

Pietrzak v. Poland, App. No. 72038/17

Bychawska-Siniarska and Others v. Poland, App. No. 25237/18

(First Section)

Written comments of Fair Trials

BACKGROUND

1. These written comments are submitted by Fair Trials, in accordance with the permission to intervene granted by the President of the First Section by letter of 30 June 2020 in accordance with Article 44§3(a) of the Rules of the Court and with the extension of submission deadline granted by letter of 23 July 2020.
2. Fair Trials focuses on the right to a fair trial protected by Article 6 of the Convention. We intervene in this case because it demonstrates how respect for the right to privacy is interlinked with the right to a fair trial. Specifically, strong and effective safeguards in respect of the right to privacy, as protected by Article 8 of the Convention, help drive good practice by criminal justice institutions and support the fairness of criminal proceedings (as protected by Article 6 of the Convention). The Court's approach to Article 8 in this context should, therefore, take into account the significant implications the decision in this case will have on criminal justice and the rule of law.

INTRODUCTION

3. The Polish measures at issue in these proceedings create broad, far-reaching powers for surveillance and law enforcement authorities to obtain information in complete secrecy. These cases raise issues of growing importance where information obtained through surveillance is increasingly being used in criminal investigations, including in the context of terrorism-related offences as well as Covid-19 related offences. More recently, states across Europe have rapidly introduced new legislation criminalising non-compliance with pandemic-related measures and broadening the powers of different authorities to collect private information, including individual's movements and contacts from mobile phones. The Court's ruling in these cases will set novel and significant standards in a context where law enforcement authorities are increasingly seeking (and obtaining) access to private electronic information held on mobile phones, computers and other electronic devices; and where information gathered through surveillance powers are increasingly used in criminal proceedings.
4. In these submissions, Fair Trials will assist the Court's assessment of the provisions in the Act of 15 January 2016 amending the Police Act of 6 April 1990 and Certain Other Acts (the "Police Act") and the Act on Counter-terrorism Activities of 10 June 2016 (the "Anti-Terrorism Act") by highlighting the inter-connectedness of the Convention system of rights and how safeguards for Article 8 are essential for the protection of the right to a fair trial (Article 6).
5. The aim of these surveillance instruments is to collect information that may lead to initiating criminal proceedings against certain persons and being used as evidence to make a finding of guilt. As such, the collection of information raises issues relating to Article 8 of the Convention but also has potential implications on Article 6 of the Convention. Secret surveillance measures must,

therefore, be subject to effective review and supervision when the surveillance is first ordered (*ex-ante*) and after it has been terminated (*ex-post*).ⁱ

6. In our submission, we will focus on six points. Article 6 does not provide sufficient protections against violations of Article 8 in the context of criminal proceedings. In particular, there are insufficient *ex-post* remedies where evidence obtained in violation of Article 8 is used against the accused (**Part A**). As such, effective *ex-ante* reviews are crucial given that surveillance often takes place without the knowledge of the individual and because digital surveillance can be very intrusive (**Part B**). *Ex-post* reviews of surveillance powers should also be especially robust to make up for the inadequacies of *ex-post* remedies under Article 6, and remedies pursuant to Article 13 of the Convention should be available even where there are no criminal proceedings (**Part C**). In this context, Article 8 should require Contracting States to adopt a robust legal framework for overseeing the use of surveillance powers that includes effective *ex-ante* and *ex-post* supervision (**Part D**). Such legal framework must include specific safeguards in relation to access by law enforcement authorities to the communications of lawyers (**Part E**). Finally, to prevent potential abuses of power, drive good practice and thereby protect the rule of law, judicial oversight must be complemented by systemic oversight with respect to interferences with privacy rights by law enforcement authorities (**Part F**).

