Kostenko OV, Ghaziani VA, 'Admissibility of illegally obtained e-evidence: A critical study of EU law and the precedents of the European Court of Human Rights' (2024) 2 EJPLT, 205 – 220.
DOI: https://doi.org/10.57230/EJPLT242OVKVAG

EJPLT
ISSN 2704-8012



Admissibility of illegally obtained e-evidence: A critical study of EU law and the precedents of the European Court of Human Rights

Ammissibilità delle prove elettroniche ottenute illegalmente: uno studio critico del diritto dell'UE e dei precedenti della Corte europea dei diritti dell'uomo

OLEKSII VOLODYMYROVYCH KOSTENKO
Associate Professor
Faculty of Law of the National Aviation University

VAHID AKEFI GHAZIANI
Pre-doctoral candidate
International University College of Turin
Attorney at law
Central Bar Association of Iran

Abstract

Whether illegally obtained evidence should be deemed inadmissible is a question that many jurisdictions still struggle with. In this regard, there is no internationally accepted standard that orients national jurisdictions in detaching valid from invalid evidence. This study focuses on the two-fold legal systems practiced within EU law and that of the European Court of Human Rights in order to identify their points of disagreement and to approximate the two systems. The outcomes suggest that the GDPR has not provided any balancing guidance for inconsistent fundamental rights; therefore, EU member states have wide discretion in prevailing one right over another. Despite this, aiming to protect EU fundamental rights, particularly the right to protection of personal data (Article 8 of the EU Charter) and the fairness procedure of a trial (Article 47 of the Charter), national courts, in the absence of domestic guidelines, are welcomed and urged to follow the ten-factor test of the judgment Beuze v. Belgium (ECHR, November 8, 2018). Finally, after examining the court's guidance, the paper at hand partially changes the test and offers a more reliable test to reconcile privacy rights with the right to a fair trial. This test could serve as a yardstick for national courts as well as upcoming ECtHR precedent.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
Se le prove ottenute illegalmente debbano essere considerate inammissibili è una questione con cui molte giurisdizioni ancora lottano. Non esiste un criterio riconosciuto a livello internazionale che orienti le giurisdizioni nazionali a tal riguardo. Questo studio si concentra sui due sistemi giuridici esistenti nel diritto dell'UE e in quello della Corte europea dei diritti dell'uomo al fine di identificare i punti di disaccordo e di avvicinare i due sistemi. I risultati suggeriscono che il GDPR non ha fornito alcuna guida per bilanciare i diritti fondamentali incoerenti; pertanto, gli Stati membri dell'UE hanno un'ampia discrezionalità nel far prevalere un diritto rispetto a un altro. Nonostante ciò, al fine di tutelare i diritti fondamentali dell'UE, in particolare il diritto alla protezione dei dati personali (articolo 8 della Carta UE) e l'equità del processo (articolo 47 della Carta), i giudici nazionali, in assenza di orientamenti nazionali, hanno accolto favorevolmente e sono sollecitati a seguire il test dei dieci fattori della sentenza Beuze c. Belgio (CEDU, 8 novembre 2018). Infine, dopo aver esaminato le indicazioni della Corte, il documento modifica parzialmente il test e offre un test più affidabile per conciliare i diritti alla privacy con il diritto a un processo equo. Detto test potrebbe servire da metro di paragone per i tribunali nazionali e per l'imminente precedente della Corte EDU.

Keywords: Admissibility of electronic evidence; European Court of Human Rights; EU Law; Fair trial; Fundamental rights; Right to privacy

Summary: Introduction. – 1. Legal sources. – 1.1. EU Legislations. – 1.2. Defensible argument. – 2. Precedents of the ECtHR. – 2.1. Discourse about the role of e-evidence. – 2.2. What has been done so far? – 2.3. Defensible argument. – Conclusion.

Introduction.

Beyond any doubt, the probative value of evidence plays a game-changing role in trial procedures. However, over time, as electronic evidence has gained similar value to old forms of evidence, traditional standards of proof have been exposed to significant changes.[1] Besides, the development of new technology, tech-friendly legal approaches,[2] and the hardships usually involved in gathering physical evidence have all eased and spurred the presentation of e-evidence in judicial procedures.[3]

[1] One major distinguishing feature of digital evidence is its authenticity. Democratic societies have often laid down lengthy and in-depth guidelines for digital forensics with respect to different stages, including pre-lab investigations and prior as well as post-trial stages. For instance, see Association of Chief Police Officers, *ACPO Good Practice Guide* (Cm version 5.0, 2012) section 2. Also see relevant attempts by the European Union in: Council of Europe, 'iPROCEEDS-2: Launching of the Electronic Evidence Guide v.3.0' (Council of Europe, 22-23 June 2022) <https://www.coe.int/en/web/cybercrime/-/iproceeds-2-launching-of-the-electronic-evidence-guide-v-3-0> accessed 21 May 2024.

[2] For instance, through the Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market [2014] OJ L 257/73, the admissibility of electronic signatures (Art. 25), electronic seals (Art. 35), electronic time stamps (Art. 41), and electronic documents (Art. 46) have been ensured and proposed for the national electronic identification scheme throughout EU member states (see P. 9 of the said Regulation).

[3] National lawmakers are not the sole actors facilitating and ensuring the e-evidence exhibition; cross-border powers likewise do the same; as an example, see European Parliament and Council Regulation (EU) 1543/2023 of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal

Moreover, national jurisdictions have different viewpoints in regard to the admissibility of illegally obtained evidence,[4] which has sparked a lot of concern among scholars in order to harmonize national jurisdictions in the paradigm of mutual admissibility. [5] Nevertheless, the idea of borderless obtaining of evidence and cross-border admissibility, however impressive it sounds, embraces various problems due to the dissimilar domestic frameworks.[6]

Such evidences simultaneously carry out two attributions: first, they form the facts of the case, and second, they indicate that the undergone investigatory procedure contained some illegal elements that led to a breach of a legal provision.[7] Whether courts should accept illegally obtained evidence will make an extensive difference; not only might the outcome of a dispute be subjected to a substantial change, but also the admission of such evidence will further impact the democratic values within a society. This paper examines the admissibility issue of e-evidence, where the evidence is gathered through infringing the right to the protection of personal data.[8] However, the paper has taken a legal-dogmatic methodology and therefore does not address interdisciplinary analyses. Meanwhile, concerning the approach, this survey attempts to develop an approximate matching point for two closely related but

proceedings [2023] OJ L191/118 p. 2 and 4. This regulation has set out the framework for preserving and production of e-evidence across the Europe. Another example is the Directive 2014/41/EU of the European Parliament and of the Council regarding the European Investigation Order in criminal matters [2014] OJ L130/1, see specifically Article 9 which ensures the without delay execution of European Investigation Orders (EIO). However, this paper does not address the judicial procedures in cross-border paradigm.

