directives adopted so far indicate that the European legislature has taken an increasingly progressive interest in establishing a framework of procedural safeguards. Yet, we must press on, as artificial intelligence and, in the near future, quantum computing usher in a new digital reality, bringing with it new challenges for criminal procedure. The time is ripe to articulate a new framework of procedural safeguards at the European level to cope with the increasing digitalisation of law enforcement.

---

1. See Bachmaier, "La lucha por las garantías procesales y el cambio de paradigma en materia de prueba: del proceso penal liberal a la mass surveillance", in L. Bachmaier Winter (ed.), *Prueba penal y derecho de defensa en la era digital. Nuevos paradigmas y nuevos retos,* Aranzadi, Cizur Menor, 2024, pp. 21-64.↩
2. See P. Galison & M. Minow, "Our Privacy, Ourselves in the Age of Technological Intrusions", in R. Ashby Wilson (ed.), *Human Rights in the «War on Terror»,* 2005, p. 260. More recently, on the use of AI in this field, see A. Sachoulidou, "Going beyond the "common suspects": to be presumed innocent in the era of algorithms, big data and artificial intelligence", (2023) *Artificial Intelligence and Law*, <https://doi.org/10.1007/s10506-023-09347-w>. All hyperlinks in this article were last accessed on 17 August 2026.↩
3. S. Brayne, *Predict and Surveil. Data Discretion and the Future of Policing*, 2020, pp. 122 ff. And, as R. Poscher, Guest editorial, *eucrim* 4/2025, 249 points out, this also requires a "re-calibration of traditional proportionality models" in digital-based surveillance.↩
4. The role of big tech corporations as necessary partners in the criminal investigation will not be further addressed here. See, in this regard, D. Bilchitz, "The Right to Privacy, Surveillance and the Global Obligations of Corporations", in D. Cole, F. Fabbrini and S. Schulhofer (eds.), *Surveillance, Privacy and Trans-Atlantic Relations*, 2017, pp. 113-136.↩
5. ECtHR, 6 September 1978, *Klass and Others v. Germany,* Appl. no. 5029/71.↩
6. ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary,* Appl. no. 37138/14.↩
7. ECtHR, 29 June 2006, *Weber and Saravia v. Germany*, inadmissibility decision, Appl. no. 54934/00.↩
8. ECtHR, 5 October 2006, *Zakharov v. Russia,* Appl. no. 14881/03.↩
9. ECtHR, 13 September 2018, *Big Brother Watch and others v. United Kingdom*, Appl. nos. 58170/13, 62322/14 y 24960/15; and later the *Grand Chamber* judgment of 25 May 2021. On this case, see L. Bachmaier Winter, "Proportionality, surveillance and criminal investigation: Strasbourg Court facing *Big Brother*", in E. Billis, N. Knust and J. P. Rui (eds.), *The Principle of Proportionality in Crime Control and Criminal Justice*, 2021, pp. 317-335.↩
10. There is a pending case seeking, once again, compliance with the Convention of the UK Investigatory Powers Act and addressing complaints about bulk interception warrants: ECtHR, *The National Council for Civil Liberties v. the United Kingdom*, Appl. no. 15250/24, lodged on 28 May 2024, published on 30 March 2026.↩
11. ECtHR (GC), 25 May 2021, *Big Brother Watch and others v. United Kingdom*, *op. cit.* (n. 9), para. 334.↩
12. Ibid., paras. 341-342.↩
13. Ibid., para. 348.↩
14. Ibid., para. 350.↩
15. Ibid., para. 354.↩
16. See the joint, partly concurring opinion of judges Lemmens, Vehabović and Bošnjak, para. 29.↩
17. ECtHR, 11 January 2022, *Ekimdzhiev and Others v. Bulgaria*, Appl. no. 70078/12.↩
18. ECtHR, 23 June 2022, *Haščák v. Slovakia*, Appl. no. 58359/12 *et al.;* See also ECtHR, 20 July 2021, *Zoltán Varga v. Slovakia,* Appl. no. 58361/12.↩
19. ECtHR, 28 May 2024, *Pietrzak and Bychawska-Siniarska and Others v. Poland*, Appl. nos. 72038/17 and 25237/18.↩
20. ECtHR, 26 September 2023, *Yüksel Yalçinkaya v. Turkiye,* Appl. no. 15669/20.↩
21. Ibid., paras. 262-266, in which the ECtHR determines that the use of the encrypted platform is not sufficient evidence for the crime of membership of a terrorist organisation, as such an interpretation would run counter to Art. 7 ECHR.↩
22. Ibid. para. 312; see also 344.↩
23. Ibid., para. 312.↩
24. Ibid., para. 329.↩
25. Ibid., para. 330.↩
26. CJEU, 30 April 2024, Case C-670/22, *Criminal proceedings against M.N.* (*EncroChat*), ECLI:EU:C:2024:372.↩
27. The concrete events have still not been fully clarified. I refer here to the CJEU's judgment (*op. cit.* n. (26)), para. 19.↩
28. I will neither examine all aspects and implications of the communications data obtained through access to an encrypted system used primarily for exchanging messages, nor all the questions revolving around the interpretation of the EIO Directive. I refer here to the vast literature on this case. See, e.g., T. Wahl, "Verwertung von im Ausland überwachter Chatnachrichten im Strafverfahren", (2021) 7-8 *Zeitschrift für Internationale Strafrechtsdogmatik (ZIS)*, 453; J.J. Oerlemann and D. A. G. Van Toor, "Legal Aspects of the EncroChat Operation: A Human Rights Perspective", *European Journal of Crime, Criminal Law and Criminal Justice, (*2022) 30(3-4), 309-328; L. Bachmaier, *op. cit.* (n. 1), 41. More recently, M. Lassalle and S. Lannier, "EncroChat – A Judicial Chronology. Interpretations from Paris, Strasbourg and Luxembourg Courts", (2025) 20 *eucrim*, 292-302.↩