Part A: The implications of the use of information gathered through the use of surveillance measures for fair trial rights in the event of criminal proceedings

7. As indicated in the Statement of Facts, the responses received by the Applicants from the relevant Polish authorities imply that an effective *ex-post* remedy in relation to the use of surveillance measures can only be sought in the context of subsequent criminal proceedings. This approach highlights the need for the Court to recognise the importance of proper safeguards for Article 8 rights in relation to Article 6. As noted in the partly dissenting opinion in *Bykov v. Russia*, evidence obtained in breach of Article 8 cannot be used without undermining the protection of that article and more generally respect for the rule of law.ⁱⁱ
8. In our view, limiting the availability of remedies to subsequent criminal proceedings falls short of the standard set by Article 13. It cannot be assumed that an effective *ex-post* remedy can be obtained in this context.
 - a. First, there is no guarantee that the information gathered through surveillance measures and needed to successfully challenge the legality of these measures will be disclosed in the criminal file regardless of the obligation to disclose material evidence in possession of competent authorities under both the Conventionⁱⁱⁱ and EU law.^{iv} As the Venice Commission noted, materials of operational control are usually treated as secret, meaning that they will most likely be kept from the defence even in criminal proceedings on merits.^v In other words, the person subject to the criminal investigation may never know that the investigation relied upon information obtained through secret surveillance measures.
 - b. Second, even where the data obtained through surveillance (and information about how the data was obtained) is disclosed in the context of criminal proceedings, the accused person may not be in a position to challenge the legality of the measure or the use of the data. To be able to challenge the decision forming the basis for the interception of

communications, the applicant must be provided with information about the decision, such as the date of the decision, the authority that issued it and the justification for the necessity and proportionality of such measure.^{vi} In the absence of such information, the person will not be able to challenge the measure during subsequent criminal proceedings.

9. Where an accused person obtains access to information about the use of surveillance measures and is able to establish an illegality, their main recourse at that stage is to rely upon evidentiary rules in criminal trials and seek the exclusion of the information obtained illegally from the evidence that the court may rely upon to assess their guilt. In other words, domestic criminal courts may be able to rule that the information is inadmissible because it was obtained illegally, e.g. through a violation of Article 8. However, even where such evidence is excluded, it will only prevent the authorities from benefiting from the violation of Article 8 of the Convention in the context of criminal proceedings, but will not offer a remedy for the unlawful intrusion into the person's private life in substance.
10. However, pursuant to Article 168(a) of the Polish Criminal Procedure Law,^{vii} evidence may not be excluded solely on the basis that it was gathered in violation of procedural law, that is, the proper procedure designed to protect the fundamental right to privacy. In addition, it is not clear whether the Polish criminal procedure, provides for a process to exclude evidence which results from "the fruit of the poisonous tree". This means that, both illegally obtained evidence and evidence derived from it can be admissible and used in a criminal trial to the detriment of defence.
11. Moreover under the Court's current case-law, information gathered by authorities under surveillance powers in violation of Article 8 may nevertheless be used as evidence in subsequent criminal proceedings against the very person whose rights under Article 8 has been violated. At present, the violation of Article 8 does not automatically lead to the exclusion of the information from criminal proceedings. Instead, the Court requires that the overall fairness test be applied, such that the proceedings as a whole could be considered to be fair, despite the evidence being obtained unlawfully.
12. For example, in *Bykov*, the applicant complained about the unlawful intrusion in his home and interception of his conversations without judicial authorisation. The Court found a violation of Article 8 in stating that "*the legal discretion of the authorities to order interception was not subject to any conditions, and the scope and the manner of its exercise were not defined; no other specific remedies were provided for.*"^{viii} However, even though the evidence was later admitted and used in the criminal trial, the Court found no violation of Article 6 of the Convention.^{ix} In *Dragoş Ioan Rusu v. Romania*, the applicant's correspondence was intercepted based on an authorisation procedure that revealed major shortcomings. Nevertheless, no violation of Article 6 was found even though the intercepted letters were decisive for the conviction.^x The above line of case-law clearly shows that criminal proceedings offer little avenue for an individual to assert their rights under Article 8 of the Convention, and remedy any violations that may have occurred during the investigation. In most cases, manifest shortcomings in evidence gathering by authorities will not result in the exclusion of such evidence from the trial.^{xi}
13. This position should be revisited. The question of admissibility in criminal proceedings of evidence obtained in breach of Article 8 is a question of principle, and the Court should be consistent in its findings in relation to the two rights protected by the Convention: what is prohibited under Article