[4] K Ligeti, B Garamvölgyi, A Ondrejová, and M von Galen, 'Admissibility of Evidence in Criminal Proceedings in the EU' (2020) 3 eucrim, 203 <https://eucrim.eu/media/issue/pdf/eucrim_issue_2020-03.pdf> accessed 6 June 2024. However, when it comes to the admissibility issue, it is indispensable to designate the grounds on which electronic evidence is deemed admissible or inadmissible. Regardless of the illegal methods through which evidence is obtained, there are often several grounds in different systems that constitute a basis for rendering e-evidence inadmissible. Depending on how we define admissibility and authenticity, the justification for which e-evidence would be suppressed differs. For instance, in *Lorraine v. Markel American Ins. Co.* 241 F.R.D. 534 (D. Md. 2007) at para 542. The judgment classified 'authenticity' as a category under 'admissibility' of e-evidence. However, we think the two concepts should have different meanings and scopes of application. The authenticity of e-evidence refers to a situation where there is a link between afforded evidence and an actor (ex., a wrongdoer or claimant). In the absence of such a link, the contested evidence shall not be attributed to the accused and is therefore invalid (not inadmissible). To see advocates of this proposal, turn to C Reed, 'The admissibility and authentication of computer evidence - a confusion of issues' (1990) 6 CLSR 13. Seemingly, the same advocacy could be seen in C Singh, *Unlocking the law of evidence* (4th edn, Routledge Publishing 2023) 17 (Questions of admissibility are questions of law.) On the contrary, section 28 U.S.C. § 1731 and the mentioned judgment in *Lorraine v. Markel* seem to have adopted a wider conceptual domain for 'admissibility.'

[5] M Kusak, 'Common EU Minimum Standards for Enhancing Mutual Admissibility of Evidence Gathered in Criminal Matters' (2017) 23 Eur J Crim Policy Res, 337. Recently, European Law Institute has published a draft proposal on the matter as well, see C Wendehorst (Director), *'ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings'* (Draft Legislative Proposal of the European Law Institute, European Law Institute 2023), in Article 2 (scope).

[6] M Corhay, 'Private Life, Personal Data Protection and the Role of Service Providers: the EU E-Evidence Proposal' (2021) 6 European Papers, 441, 444.

[7] Legal duties or rights, and manifestly fundamental rights, might be the subjects of a breach. However, minor breaches are mostly overlooked by legal systems. These types of violations usually do not form a situation in which a judge should consider their dismissal or approval of admissible and authentic evidence. This idea of ignoring minor breaches has also been reflected in the well-known maxim '*De minimis non curat lex*' which translates to 'trifles are not the matter of the law's consideration.' See, BA Garner, *Black's Law Dictionary* (9th edn, Thomson Reuters 2009) 496.

[8] Article 8 of the EU Charter of Fundamental Rights (Protection of personal data) and Article 8 of The European Convention on Human Rights (Right to respect for private and family life).

different legal systems: The European Union and the European Court of Human Rights. (ECtHR).[9]

Nevertheless, since the market for sensitive data is astonishingly influencing the data economy[10] and correspondingly gaining intense consideration in scholarly debates and academic research,[11] the paper also examines evidence related to sensitive information to better organize its context.[12] The trajectory of the present paper could be sketched out as follows: The first part examines the current legal framework of the EU in response to the illegitimate obtaining of e-evidence. Cross-border disputes, such as those initiated with the issuance of EU warrants and the EU itself, are entirely outside the scope of our argument.[13] Conversely, part one clarifies the perspective of the EU's legal instruments, including the General Data Protection Regulation (2016). This part, along with exploring GPRS' relevant provisions on the admissibility issue, argues that the topic has fallen beyond the interest sphere of the EU's legislative. In other words, this part clarifies two issues: 1. Has the EU touched upon domestic procedures in any manner that serves member states in determining the admissibility of ill-founded evidence? 2. To what extent is the EU's legal framework capable of balancing different conflicting fundamental rights (namely, data protection on one side and other fundamental rights on the other)? This part also considers an argument about sensitive data (Article 9 GDPR), since it may shed light on the status of non-sensitive personal data. Consequently, the second part discusses the approach of the European Court of Human Rights' approach in terms of the admissibility issue. In this part, two questions have been raised and answered: 1. What is the perspective of the

[9] Although the two distinct systems stem from dissimilar treaties, they relatively hold a close connection in our argument since Articles 6 and 13 of the Convention are reaffirmed by Article 47 of the EU Charter. See, the Judgment of 27 Februrary 2018, Associação Sindical dos Juízes Portugueses v. Tribunal de Contas, C-64/16, EU:C:2018:117, paragraph 35.

[10] Namely, health data (as classified under Article 9(1) GDPR) has seen glaring economic growth over recent years. It is noteworthy that, while the worldwide market for digital health reached 45.69 billion dollars in 2017 and 170.25 billion dollars in 2023, it is estimated to peak at 274.93 billion dollars by 2028. See Statista Market Insight, 'Digital Health – worldwide' (Statista, Updated February 2024) <https://www.statista.com/outlook/hmo/digital-health/worldwide> accessed 21 May 2024.

[11] In addition to economic value, many research studies also address ethical issues of the case. For instance, considering the de-identification of personal data through available or publicized information has led some authors to propose the idea of prioritizing regulatory attempts on the public flow of data rather than private shares. Therefore, if a website faces normative restrictions on publicizing personal information, the tactics of hackers and infringers (which are similar to reverse engineering methods) would probably reach a dead end. See, P Ohm, 'Broken promises of privacy: Responding to the surprising failure of anonymization' (2010) 57 UCLA LR 1701, 1776.

[12] Vividly, whenever a legal instrument addresses one of the two categories of data (sensitive or non-sensitive personal data) due to their shared features of being, firstly, 'data' and secondly, 'personal data,' which are not yet publicized, it tacitly addresses the other category. For instance, in light of the provisions of GDPR, one could benefit from both Art. 6 and 9 when they are normalizing a share feature. This is due to the fact that the tenors of specific provisions (or, let's say, propositions in general) are often enlightened through the context of the general ones. Canon principle of 'Ejusdem generis' namely remarks how the sequence of general and specific should be used in interpreting the text of law. See related judgments in G A Dietz, 'Statutory Construction: Ejusdem Generis Versus Legislative Intent' (1950) 3 Fla. LR 258. At the time of writing this paper, the famous case (of *Fischer v. United States* (Docket No. 23-5572)) related to the U.S. Capitol attack of 6 January 2021 is pending in the Supreme Court of the United States. The case, however, deals with the interpretation of section 18 U.S. Code § 1512(c)(2) regarding obstructing official proceedings and one of the centralized arguments in the case touches on the role of Ejusdem maxim in the interpretation of the article; see, for example, pp. 13–15 of the filed response of petitioner 'J. Fischer' (filed on 28 March 2024) in the case.