29. ECtHR, 10 March 2009, *Bykov v. Russia*, Appl. no. 4378/02, paras. 88-90; ECtHR, 26 July 2011, *Huseyn and Others v. Azerbaijan*, Appl. nos. 35485/05, 45553/05, 35680/05, and 36085/05, paras. 199, 200, and 211; ECtHR [GC], 18 December 2018, *Murtazaliyeva v. Russia,* Appl. no. 36658/05; ECtHR, 14 February 2019, *SA-Capital Oy v. Finlandia*, Appl. no. 5556/10, para. 78; ECtHR, 14 March 2019, *Kobiashvili v. Georgia*, Appl. no. 36416/06, para. 56.↩
30. See, *inter alia*: CJEU, 17 December 2015, Case C-419/14, *WebMindLicenses*, ECLI:EU:C:2015:832; CJEU, 2 March 2021, Case C-746/18, *Criminal proceedings against H.K (Prokuratuur),* ECLI:EU:C:2021:152; CJEU, 30 April 2024, Case C-470/21, *La Quadrature du Net and Others v. Premier Ministre and Ministre de la Culture ('La Quadrature du Net 'II"),* ECLI:EU:C:2024:370.↩
31. CJEU, *EncroChat*, *op. cit.* (n. 26), para. 105.↩
32. On the problematics of AI evidence, see P.W. Grimm, M.R. Grossman and G.V. Cormack, "Artificial Intelligence as Evidence", 19 (2021) *Northwestern Journal of Technology and Intellectual Property*, 9. See also, in the EU context, the comparative study by K. Ligeti (ed.) *Artificial Intelligence as Evidence in Criminal Proceedings*, 2025.↩
33. See ECtHR [GC], 25 May 2021, *Big Brother Watch, op. cit.* (n. 9), para. 421; L. Bachmaier Winter, "Información de inteligencia y proceso penal", in L. Bachmaier (ed.), *Terrorismo, proceso penal y derechos,* Marcial Pons, Madrid, 2012, pp. 45-101, 49.↩
34. E.g., U. Sieber, "Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld terroristischer Gewalt – Eine Analyse der Vorfeldtatbestände im Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten", (2009) *Neue Zeitschrift für Strafrecht (NStZ)*, 353-364; U. Sieber, "Risk prevention by means of criminal law – On the legitimacy of anticipatory offenses in Germany's recently enacted counter-terrorism law", in F. Galli and A. Weyembergh (eds.), *EU counter-terrorism offences: What impact on national legislation and case-law?*, 2012, pp. 251-279; M.F.H. Hirsch, *Anticipative Criminal Investigation. Theory and Counter-terrorism Practice in The Netherlands and in the United States,* 2012.↩
35. L. Bachmaier, "The shift from criminal to administrative sanctions: the quest for fair trial rights in new crime control scenarios in the ECtHR case law", in M. Donini and L. Foffani (eds.), *La "materia penale" tra diritto naeionale ed europeo*, 2018, pp. 37- 62; F. Galli, "The freezing of terrorists' assets: preventive purposes with a punitive effect", in F. Galli and A. Weyembergh (eds.), *Do labels still matter?,* 2014, pp. 43-68.↩
36. See A. Ashworth and L. Zedner, *Preventive Justice*, 2014, pp. 181-190.↩
37. I already analysed the situation of the pre-suspects or persons of interest in L. Bachmaier Winter, "Countering Terrorism: Suspects without Suspicion and (Pre-)Suspects under Surveillance", in: U. Sieber, V. Mitsilegas, C. C. Mylōnopulos, E. Billis, & N. Knust (eds.), *Alternative systems of crime control: national, transnational, and international dimensions*, 2018, pp. 171-191. I refer to the literature cited there.↩