8 cannot be permitted under Article 6. The Court must read the Convention as a whole, and what is considered unlawful in relation to one right must also be considered unlawful in relation to another. Otherwise, protections under Article 8, at least with regards to information gathered by secret surveillance used in criminal proceedings, will be rendered ineffective in practice. As stated by Judge Loucaides in the partly dissenting opinion in *Khan v. the United Kingdom*: “I cannot accept that a trial can be “fair”, as required by Article 6, if a person’s guilt for any offence is established through evidence obtained in breach of the human rights guaranteed by the Convention. (...) I do not think one can speak of a ‘fair’ trial if it is conducted in breach of the law”.^{xii}

14. In the absence of a clear remedy under Article 6 of the Convention where unlawfully obtained information is used in criminal proceedings, it is all the more incumbent on the Court to ensure that Contracting States have an effective oversight framework to scrutinise the use of surveillance powers, and to provide effective remedies where there are violations of Article 8. This framework has to include *ex ante* judicial checks on the necessity and proportionality of the use of surveillance powers (see further Part B), as well as *ex post* judicial review that provides effective remedies for Article 8 violations (see further Part C).

Part B: The importance of robust *ex-ante* safeguards for surveillance measures

15. The possibility of using evidence obtained through unlawful surveillance in criminal proceedings heightens the need for effective safeguards to prevent unlawful practices in the first place. There must be robust *ex ante* case-specific reviews of the proportionality and necessity of surveillance measures.
16. States do not enjoy an unlimited discretion to subject persons to secret surveillance measures.^{xiii} Secret surveillance is an interference with the right to privacy, and such measures may only be used if they are deemed to be necessary and proportionate.^{xiv} In view of their impact on Article 8 of the Convention, the use of such measures must be subject to a strict *ex-ante* necessity and proportionality control by requiring an adequate and effective prior judicial authorisation to prevent unlawful information gathering.
17. The very nature of secret surveillance entails that not only the surveillance measure itself but also the accompanying *ex-ante* necessity and proportionality control must be carried out without the individual’s knowledge. Consequently, given that the person concerned will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings at an *ex-ante* stage, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the person’s rights. The Court has consistently held that in the context of secret surveillance, a judge should be entrusted with the effective control, review and supervision of any interference by an authority with an individual’s rights, as judicial control offers the best guarantees of independence, impartiality and a proper procedure.^{xv}
18. Further, it is important for the Court to recognise that evidence-gathering measures such as communication surveillance and metadata collection can allow law enforcement authorities to obtain vast quantities of data through digital searches – often more than they can through most forms of physical searches. This is so even with individually targeted collection of “content-related” metadata such as the websites a person has visited or the headings of email messages.^{xvi} In this context, the control of the proportionality of the measure is also fundamental to ensure

that digital searches are not overly broad. The facts at issue in *M.N. and Others v. San Marino*^{xvii} reveal the potential reach of digital searches. A request from Italian law enforcement authorities for bank data affected over a thousand persons, none of whom were suspects in the investigation.