[13] See, n 2 and 3.

ECtHR in confronting claims where the evidence of a dispute was obtained in such a manner that undermines the Article 8 of the European Convention on Human Rights (hereinafter, the Convention)? 2. Despite what the court has done so far, should the court's practical guidelines be altered or replaced by a new instruction in order to protect the effectiveness and objectives of the Convention?

Finally, It should be pointed out here that the current paper delimits its scope to precedents of the ECtHR[14] and EU law. Undoubtedly, the procedures of the CJEU will contribute to the interpretation of the GDPR. Therefore, the basis of the old case laws of the court related to Directive 95/46/EC will gradually phase out and be substituted by new perspectives outlined in GDPR (2016).[15] Likewise, the decisions of the ECtHR have the same role. Furthermore, since there are numerous grounds for evidence to be rendered inadmissible, except the one that deals with inadmissibility given to individuals' privacy infringement, other grounds are not considered in this paper.

1. Legal Sources.

1.1. EU Legislations.

Incident response, which is often conducted by parties to a case or their agents[16], digital forensics, and typical legal discoveries could all be involved before presenting digital evidence at trial. Courts, however, by being cautious about admitting this evidence, have highlighted the pivotal role of e-evidence in judicial hearings. [17] Nevertheless, no unique standard has so far been introduced by the EU lawmaker in harmonizing domestic judicial procedures or the EU's internal judicial order. [18] Whereas the EU Charter grants discretion to

[14] Since the protection of individuals' privacy falls within the scope of the EU Charter (Articles 7 and 8), the Court of Justice also has the authority to practice its competence in order to judicially preserve the said right. In doing so, an action for annulment (according to Art. 263 of the Treaty on the Functioning of the European Union) or either a preliminary reference by a national court (Art. 267 TFEU) are the two routes through which the court decides on the mentioned issue. Take as an example the recent case of the Court, wherein the Court, in response to the preliminary reference by the Brussels Court of Appeal, recognized TC String (transparency and consent string) as personal data under Art. 4(1) of the GDPR if there is a reasonable likelihood of re-identification (in the phrasing of the Court, the criterion is 'reasonable means'). See Judgement of 7 March 2024, *IAB Europe,* C-604/22, EU:C:2024:214, paragraph 43. For action of annulment, turn to the Order of the General Court on 7 December 2022, *WhatsApp Ireland Ltd v EDPB*, T-709/21, EU: T:2022:783, paragraphs 15 and 16.

[15] A Guzewicz, 'Uniform interpretation of General Data Protection Regulation concepts as a new challenge for CJEU' (2020) special Issue EJPLT, p. 8.

[16] Cyber engineers, for ensuring the organisation's network, take into account all the present or forthcoming incidents that may threaten its security. A Zamfiroiu and R C Sharma, 'Cybersecurity Management for Incident Response' (2022) 4 RCSJ 69, 69-75. Therefore, digital evidence of a crime might be gathered through this route.

[17] For instance, see *State v. Acosta* 311 App. 136, 489 P.3d (Or 2021) at para 608; *Commonwealth v. Carrasquillo* 13122 (Mass 2022). Both cases directly addressed the admissibility issues of evidence arising from sharing incriminating posts on social media. Also see the judgement in *Commonwealth v. Yusuf* 488, 379 (Mass 2021).

[18] While in recent years the issue has captured the EU's attention, the endeavours culminated in proposal 2018/0108 (European Production and Preservation Proposal) and ended up with the Regulation of 2023/1543, which sought to harmonize the existing context of obtaining e-evidence across borders. Regardless of this commendable move, the current legacy for diagnosing data safety within undertakings of national jurisdictions can be found in the provisions of the General Data Protection Regulation and the e-

the member states to codify effective regulations in compliance with EU fundamental rights, this, at first glance, justifies the silence of EU legislators in the case. Article 15 of Directive 2002/58/EC (ePrivacy) mandates member states to enact proportionate legislative measures to protect against the unauthorized use of electronic communications or activities that pose a risk of breaching the confidentiality of e-communications (as provided in Art. 5).[19] The general principles of the GDPR, on the other hand, reflect a clear-cut outlook for minimizing the risks of unlawful data processing. For instance, Article 5(1)(c) [20] and Art. 25 (Privacy by design and by default) have laid the groundwork for optimized methods of de-identifying, which must be followed by member states' domestic laws. [21]

However, a subtle inconsistency between the objectives [22] and other provisions of the GDPR could be observed.[23] GDPR allows holders of sensitive data, for instance, healthcare centers, to freely exchange patients' data; under the circumstances of Article 9(2)(f) processing of special categories of data (sensitive personal data) is not prohibited. The paragraph reads:

'processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity'

Privacy Directive. Frustratingly, given the tenor of Art. 15(1) of the European e-privacy directive, member states may approve legal guidelines for preventing illegal disclosure of personal data, such as interception of communication (Art. 5, e-privacy), but the directive per se has not provided detailed consideration about the admissibility of e-evidence.

[19] Since the evaluation of evidence, introducing standards of proof, and the allocation of *onus probandi* often mingle with the domestic sense and traditional legal customs of each member state, this might justify the lack of intervention from the EU. Also, the relevant competences of the EU should be considered. Whether regulating the current issue falls within the competencies alluded to in the Treaty on the Functioning of the European Union (TFEU), notably Articles 3 and 4, which have addressed the exclusive and shared competences of the EU, is also a crucial matter in need of solution.

[20] Principle of Data Minimisation.

[21] The exact method for de-identification, such as anonymization or pseudonymization, has not yet been established through EU law. In terms of sensitive data, specifically health data, Art. 44(2)(3) of the proposal for European Health Data Space (2022/0140 (COD)) signaled both anonymization and pseudonymisation as safe methods under the principle of data minimisation. Even with this clarification, the acceptable techniques of anonymization and pseudonymization still suffer from a lack of certainty, which makes health service centers and, in general, holders of sensitive data hesitant to employ legitimate techniques.

[22] See, Article 1 (2) GDPR and Recital 4.