38. M. Rich, "Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment", (2016) 164 *Univ. Pennsylvania Law Rev.*, 870-929.↩
39. See Brayne, *op. cit.* (n. 3), pp. 118 ff.↩
40. L. Bachmaier (2024), *op. cit.* (n. 1), p. 42.↩
41. Ibid., 55.↩
42. As stated by the CJEU [GC], 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland et al*. para. 34. See also, on the chilling effect upon the rights of citizens and the impact upon the rule of law, D. Murray and P. Fussey, "Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data", (2019) 52 *Israel Law Review,* 31-60, at 43-47.↩
43. ECtHR [GC], 25 May 2021, *Big Brother Watch, op. cit.* (n. 9), para. 317. Nevertheless, in ECtHR, 28 April 2026, *Kanev and Bulgarian Helsinki Committee v. Bulgaria*, Appl. no. 45864/22, a case that concerned mass interception of communications by the intelligence services targeting numerous individuals in Bulgaria, the Court referred to the safeguards set out in *Big Brother Watch* (paras. 240-243). However, this case dealt with the agency's denial of information on the surveillance carried out.↩
44. See R. Lippke, "Plea Bargaining, Principled Sentencing, and Artificial Intelligence", in J. Ryberg and J. V. Roberts (eds.), *Sentencing and Artificial Intelligence*, 2022, 184-204.↩
45. See, e.g., Fair Trials, *The Disappearing Trial - What does justice mean in a world with more guilty pleas and fewer trials?*, 2017, <https://www.fairtrials.org/app/uploads/2022/01/The-Disappearing-Trial-Summary-Document-SF.pdf>.↩
46. See L. Bachmaier "Probable cause y la Cuarta Enmienda de la Constitución estadounidense: una garantía tan imprecisa como necesaria", *Quaestio Facti*, vol. 4, 1/2023, 191-220, <https://revistes.udg.edu/quaestio-facti/article/view/22858/26542>.↩
47. B.A. Antkowiak, "Saving Probable Cause*", (*2007) 40(3) *Suffolk University Law Review*, 578.↩
48. As held in the CJEU *Encrochat* judgment (*op. cit.* (n. 26)), para. 105 and the ECtHR *ByLock* case (*op. cit.* (n. 20)), para.312.↩
49. As we proposed in Art. 7(5), of the ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings, <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf>. This is also implicitly suggested in the judgement of the ECtHR, 4 June 2019, *Sigurđur Einarsson and Others v. Iceland*, Appl.no. ; see also the dissenting opinion of judge *Pavli* there.↩

* Author statement

The present article was written within the framework of the research project NEO-TRANSCRIM: Criminal Evidence and New Challenges in Transnational Criminal Proceedings (PID2023-148413NB-I00), Spanish Ministry of Science, Innovation and Universities.

COPYRIGHT/DISCLAIMER
© 2026 The Author(s). Published by the Max Planck Institute for the Study of Crime, Security and Law. This is an open access article published under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND

4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. If users remix, transform, or build upon the material, they may not distribute the modified material. For details, see https://creativecommons.org/licenses/by-nd/4.0/.
Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union