19. The level of interference with the right to a private life through surveillance measures such as the collection of metadata must be treated as at least equivalent to measures such as house searches, if not more so. In relation to investigative measures such as house searches, the Court requires that there is effective judicial scrutiny of lawfulness and necessity, which also includes the proportionality of the measure.^{xviii} A house search ordered without scrutiny by a judicial authority would be in breach of Article 8.^{xix} Where an investigative search is carried out at an early stage of a criminal investigation, the lack of prior judicial scrutiny, and the lack of immediate retrospective judicial review suggest that a search was disproportionate.^{xx}

Part C: *Ex-post* review and effective remedy in accordance with Article 13 of the Convention

20. Given the inadequacy of remedies for unlawful surveillance under Article 6, and recognising the fact that not all unlawful surveillance results in criminal proceedings, Articles 8 and 13 of the Convention should require Contracting States to have a particularly robust mechanism for the *ex-post* review of the use of surveillance measures. In this section, we highlight three key factors that the Court should consider as necessary for determining whether or not an *ex-post* review mechanism can be viewed as ‘effective’.
21. First, in our view, an effective *ex-post* remedy in cases of covert surveillance must be judicial. While a judicial remedy is not in principle required pursuant to Article 13 of the Convention, the Court recognises that a higher institutional standard should be required to review covert surveillance measures because “*abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole*”.^{xxi} In other words, a judicial mechanism should be available to the person concerned to protect the rule of law. This requires that an interference by the executive authorities with an individual’s rights be subject to an effective control which should normally be assured by the judiciary, as it offers the best guarantees of independence, impartiality and a proper procedure.^{xxii}
22. Second, it is necessary to recognise that practically, in order to initiate judicial review, the person concerned must be informed about the use of surveillance measures. The availability of an effective *ex-post* remedy therefore depends on the due notification of the measures to the person concerned. Recourse to a remedy is only possible if a person affected by surveillance measures is informed that the measures were implemented and that they have a right to challenge their legality retrospectively.^{xxiii} The Court recognises that notification can be delayed temporarily in certain instances where there are valid justifications for carrying out secret surveillance over a prolonged period of time, and where immediate *ex-post* notification would defeat the purposes of such surveillance. However, notification must be made as soon as possible without jeopardising the purpose of such delay.^{xxiv} After the surveillance has ceased, individuals should be notified of the measures taken against them without their knowledge to enable them to seek an effective remedy.
23. In the absence of notification, the law should at least provide for an independent mechanism that could enable individuals to ascertain whether they have been subject to secret surveillance, and if so, whether these measures have been implemented within the bounds of law or judicial

authorisation. In other words, this mechanism should be able to review the legality and proportionality of such measures *ex-post*, i.e. after their implementation, and, where a violation is found, to offer a remedy.^{xxv}

24. Finally, robust procedural guarantees must apply in the context of judicial review proceedings to enable the person concerned to challenge the surveillance measures effectively. The Court accepts that there can be certain limitations where the subject matter of judicial review concerns secret surveillance measures.^{xxvi} However, any restrictions on access to information which affect the adversarial nature and equality of review proceedings should be assessed individually by the competent judicial authority, and be applied only if the individual circumstances of the case so require. In accordance with the Court's ruling in *Zakharov*, certain minimum guarantees should not be subject to limitations at all: "[i]n order to be able to challenge the decision forming the basis for the interception of communications, the applicant must be provided with a minimum amount of information about the decision, such as the date of its adoption and the authority that issued it".^{xxvii}

Part D: Effectiveness of judicial control requires clear and foreseeable legal framework