[23] However, not to mention that governments also tend to accept illegal evidence, even if it is obtained through an illegitimate route. They might justify this policy with countless arguments. Mostly, such excuses try to overweight public interest or much more convoluted notions such as national security. However, in the digital era and in the context of sensitive data, the policy of 'ends justifies means' should be interpreted narrowly. Several reasoned explanations are capable of reinforcing the proposition. First and foremost, the abstract concepts of public interest or security are extremely flexible. They are prone to being easily abused or misused by their supplicants; whatever they plead for, they can simply interpret such concepts in their own favor. Second, the proliferation of digital means and the rapid reliance of society on digital areas have given rise to high expectations among users and are transforming the present form of life. In the meantime, in accordance with social needs and expectations, the law should be tasked with organizing an intense volume of human behavior in terms of legality and accountability. Moreover, in any case where illegitimate evidence finds its way to the tribunal, there will always be numerous negative consequences: 1. The exhibition of ill-founded evidence, even if suppressed by the court, leaves its traces on judge's bias and state of mind, which directly target the impartiality of judges. However, since there is no palpable deviation of the court from the rule of law, there would be a minor chance for the defendant to successfully challenge a biased decision in these circumstances. 2: The judgment allowing such evidence opens the floodgate to many other allegations and disputes. It may also pave the way for frivolous claims as well as dilatory tactics by parties. 3: The judgments trying to balance 'right to a fair trial' or 'public interest 'and 'protection of data' intensively influence the interpretation of the aforementioned concepts. The court's interpretation methodology, even if mistakenly applied in a specific case, potently inspires future judgments, the legal framework of the nation, and scholarly debates.

GDPR has not only left the issue of admissibility unresolved but also, given the general tenor of Article 9(2)(f), has offered a conservative and broad leeway for member states. The four grounds of necessity, as marked out in this paper, allow national courts to arbitrarily apply the law. Should the warrantless prosecutorial interrogations, police interrogations or even an inquiry from a potential claimant fall in the domain of 'establishment' or 'exercise,' it would have a game-changing role in legal procedures. However, Article 10 demystifies the procedure that is legitimate for gathering incriminating data. Here we are not arguing that the essence of 'data protection' entails banning warrantless access to sensitive data, which both Article 10 of GDPR and the Law Enforcement Directive (2016)[24] emphasize, but the sole suggestion is that warrantless access or any other type of illegitimate evidence gathering should not divert courts from assessing the admissibility of afforded evidence in their decision-making process. In other words, the GDPR does not balance the contradictory battle of fundamental rights;[25] rather, it hands over the task of weighing two or more inconsistent rights to national courts. Therefore, if an inquiry into a hospital has been made by an interrogator, government officer, or individual who has asked the data holder for the personal information of a patient, the court should assess the validity of the evidence with respect to GDPR. This is because the GDPR does not aim to balance two conflicting fundamental rights, and its provisions attempt to protect personal data in a pre-dispute area with an inhibitory approach.[26]

However, if an objection raises and alleges that GDPR provided by Recitals 1, 2, and 4 considers a potential clash of different fundamental rights, such as the right to a fair trial as pointed out in Recital 4, we dispute this argument by three major points:

1. Recital 4 calls for three conditions in order to strike a balance between 'protection of personal data' and other fundamental rights: a) This right should not be considered an absolute right; b) It should be perceived with respect to its societal functions. c) The balance between its peer fundamental rights should be stuck in accordance with the principle of proportionality. Consequently, the Recital tips off what the regulation has

[24] Article 10 of the Directive (EU) on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data [2016] OJ L 11/89.

[25] For instance, if privacy, freedom of speech, or the right to a fair trial contradict each other, no reasoned measurements have been taken by the Regulation.

[26] The main goal of GDPR is to leave behind a deterrent effect. Hence, provisions imposing rigid requirements of opt-in consent (e.g., Art. 7 and Recital 32), severe sanctions (e.g., Art. 83), and uncompromising obligations on the part of data holders (e.g., Art. 24, 25, and 31), all together with the asymmetrical distribution of rights and duties among data subjects and data holders (see GDPR, Chapter 3, Arts. 12–23), convey an overemphasis on the inhibitory approach of its nature. Albeit, the objectives of GDPR as set out in Article 1 are twofold: 1) protecting fundamental rights; and 2) free flow of personal data. See General Secretariat of the Council 14994/1/19 REV 1 of Council's position and findings on the application of the General Data Protection Regulation (GDPR) [2020] JAI 1312, paragraph 1); However, the provisions of GDPR lack an all-inclusive balancing between different fundamental rights, examining relevant rights and duties in court procedure, a profound examination of moral damages with delimitation of their applicatory scope (Art. 82), and frustratingly, a lack of any provision in regard to allocating administrative fines (in particular whether or not the lack of negligence would completely eliminate or diminish the amount to a trivial sum).

done so far with these words: 'This regulation respects all fundamental rights and observes the freedoms and principles recognized in the Charter.' However, this enigmatic silence right after addressing the three requirements of balancing, which baffles every reader in the latter two phases (societal function and accordance with the proportionality rule), should be considered a clue that singles out the imbalance approach of GDPR's measurement. [27]

2. The convoluted process of balancing two or more fundamental rights is fettered by a deep analysis of the different matrixes of each case and is a time-consuming process that seems to be much more case-based than an absolute theory capable of applying in all circumstances. The same approach was followed by the *Satamedia* case, where the judgments declare: 'In order to strike a balance between two different fundamental rights, the protection of the right to privacy requires that the limitations of Directive 95/46/EC in regard to data protection must apply where it is strictly necessary.[28]
3. The objective of the Regulation targets the main concern that matters to the legislator, which is prioritizing free movement of data over data protection (Art. 1 para. 3).[29]

1.2. Defensible argument.

Considering all factors above, the admissibility of e-evidence data in court is completely an alien subject to GDPR. Although the issue directly influences trial procedure, judgments' impartiality, and eventually the probable undermining of the right to a fair trial, the GDPR provides no guidance. Be that as it may, even though the admissibility test has been left blank in the EU legal framework, national courts in abiding by their domestic legal system, take charge of deciding whether the evidence should be suppressed in cases of illegal processes or not. Therefore, where a public body or law enforcement legally gathers sensitive data that is evidence of an imminent threat to public interest or security, there would be no perplexity since a clear-cut rule of law governs the matter. Conversely, a vexing dilemma emerges in a case where such evidence was obtained illegally and both parties are before a national court, struggling to overcome each other by bolstering their own baskets of evidence. In the scenario mentioned, the judge should first decide the validity

[27] Falling into semantic traps where the speaker mentions half-information (half-truth) and leaves the conclusion open to audiences has always been typical among people. Over time, this experience led to the coining of a pertinent proverb: '*qui tacet consentire videtur ubi loqui debuit ac potuit*,' which translates to 'He who is silent in a situation where he ought to have spoken and was able to, is taken to agree.' In parallel with this common understanding among people, different legal systems started to normalize legal conditions of silence and half-truths. Nowadays, almost all legal systems have codified the rule and encapsulated it in various sub-principles, such as misrepresentation and fraud. There are cases where silence might be a ground for recognizing implied consent; for instance, see *B.Shanmugam v. Thulasirama Reddy* S.A.No.495 (Madras 2011) (silence of counsel before the court), *Nottingham Patent Brick & Tile Co v Butler* [1886] 16 QBD 778 (CA) (half-truth may amount to misrepresentation).

[28] Judgment of 16 December 2008, *Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 56

[29] This reading from the third paragraph might be challenged in various ways due to its flexible tone. Nonetheless, it is noteworthy to mention that the free flow of data holds significant importance for GDPR as it has been allocated in the first article. On the other hand, the silence of the provision about balancing fundamental rights must not be overlooked.

and authenticity of the data and then examine the substantive issues of the case. The way in which a judge evaluates the admissibility of e-evidence has a direct influence on the EU's fundamental right to a fair trial. We suggest that this gray zone should not be solved by referring to GDPR, which does not deal with balancing fundamental rights. Up to now, it is perceivable that harmonizing right to data protection and the right to a fair trial must not be interpreted according to the provisions of the GDPR. However, in the next part, a reliable standard for courts and legal practitioners will be provided in order to resolve the quarrel.

2. Precedents of the ECtHR.

While EU legislation tends not to oversee the e-evidence admissibility issue, the current stance of the ECtHR (hereinafter, the court) system reveals a much more practical approach. However, the admissibility of a claim in the Court is completely different from admissibility of an evidence. The criteria for the latter has been enshrined in Article 35 ECHR.

The Court in order to assess the impact of procedural failings has established a test known of 'overall fairness'.[30] According to this test, the court must consider ten factors in order to determine the admissibility of evidence. The ten-factor test is designed to ensure that obtaining and presenting evidence at trial and procedural actions of domestic law enforcements do not jeopardize the accused's fundamental rights, notably the right to a fair trial (Art. 6 ECHR). The factors introduced by the court are as follows:

1. 'The court determines whether the applicant holds a type of physical or mental vulnerability;
2. The legal framework applied in pre-trial stage and the admissibility of evidence gathered at trial. In addition, the court should consider the chance of applying the exclusionary rule to inadmissible evidence, although it is unlikely that the whole proceeding will be considered unfair;
3. The opportunity to challenge the authenticity of the evidence and oppose its use;
4. Whether the evidence is reliable (quality of evidence), and the circumstances in which the evidence was obtained may raise doubt on its reliability, the court should also consider the nature and degree of any compulsion.
5. If the evidence was gathered unlawfully, the court should take into account the nature of the unlawfulness process and, where it violates other Convention Articles, also the nature of the violation.
6. In case where evidence is in the form of statement, the nature of the statement and whether it was immediately retracted or modified;
7. Evaluating the probative weight of the evidence, whether it forms an integral or significant part of probative evidence, and the strength of the other evidence in the case;

[30] *Beuze v. Belgium* [GC], 09 november 2018, no. 71409/10, § 150, ECHR 2018

8. Whether the evaluation of guilt was conducted by professional judges, lay jurors or lay magistrates. Also, any given direction or guidance made by them;
9. The existence of public interest and its weight in the prosecution and punishment of some specific offenses in issue;
10. Relevant procedural measurements given to domestic law or it's practice.'

The Court, however, has no tendency to evaluate validity of each piece of evidence. This is not the court's task.[31] In fact, the court practices its judicial capacity after the exhaustion of 'all domestic remedies'.[32] Nevertheless, the aforementioned test even though attempts to provide an overall fairness test, lacks in linking the domain of Article 6 (ECHR) [33] to Article 8 (ECHR) [34]. Nevertheless, up to now, the court's judicial records show a less supportive approach in order to establish a nexus between the two said rights. Most judges have so far overlooked the junction either by interpreting Art. 6 and 8 independently and ignoring the existence of any correlation between the two or by noting that the Convention does not address the admissibility issue of evidence due to its domestic essence.[35] On the contrary, the court in some specific areas has shown an extremely different perspective on protecting fair trial procedures. This often happens when the factual matrixes of a case hint at a breach of a law that could directly hamper the fairness of a trial. For instance, regarding the lawyer-client relationship (concerns about times of visit, access limitations, and the safety concerns of video conferences), [36] the court has intertwined the confidentiality of lawyer-client communications with the right to fair trial. In addition, while it is hard to discover the exact scope of Art. 6 due to its abstract wording, judges have tended to include various cases within the domain of a fair trial. Besides, the abstract wording of Art. 6 of the Convention did not hinder the court from further recognizing other look-alike scenarios in which fairness could be endangered. In doing so, the court has also successfully linked questioning the accused, confession, the right to remain silent, [37] inciting

[31] See *Vučković and Others v. Serbia*, 25 March 2014, no. 17153/11, § 69-77, ECHR 2014
[32] See Articles 13 and 35 (1) of the ECHR
[33] Related to 'right to a fair trial '
[34] Related to 'right to respect for private and family life'
[35] See the decision in *Bykov v. Russia* [GC], 10 March 2009, no. 4378/02, § 88, ECHR 2009 (the admissibility of evidence primarily falls within the national law regulations); *Khan v. the United Kingdom,* 12 May 2000, no 35394/97, § 34, ECHR 2000; *Schenk v. Switzerland*, 12 July 1988, no 10862/84, § 45, ECHR 1988; and *Moreira Ferreira v. Portugal* [GC], 11 July 2017, no. 19867/12, § 83, ECHR 2017-II.
[36] *Gorbunov and Gorbachev v. Russia*, 1 June 2016, nos. 43183/06 and 27412/07, § 37, ECHR 2016 (Lack of sufficient time for lawyer-client communications); *Salduz v. Turkey* [GC], 27 November 2008, no 36391/02, § 54, ECHR 2008 (Restriction on early access to lawyer); *Sakhnovskiy v. Russia* [GC], 2 November 2010, no. 21272/03, §§ 101,102, ECHR 2010 (limited time for lawyer to study the client's case file). *Öcalan v. Turkey* [GC], 12 May 2005, no. 46221/99, §§ 133, 135, ECHR 2005 (client's inability to consult a lawyer out of the hearing of a third party); *Rybacki v. Poland*, 13 April 2009, no. 52479/99, § 61, ECHR 2009 (safe and unhindered contacts of lawyers with their clients); *Moroz v. Ukraine*, 18 September 2017, no. 5187/07, § 68, ECHR 2017 (denial of private conversation between lawyer and client).
[37] *John Murray v. the United Kingdom* [GC], 8 February 1996, no. 18731/91, § 45, ECHR 1996; *Bykov v. Russia* [GC], no 4378/02, § 92, ECHR 2009.