25. The effectiveness of judicial control (whether *ex-ante* or *ex-post*) depends upon the robustness of the relevant applicable legal framework. The Court has clearly established that for interferences to be considered lawful under Article 8 of the Convention, the national law permitting surveillance measures must be (a) clear in relation to the conditions and circumstances in which authorities are empowered to resort to measures of secret surveillance and collect data; (b) foreseeable, especially in so far as the technology available to implement these actions is increasingly sophisticated,^{xxviii} and (c) adequately accessible.^{xxix} The national law must also set out minimum safeguards to avoid abuses in relation to secret surveillance including the nature, scope and duration of the possible measures; the grounds required for ordering them; the authorities authorised to permit, carry out and supervise such measures; and the type of available remedy.^{xxx}
26. In the field of criminal law and procedure, lack of clarity as to the definition of the offence for which certain powers may be used typically leads to overly broad use of powers by law enforcement authorities.^{xxxi} There is a particularly strong risk of surveillance powers being misused for counter-terrorism purposes. In the absence of a clear legal definition of what amounts to 'terrorism', counter-terrorism surveillance laws could end up subjecting an unnecessarily wide class of persons to surveillance measures, and they could undermine ability of judicial authorities to limit the use of surveillance powers.
27. Another key area of legal certainty which can give rise to abuse in the context of criminal investigations is around the definition of technological concepts such as the distinction within electronic information between "content data" and "metadata". There is no commonly accepted definition of either term. Definitions of electronic information are complex and constantly changing, as we see for instance in EU law.^{xxxii} Yet electronic information is increasingly being used in criminal investigations in Europe. According to the European Commission, electronic evidence in some form is relevant in around 85% of total criminal investigations.^{xxxiii} Poland is no exception. The Venice Commission indicated that the collection of metadata under Article 20(c) of the Police Act is "a widely used method of investigation".

28. Depending on how metadata is defined, surveillance laws could give relevant authorities intrusive access to sensitive personal data (including email headings and internet search records) without the checks or safeguards reserved for interceptions of content data. It is crucial that surveillance laws have clear, objective definitions to ensure that surveillance powers are subject to strict regulation.

Part E: The need to include specific safeguards to protect the right to legal privilege

29. The lack of clarity and foreseeability in surveillance laws pose a particularly direct risk to the right to a fair trial, where there are insufficient safeguards to protect privileged client-lawyer communications from state surveillance.

30. Confidentiality of communications between a defence lawyer and their client is protected not only by Article 8, but also by Article 6(3)(c) of the Convention. The privacy of client-lawyer communications is an individual human right, which is inextricably linked to the broader role defence lawyers play in safeguarding the right to a fair trial for their client, and the same stringent safeguards should apply under both articles. The absence of specific safeguards that prevent lawyers, including criminal defence lawyers, from being subject to surveillance measures seriously undermines the effectiveness of protections for client-lawyer confidentiality under the Convention.

31. The Court recognises this link in stating that *“an encroachment on [a lawyer’s] professional secrecy may have repercussions on the proper administration of justice and hence on the rights guaranteed by Article 6 of the Convention.”*^{xxxiv} Moreover, the role of a lawyer may and often does go further than safeguarding their client’s right to a fair trial. The Court recognised in *Salduz* that the right of a detainee to have access to legal advice is a fundamental safeguard against ill-treatment.^{xxxv} Any interference with the work of defence lawyers, including through secret surveillance, can have a serious negative effect on the protection of multiple Convention rights, including the protection of ‘core rights’.

32. It is also well-established in the Court’s jurisprudence that *“if a lawyer were unable to confer with his client and receive confidential instructions from him without such surveillance, his assistance would lose much of its effectiveness whereas the Convention is intended to guarantee rights that are practical and effective”*.^{xxxvi} Effective legal assistance is predicated on trust between the lawyer and client which requires the ability to communicate freely and openly, without fear or suspicion of these conversations being heard by someone else. The Court has recognised that *“lawyers are assigned a fundamental role in a democratic society, that of defending litigants. Lawyers cannot carry out this essential task if they are unable to guarantee to those they are defending that their exchanges will remain confidential. It is the relationship of trust between them, essential to the accomplishment of that mission, that is at stake.”*^{xxxvii} It is therefore of paramount importance that defence lawyers can use the available channels of communication with their clients freely, and are not hindered in the exercise of their function by the possibility of being subject to surveillance measures without proper safeguards.

33. *Ex-post* safeguards that prevent the retention, or that regulate the subsequent use of evidence obtained in breach of client-lawyer privilege cannot be regarded as sufficient on their own. This is especially the case where surveillance laws and/or evidentiary rules prevent the use of the

recorded information, but not the knowledge gained as a result of the interference. As the Venice Commission observes, *“listening to the conversations between the lawyer and his/her client the police may obtain important information which may lead to the discovery of inculpatory evidence, which may, in turn, be introduced in the criminal proceedings. Even if in the Polish criminal procedure evidence which is “the fruit of the poisonous tree” is inadmissible, listening to the conversations between the lawyer and the client gives the police a tactical advantage and undermines the trust which must exist between the defence lawyer and the accused.”*^{xxxviii}

34. The ability of law enforcement authorities to apply surveillance measures to lawyers will undermine trust and lead to self-censorship, creating a “chilling effect” on open lawyer-client communication and undermining the effectiveness of legal assistance. This amounts to an unjustifiable interference with the proper administration of justice. Strict safeguards should be in place to limit the possibility of applying surveillance measures to defence lawyers only to cases where there is strong evidence of personal and conscious involvement of a lawyer in the commission of a crime of sufficient public importance or gravity and only where the particular method of surveillance is appropriate for its effective investigation.^{xxxix}
35. The privacy of client-lawyer communications is currently an issue of heightened importance across Contracting States. Fair Trials’ research has found that criminal defendants have become increasingly dependent on remote communications to obtain legal assistance due to the COVID-19 pandemic, and increased restrictions on in-person legal assistance, especially for those deprived of their liberty.^{xl} This makes client-lawyer communications more susceptible to interception, and there is now a stronger need for clearer and more robust articulation of Articles 8 and 6(3)(c) rights by the Court to meet this challenge.

Part F: The need for systemic oversight

36. In our view, judicial oversight on a case-by-case basis must be complemented by systemic oversight by independent bodies that can oversee the operational activities of surveillance and law enforcement authorities, including the interception, collection, exchange and use of personal data, as well as the protection of the right to a private life.
37. The Court recognises the role of effective, independent expert bodies as an alternative to judicial supervision to exercise oversight of state surveillance powers.^{xli} When reviewing national legislation governing secret surveillance for compliance with Article 8, the Court held that *“where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.”*^{xlii} However, it also acknowledged that alternative independent bodies can be entrusted with similar powers, where those bodies are composed of suitably qualified decision-makers, such as those with experience of, or qualifications for judicial office, and experienced lawyers,^{xliii} and have powers to make independent and binding decisions.^{xliv}
38. In our view, independent expert bodies play a crucial role not as alternatives to judicial supervision, but as a supplementary form of supervision that is intrinsic to an Article 8 compliant regulatory framework on surveillance. In his concurring judgment in *Szabo and Vissy v Hungary*, Judge Pinto de Albuquerque remarked that *“in view of the enlarged consensus in international law ... and the gravity of the present-day dangers to citizens’ privacy, the rule of law and democracy, the time has come not to dispense with the fundamental guarantee of judicial authorisation and*

review in the field of covert surveillance gathering. Obviously, the judicial guarantee is not incongruous with an additional external guarantee of political, e.g. parliamentary, nature”.^{xlv}

39. *Ex-post* judicial control of the use of surveillance powers in specific cases cannot, on its own, amount to a comprehensive mechanism for ensuring systemic compliance with the Convention and the rule of law. Individual cases provide a snapshot of how digital information is being gathered, but they cannot provide a broader overview of practices. A more systemic overview of how electronic data is being used may, for example, be needed to assess whether there is a basis for concern about certain practices, such as the use of mass fishing expeditions or compliance with requests from states known to pursue politically-motivated prosecutions. Systemic oversight is essential in keeping state authorities in check and maintain public trust in law enforcement authorities. Adequate and effective oversight and control over executive authorities’ access to private information in the form of electronic data, as protected by Article 8 of the Convention, would help to ensure good practice by law enforcement and other authorities, by helping to identify systemic abuses of surveillance powers.
40. In Poland, Article 20(c) of the Police Act includes a requirement for a generalised summary report on metadata collection to be prepared every 6 months, which details only the number of cases where telecommunications, postal or internet data has been obtained and the type of data, and the legal or other justification for the use of such measures. Article 20(c) allows a district court judge to review and inspect this report, but this is not obligatory, and it is unclear what might motivate a judge to do this, which renders this already poor safeguard effectively meaningless. The Venice Commission noted that this reporting is insufficient to ensure the accountability of the police in respect of the operations related to metadata collection.^{xlvi}
41. According to the Statement of Facts, the Anti-Terrorism Act does not provide for systemic oversight of the surveillance activities carried out under that law. The Head of Prosecution is informed about the surveillance measures and, if he so requests, about the implementation of these measures and the information collected. However, there is no obligation for him or her to carry out systemic oversight, including systemic assessment of the justifications given for the application of surveillance measures nor their necessity or proportionality.