suspects to commit crimes by entrapment,[38] and degrading treatments such as torture [39] (subject to Art. 3 of the Convention).[40]

In summary, it could be perceived from the above judgments that if a breach of legal duty is capable of significantly affecting the trial procedure, it is highly likely to establish a connection between the notions of Articles 6 and 8. Nonetheless, if the breach relates to privacy rights and not those mentioned earlier, the court tends not to overshadow the priority of delivering justice by excluding evidence obtained unlawfully. [41] It is remarkable to address here that many cases of the court merely deal with the tenor of the Art. 35 (1) ECHR. The procedural orders of the court necessitate a complaint to be meticulously cautious in bringing up his claim. If by any means, one of the admissibility requirements ignored, the court release itself from further examination of case and instantly makes its' mind to dismiss the case.[42]

---

[38] *Khudobin v. Russia*, 21 January 2007, no. 59696/00, § 128, ECHR 2006.

[39] *Jalloh v. Germany* [GC], 11 July 2006, no 54810/00, § 99, 105, ECHR 2006. The most relevant and unmentioned element in Article 6 ECHR, which is directly laid down in Article 14(3)(g) of the International Covenant on Civil and Political Rights, is the 'right against self-incrimination.' However, this is a 'generally recognized international standard,' and it might be the reason for the certainty of the court's rulings concerning discriminating treatments. See T Thienel, 'The Admissibility of Evidence Obtained by Torture under International Law' (2006) 17 EJIL, 349, 356.

[40] For a more elaborated list of case laws, see Council of Europe, Guide on Article 6 of the European Convention on Human Rights, updated on 31 August 2020, pp. 41, 44-47, 92-93, available at <https://www.echr.coe.int/documents/d/echr/guide_art_6_criminal_eng > accessed 09 February 2024.

[41] This approach echoes the old edict of '*Fīat iūstitia ruat cælum*' which suggests that justice must be done regardless of any consequences it may have. The famous axiom '*Justice must not only be done, but must also be seen to be done*' laid down by Lord G. Hewart also reflects the high public demand for delivering justice. For more useful explanations on the literature and relevant topics to the dictum, see A R Oakes and H Davies, 'Justice Must Be Seen to be Done: A Contextual Reappraisal' (2016) 37 ADLR 461. The applicable sphere of the dictum, moreover, has already been highlighted by Art. 6 of the ECHR; see Justice Committee of the House of Commons, *Public opinion and understanding of sentencing: Government and Sentencing Council responses to the Committee's Tenth Report of Session 2022–23*, (2024-01, HC 442) 2.

[42] For instance, see *Schenk v. Switzerland*, 12 July 1988, no. 10862/84, § 47, ECHR 1988. In a recent case, one of the main justifications of the judgement was that defendant had not used the opportunity to challenge the authenticity of incriminating evidence. in a case where the applicant, who was an employee (a medical representative) of the defendant (a pharmaceutical company), filed a complaint with the National Data Protection Commission (CNPD) in regard to breach of private data committed by the company through the installation of GPS in employees' vehicles. Subsequently, the CNPD did not affirm any privacy infringement. The applicant then challenged the decision, but the CNPD reaffirmed the previous resolution. In 2014, the company dismissed the applicant due to the outcome of a disciplinary proceeding based on the accusation that the applicant had manipulated the installed GPS to reduce the traveled distance and therefore evade the company's travel limitations. Consequent to the justification made by the first instant court and the Court of Appeal for his dismissal, he eventually, in 2016, lodged a complaint before the ECtHR, where four judges unanimously held that the signed agreement between the company and the applicant, by its wording clearly grants the company the right to monitor the travelled distance of the employees by installing GPS. Despite this, the Court stated that all the obtained geolocation data are not valid since some of those data consist of monitoring the applicant's professional activities. The Court, nevertheless, to evaluate whether there was an infringement or not, somehow absolved its duty by indicating that the applicant had enough opportunity to avert his dismissal by challenging the domestic court's decision. Following this vindication, the Court concluded that the use of GPS in the case did not undermine the principle of fair trial under Art. 6(1) of the ECHR. See paragraphs 4-26, 132, 142 and 145 of the case. The court, however, did not exclude the evidence gathered by GPS. See *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, 13 December 2022, no. 26968/16-2022, ECHR 2022. Furthermore, the judgment in *Uzun v. Germany* also considers whether geolocation data gathered during governments' surveillance measurements were valid. The court stated that, in accordance with the case law of the court, Article 8(2) of the Convention, notably the phrase 'the law' therein, should be interpreted in the sense that the measurements must have some basis in domestic law. See *Uzun v. Germany*, 2 December 2020, no. 35623/05, § 60, ECHR 2010.

[42] Beuze v. Belgium (n. 27) 150 (C).

Regardless of the articulated situations where the court has a clear standpoint, [43] the delimitation of the applicable scope of fair trial and illegitimate evidence gathering has yet to be explored.

2.1. Discourse about the role of e-evidence.

Back to e-evidence, the literature of the Court is even more blurry than expected. However, among the sparse literature available, there are some unproductive discussions that do not contribute to mapping out boundaries for the present debate. Nevertheless, the reluctance of the court in broaching a general test is noticeable in concurring opinion of Judge Cabral Baretto in case of Bykov v. Russia[44] where he states:

'I find it regrettable that the Grand Chamber missed the chance to elucidate once and for all an issue which has made the Court for a long time to challenge: whether the use of evidence obtained in breach of Article 8 of the Convention and used in criminal proceedings undermines the fairness of a trial as assured by Article 6'.[45]

Bykov v. Russia deals with covert operation of Federal Security Service of the Russian Federation (FSB) to obtain evidence that proves Bykov intended to murder 'S.'. In this case police instructs a third person (V.) to carry on hidden radio-transmitting device join the applicant in a guest-house where he was residing. After all, V. opened assassination discussion with the applicant, and pretended he himself conducted the crime. To persuade the applicant, V. showed him some evidence such as a watch belonging to S. Ending their chat, V. received a reward in cash as previously suggested by the applicant. In recourse of the applicant to the Court after passing over national procedural, the court recognized that conducting covert listening constitutes a breach under Article 8 of the Convention.[46] Nevertheless, this does not render the obtained evidence illegal in case to meet the requirements of Article 6 (1). Finally, the court in respect of non-pecuniary damages awards the applicant 1000 Euros (which was 118,089.25 lower than his request)[47]. Moreover, the court also found a breach of Article 5 (3) Convention due to excessively long pre-trial detention (20 months and 15 days).[48] Very alluring point of the judgment is where the court emphasizes on the up-hand position of Article 8 Convention in interpreting national laws.[49] The Court stated:

---

[43] See notes 33-37.
[44] *Bykov v. Russia* [GC], 10 March 2009, no. 4378/02, ECHR 2009.
[45] Ibid Concurring Opinion of Judge Cabral Baretto. Also see Concurring Opinion of Judge Kovler in the same case.
[46] Ibid, *Bykov v. Russia* (n 41) § 91
[47] Applicant claimed 4,059,061.80 Russian Roubles (119,089.25 euros) for both pecuniary and non-pecuniary damages. See Ibid, *Bykov v. Russia* (n 41) § 108
[48] Ibid, *Bykov v. Russia* (n 41) §67.
[49] Russian Government tried to legalize the covert surveillance by a literalism approach towards Article 8 of Operational-Search Activities Act of 12 August 1995(national legislation). The Article provides: 'Operational-search activities involving interference with the constitutional right to privacy of postal, telegraphic and other communications transmitted by means of wire or mail services, or with the privacy of the home'. Defendant, however argued that the means of their operation (radio-transmission) was neither wire or mail, therefore the action was legitimate, and even if it is covered by the said Act the 'gust-house' is not considered 'the home' in the article. On the contrary, the court observed the action contrary to law and

'The phrase 'in accordance with the law' must be interpreted with respect to the quality of law in associate with the compatibility to the rule of law. In addition, national law should clearly provide adequate indication for individuals the circumstances in which public agents might be entitled to take covert measures'.[50]

Alongside all the mentioned facts and two breaches of the Convention, the Court appraises the fairness of trial by highlighting following factors and finds no violation of Article 6(1) of the Convention:

'1) The applicant was free to receive V. 2) Not only he was free not talking to V. but also he himself was willing to do so because of his personal interest, 3) The Domestic court did not merely examine the transcript of the record, instead they have considered the expert view in order to assess the applicant's relationship with V. and the method in which he involved in the conversation.'[51]

Astonishingly, while the facts of the case clearly orient readers to 'third-party consent search' doctrine, the judgments avoid any illustrative examination in this regard. Whether, V. had a shared privacy in respect to his conversation with S. or the carried out action on behalf of the government would be flagged as illegal entrapment remained silent. [52]

2.2. What has been done so far?

To our knowledge, the issue has not yet been explored by ECtHR, and there is no benchmark guideline for the issue at hand. As mentioned earlier, the ECtHR still suffers from a lack of relevant cases, and no judicial opportunity has yet come to seize the matter, considering the issue in ample detail. Some legal systems, such as many states in the USA, have a solid background in judicial adjudications concerning violations of the 4th Amendment (unreasonable search and seizure).[53] Some countries have also granted wide discretion to courts in order to suppress illegally obtained evidence.[54] Nonetheless, the ECtHR tends to confine its authority to interfere in domestic procedures and does not overwhelm national prosecutory investigations owing to ill-privacy

found no sense in assessing further condition (values of democratic society) set out by Art. 8(2) Convention. See, Ibid, *Bykov v. Russia* (n 41) § 61-83.

[50] Ibid, (n 41) §§ 76 and 78.

[51] Ibid, (n 41) §§102 and 103.

[52] However, the issue of entrapment was addressed by Partly Dissenting Opinion of Judge Costa, Judge Spielmann joined by Judges Rozakis, Tulkens, Casadevall and Mijović.

[53] For instance, to see cases related to outside-warrant measurements: *United States v. Abbell* 963 F. Supp. 1178 (S.D. Fla. 1997); *United States v. Upham* 168 F.3d 532 (1st Cir. 1999) para536; *United States v. Carey* 172 F.3d 1268 (10th Cir. 1999); *United States v. Walser* 275 F.3d 981, 987 (10th Cir. 2001). Seemingly, there is a rapid growth in cases related to Amendment 4; to see the list of recent cases, turn to: R J. Hedges (Editor), 'Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials' (2022), <https://www.mass.gov/doc/electronic-evidence-in-criminal-investigations-and-actions-april-2022/download> accessed on 19 May 2024.

[54] Article 78(1) of the Police and Criminal Evidence Act 1984 grants courts the power to suppress any evidence if their entrance into the case would have such an adverse effect on the fairness of trial. For instance, in a case where a 19-year-old girl was accused of manslaughter, the appeal court quashed all the confessions of the accused. The court, however, justified this decision based on the granted discretion of Article 78 and due to the fact that the accused had been refused access to her lawyer in her first investigatory interview. Therefore, in the court's view, the lack of this right in her first interrogation had affected all subsequent decisions and confessions. See, R v McGovern 92 Cr. App. R 228 (App1991).

safeguards or infringements. It seems the Court cannot designate the tight relationship between Articles 6 and 8.

2.3. Defensible argument.

As seen in *Beuze v. Belgium* [55], the judgment laid down a non-exhaustive list comprising ten factors. However, the offered suggestion has three drawbacks, which hinder its effectiveness and future applicability. First and foremost, the provided guideline is not palpably measurable by the Court. The fifth assessment requires the Court to weigh the unlawfulness of the evidence-gathering processes and any violation of the Convention's provisions. However, how future judgments could evaluate the nature and weight of unlawful actions or the strength of some human rights over others is not clear. Secondly, the seventh factor of the test does not clarify whether the Court should suppress those illegally obtained evidence that forms the significant probative part of proofs or should allow them. Each will result in different outcomes; supposedly, if the only evidence of the claimant's conviction is found illegitimate during the Court's assessment, allowance and suppression represent dissimilar viewpoints upon fairness of a trial. If the sole evidence is the product of illegal government surveillance, suppression could in some scenarios undermine the public interest [56] and no reasonable person would likely agree on this hypothetical equilibrium wherein a society is endangered by a potent risk, but the Court rejects delivering justice because of a trivial outside-warrant action by a police officer. Not to mention that it is quite imaginable that the infringement of privacy might not be at all a matter of interest for the accused, but he wills to use his right in order to try his chance and dismiss the case. However, if there are several evidences in a case and the first piece of evidence was afforded in an illegitimate way, the second piece (correlated or irrelevant to the subject of the first) must be suppressed in order to protect the fundamental rights of the accused (in case there is no opposing interest from the public community). Moreover, the Court should distinguish between the two following orders in gathering supportive evidence: first, if legitimate-looking evidence stems from an illegitimate measurement or evidence which was itself a product of illegal action, all further evidence (no matter whether correlated to the first or not) must be disregarded by applying the exclusionary rule.

[55] See, *Beuze v. Belgium* (n 27) §150 (C).
[56] See Article 1 of the Convention. The weakness of the seventh factor relies on common understanding since people completely overlook the quantity of evidence where there is an immense threat to public interest, for example, in cases of severe crimes.