ⁱ *Klass and Others v. Germany*, App. No. 5029/71, Judgment of 6 September 1978, § 55.

ⁱⁱ Partly Dissenting opinion of Judge Spielmann joined by judges Rozakis, Tulkens, Casadevall and Mijović in *Bykov v. Russia*, App. No. 4378/02, Judgment of 10 March 2009.

ⁱⁱⁱ *Beraru v. Romania*, App. no. 40107/04, Judgement of 18 March 2014, §§ 69-70.

^{iv} Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, Article 7(2) and (3).

^v European Commission for Democracy through Law (Venice Commission), Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts, Opinion No. 839/2016, 13 June 2016, § 100.

^{vi} *Roman Zakharov v. Russia*, App. No. 47143/06, Judgement of 4 December 2015, §§ 291 *et seq.*; *İrfan Güzel v. Turkey*, App. No.35285/08, Judgment of 7 February 2017, § 105.

^{viii} *Bykov v. Russia*, App. No. 4378/02, Judgment of 10 March 2009, § 80.

^{ix} *Bykov v. Russia*, App. No. 4378/02, Judgment of 10 March 2009, §§ 96-98, 104.

^x *Dragoş Ioan Rusu v. Romania*, App. no. 22767/08, Judgment of 31 October 2017, §§ 51-55.