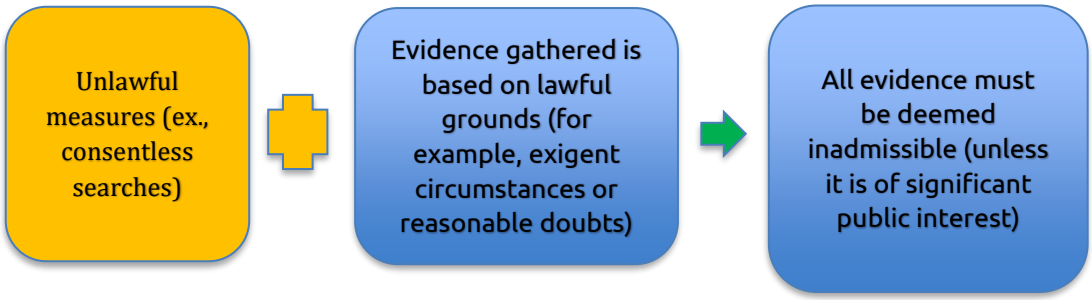


Figure A

For instance, a police officer, based on a consent provided by a premise owner, starts searching the consented areas; however, the officer goes further and searches other areas as well (such as the owner's laptop) and finally discovers digital evidence of a crime (related or irrelevant to the reason for the search). Since there was no consent to allow officers to search the landlord's laptop, the obtained evidence should be suppressed.[57] Even if the second evidence appears legitimate at first glance, the circumstances that gave rise to obtaining further evidence were due to the conduct of an unlawful measure. (see, Figure-A) on the other hand, if the chain of evidence started with legitimate discovery, and ended in illegitimate findings, the latter would not invalidate the earliest findings. (See, Figure B).[58]

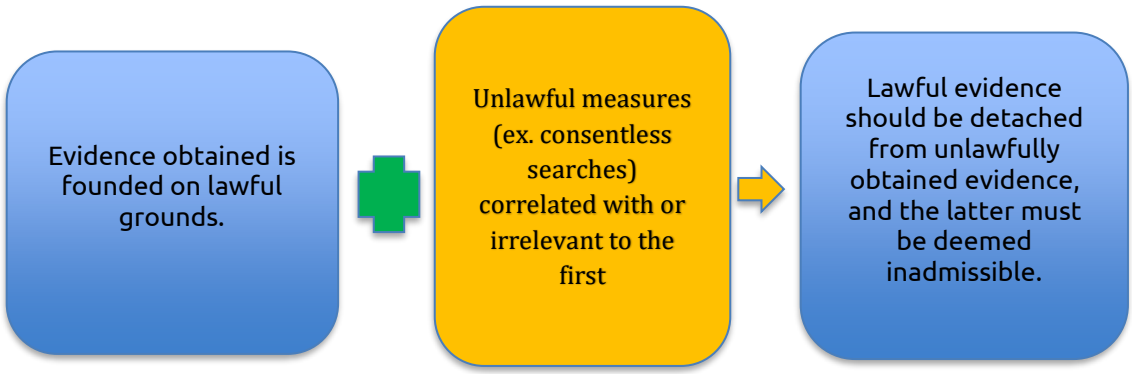


Figure B

[57] This example is inspired by a real case where a dweller of a premise (Turner) consented to two detectives searching his premise. The consent given was to help detectives find the person who assaulted Turner's neighbor (Mrs. Thomas). Nevertheless, Mr. Turner was not a suspect, but since his home was located next to Mrs. Thomas's, the detectives were concerned about the possibility that the intruder might have fled into Turner's apartments. In the middle of the investigation, while Turner was talking to one of the detectives downstairs, another detector started checking Turner's laptop and discovered many pieces of data related to child pornography. The court, however, called all evidences invalid based on the Fourth Amendment, and justified the ruling by remarking that Turner did not consent to the computer search and neither had the opportunity to object to the search. *United States V. Turner* 169 F. 3D 84, United States Court of Appeal, (1 Cir, 1999) para 87-89. Also see *United States v. Carey* 172 F.3d 1268 (10th Cir. 1999) para 1270-1272 wherein a detective had been appointed for drug investigation and tasked with discovering any related evidence of drug transactions through searching JPG files on the defendant's computer. However, he did not find any pertinent evidence; rather, he found 244 JPG files containing child pornography.

[58] This scenario is similar to a situation where an investigator has already found some legal evidence but further expands his search domain and extends the sphere of the warrant. For instance, if in the said scenario, the detective could have found some drug evidence and afterwards expanded his action regardless of the specifications of the warrant, this could be an example of when illegitimate actions follow legitimate ones.

Therefore, the proposed guideline in *Beuze v. Belgium* should be revised as follows in modification of the 7th test:

'7-The court must evaluate the probative weight of the evidence by determining whether the suppression of evidence would challenge the interests of society. However, if any afforded lawful evidence supports the illegal evidence, the court must orderly assess the correlation between them. If lawfully obtained evidence is the result of illegal evidence (or measurement), in case there is no significant interest of the public, the court should reject all evidence'.

Conclusion.

The perplexities in admissibility issues are often associated with the wide power of national jurisdictions in interpreting relevant legal provisions, which enhances the complexity of the riddle. In interpreting the GDPR or derived national standards, courts should consider that the said regulation does not develop any balance between inconsistent fundamental rights. Not to mention that striking a balance that links two or more fundamental rights is a backbreaking task to be carried out and often deemed to fail due to the lack of suitable gratification from legal practitioners and societies. This paper suggested that the ten-factor test addressed in the judgment of Beuze v. Belgium (2018) could serve as a yardstick for further national judgments as well as ECtHR future procedures. In the absence of any national law establishing a balance between the right to a fair trial and the right to protection of personal data (or the right to privacy as followed by the ECHR), member states of the European Union shall adhere to the aforementioned guideline of the Court. As a result of this adherence, not only an internal EU-level harmonization will be reached, but members will also, in the meantime, protect EU fundamental rights and comply with the spirit of the union's legislation, namely those enshrined in the Charter and other EU law principles. However, the paper further criticized some factors of the provided test, which it realized may expose a manifest injustice to the parties to a dispute. Finally, the paper modified the test in the judgment's seventh factor, as follows:

'The court must evaluate the probative weight of the evidence by determining whether the suppression of evidence would challenge the interests of society. However, if any afforded lawful evidence supports the illegal evidence, the court must orderly assess the correlation between them. If lawfully obtained evidence is the result of illegal evidence (or measurement), in case there is no significant interest of the public, the court should reject all evidence'.