-
- ^{xi} ‘Fruit of the poisonous tree’ doctrine is derived from the exclusionary rule. Under this doctrine evidence which is obtained through or stems from illegally obtained evidence, such as illegally recorded conversations or mobile phone data, must also be excluded from the trial.
- ^{xii} Partly concurring, partly dissenting opinion of Judge Loucaides in *Khan v. the United Kingdom*, App. No. 35394/97, Judgment of 12 May 2000.
- ^{xiii} *Klass and Others v. Germany*, App. No. 5029/71, Judgment of 6 September 1978, § 49.
- ^{xiv} See. e.g., *Roman Zakharov v. Russia*, App. No. 47143/06, Judgment of 4 December 2015, § 232; *Kennedy v. The United Kingdom*, App. No. 26839/05, judgment of 18 May 2010, §§ 153-154.
- ^{xv} *Klass and Others v. Germany*, App. No. 5029/71, Judgment of 6 September 1978, §§ 55-56.
- ^{xvi} European Commission for Democracy through Law (Venice Commission), Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts, Opinion No. 839/2016, 13 June 2016, §§ 61 *et seq.*
- ^{xvii} *M.N. and Others v. San Marino*, App. No. 28005/12, 7 July 2015, § 81.
- ^{xviii} *Işıldak v. Turkey*, App. No. 12863/02, Judgment of 30 September 2008, § 51; *Gutsanovi v. Bulgaria*, App. No. 34529/10, Judgment of 15 October 2013, § 133, *Dragan Petrović v. Serbia*, App. No. 75229/10, Judgment of 14 April 2020, § 73.
- ^{xix} *Varga v. Romania*, App. No. 73957/01, Judgment of 1 April 2008, §§ 70-74.
- ^{xx} *Modestou v. Greece*, App. No. 51693/13, Judgment of 16 March 2017, §§ 52-54.
- ^{xxi} *Klass and Others v. Germany*, App. No. 5029/71, Judgment of 6 September 1978, § 56.
- ^{xxii} *Ibid.*, § 55.
- ^{xxiii} *Ibid.*, § 57, and *Weber and Saravia v. Germany*, App. No. 54934/00, Decision of 29 June 2006, § 135.
- ^{xxiv} *Roman Zakarov v. Russia*, App. No. 47143/06, Judgment of 4 December 2015, § 287.
- ^{xxv} *Kennedy v. The United Kingdom*, App. No. 26839/05, judgment of 18 May 2010, § 167: “[T]here is in principle little scope for recourse to the courts by the individual concerned unless (...) any person who suspects that his communications are being or have been intercepted can apply to courts, so that the courts’ jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications”, see also *Roman Zakharov v. Russia*, App. No. 47143/06, Judgment of 4 December 2015, § 234.
- ^{xxvi} *İrfan Güzel v. Turkey*, App. No. 35285/08, Judgment of 7 February 2017, § 99.
- ^{xxvii} *Roman Zakarov v. Russia*, App. No. 47143/06, Judgment of 4 December 2015, §§ 291 *et seq.*
- ^{xxviii} *Kopp v. Switzerland*, App. No. 23224/94, Judgment of 25 March 1998, § 2.
- ^{xxix} *Silver and Others v. the United Kingdom*, App. Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 and 7136/75, Judgment of 25 March 1998, § 87.
- ^{xxx} *Weber and Saravia v. Germany*, App. No. 54934/00, Decision of 29 June 2006, § 95; *Shimovolos v. Russia*, App. No. 30194/09, Judgment of 21 June 2011, § 68.
- ^{xxxi} Fair Trials, ‘Fundamental Freedoms on Trial – The human rights impact of broad counter-terrorism and anti-extremism laws’ (2019)
- ^{xxxii} Fair Trials, *Policy Brief: The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters*, October 2018, p. 8.
- ^{xxxiii} European Commission Impact Assessment, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, Brussels, SWD(2018) 118 final, 14 April 2018, p. 14.
- ^{xxxiv} *Erdem v. Germany*, App. No. 38321/97, Judgment of 5 July 2001, § 65.
- ^{xxxv} *Salduz v. Turkey*, App. No. 36391/02, Judgment of 27 November 2008, § 54.
- ^{xxxvi} *S. v. Switzerland*, App. Nos. 12629/87 and 13965/88, Judgment of 28 November 1991, § 48.
- ^{xxxvii} *Michaud v. France*, App. 12323/11, Judgment of 6 December 2012, § 118.
- ^{xxxviii} European Commission for Democracy through Law (Venice Commission), Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts, Opinion No. 839/2016, 13 June 2016, § 78.
- ^{xxxix} See also European Commission for Democracy through Law (Venice Commission), Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts, Opinion No. 839/2016, 13 June 2016, § 80.
- ^{xl} Fair Trials, ‘Beyond the Emergency of the COVID-19 Pandemic – Lessons for Defence Rights in Europe’, 2020, pp. 24-25.
- ^{xli} *Telegraaf Media Nederland Landelijke Media BV and Others v. The Netherlands*, App. No. 39315/06, Judgment of 22 November 2012, § 98.

^{xlii} *Klass and Others v. Germany*, App. No. 5029/71, Judgment of 6 September 1978, § 167.

^{xliii} *Klass and Others v. Germany*, App. No. 5029/71, Judgment of 6 September 1978, § 21 and 51; *Weber and Saravia v. Germany*, App. No. 54934/00, Decision of 29 June 2006, §§ 25 and 117.

^{xliv} See e.g., *Kennedy v. The United Kingdom*, App. No. 26839/05, judgment of 18 May 2010, § 166-168.

^{xlv} *Szabó and Vissy v. Hungary*, App. No. 37138/14, Judgment of 12 January 2016, § 23.

^{xlvi} European Commission for Democracy through Law (Venice Commission), Opinion on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts, Opinion No. 839/2016, 13 June 2016, § 113.