CM2602

MEIJERS COMMITTEE COMMENT AND RECOMMENDATIONS ON THE EU DATA RETENTION ROADMAP

JANUARY 2026

This commentary outlines the Meijers Committee's concerns and recommendations regarding the Commission's Roadmap on lawful and effective access to data in anticipation of its proposal on data retention in the first quarter of 2026.

Should the Commission decide to propose legislation, in addition to the established parameters of the CJEU, the Meijers Committee wishes to emphasise the attention warranted by the privacy and data protection rights of individuals, the freedom of expression, cybersecurity and the rights of defence within any future frameworks. After careful consideration of the Commission's Roadmap for lawful and effective access to data for law enforcement and the conclusions and recommendations of the Higher Level Working Group ("HLG"), the Meijers Committee shall present its preliminary points of concern and corresponding recommendations herein.

Meijers Committee

Standing committee of experts on international immigration, refugee and criminal law

This commentary outlines the Meijers Committee's concerns and recommendations regarding the Commission's Roadmap on lawful and effective access to data in anticipation of its proposal on data retention in the first quarter of 2026.

Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks ("Data Retention Directive") was declared invalid due to its infringement of Art. 7, 8, 11 and 52 of the Charter of Fundamental Rights of the European Union ("CFREU") by the Court of Justice of the European Union ("CJEU") in the landmark judgement *Digital Rights Ireland*.[1]

The invalidity of the Data Retention Directive has left the regulation of data retention fragmented across the European Union, with divergent data retention regimes across the Member States. Member States enacted national data retention regimes based on Art. 15 (1) of the ePrivacy Directive, which allows for the restriction of the rights provided for by the Directive with the objective of the prevention, investigation, detection and prosecution of criminal offences.[2] The parameters of data retention for the objective of the prevention, investigation and prosecution of crime have been largely defined by the CJEU, which has produced a considerable volume of judgments on the issue.

Should the Commission decide to propose legislation, in addition to the established parameters of the CJEU, the Meijers Committee wishes to emphasise the attention warranted by the privacy and data protection rights of individuals, their cybersecurity and the rights of defence within any future frameworks. After careful consideration of the Commission's Roadmap for lawful and effective access to data for law enforcement and the conclusions and recommendations of the Higher Level Working Group ("HLG"), the Meijers Committee shall present its preliminary points of concern and corresponding recommendations below.

1. <u>The exploitation of the targeted retention exception</u>

The present section addresses the expansive interpretation of "targeted retention" in the Conclusions and Recommendations of the HLG. The CJEU has adopted a firm and consistent stance against the general and indiscriminate retention of data, with a small and restrictive number of exceptions.[3] One such exception are targeted retention regimes. This is data retention limited to a certain geographical area with a high instance of crime or a certain category of persons, such as persons previously convicted of serious crimes.[4] The Recommendations/Conclusions of the HLG and the Roadmap of the

[1] Joined Cases C-293/12 & 594/12 *Digital Rights Ireland* EU:C:2014:238.
[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002) OJ L 201/37, Art 15 .
[3] Joined Cases C-793/19 and C-794/19 *Spacenet* EU:C:2022:702, para 75.
[4] Case C-203/15 *Tele2Sverige* ECLI:EU:C:2016:970, 111. Eleni Kosta, 'The Evolution of the CJEU Case Law on Data Retention: Towards the Regulation of Access' in eds Eleni Kosta and Irene Kamara *Data Retention*

Commission apparently mean to utilise this mode of exception: repeatedly emphasising targeted interception.

Targeted retention is to be employed only in the combatting/prevention of *serious* crime, protection of public order and national security. The CJEU made targeted retention subject to several conditions including a causal link between the data retained and the objective pursued by targeted retention schemes, safeguards for individuals affected by the retention and its limitation to what is strictly necessary.[5] Moreover, in instances of geographical targeted retention, the competent authority must regularly update its targeting operation and the duration of targeted retention must not extend beyond what is necessary.[6] Overall, the Court has been eager to stress that this *exception* should not become the *rule*.[7]

The Meijers Committee strongly opposes the views of experts expressed in the Recommendations of the HLG that data retention regimes should only be 'targeted' by way of access, for example through the time limits for access to retained data, as this is contradictory to the limits set by the CJEU.[8] Additionally, the HLG's Conclusions reference the case of *La Quadrature du Net II* to claim that the CJEU's jurisprudence permits indiscriminate retention accompanied by strict access measures. This is an over-simplification and generalisation of reasoning which related to the retention of IP addresses in a highly stratified system for breaches of copyright.[9] Indeed the CJEU has introduced a number of robust protections applying to the access of retained data, including prior authorisation by an independent judicial authority, but they can by no means compensate for a lack of safeguards in the initial data retention.[10] This is supported by the stance of the European Court of Human Rights ("ECtHR") and the CJEU that the retention of personal data is itself an interference with the right to private life, regardless of conditions of access/usage that follow.[11]

Whilst the Meijers Committee advocates for adherence to the targeted retention limitations as established by the CJEU, it wishes to draw attention to discriminatory bias

---

in Europe and Beyond: Law and Policy in the Aftermath of an Invalidated Directive (Oxford University Press 2025), 24. Alena Birrer et al, 'The state is watching you- A cross-national comparison of data retention in Europe' (2023) 47 Telecommunciations Policy 1, 10.

[5] Case C-203/15 *Tele2Sverige* ECLI:EU:C:2016:970, 108-110.

[6] C-140/20 *Garda Síochána ,* 82. Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* EU:C:2020:791, para 151.

[7] Joined Cases C-793/19 and C-794/19 *Spacenet* EU:C:2021:939, Opinion of AG Sánchez-Bordona, para 50.

[8] Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, pg 8.

[9] Concluding report of the High-Level Group on access to data for effective law enforcement, 35.

[10] C-746/18 *HP v Prokuratuur* EU:C:2021:152, para 51. Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* EU:C:2020:791, para 158.

[11] *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECHR, 4 December 2008), para 67. *Amann v Switzerland* [GC] App No 27798/95 (ECHR, 16 February 2000), para 69. Opinion 1/15 on the Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, Opinion of the Court (Grand Chamber), 26 July 2017, para 124-125.

and/or stigmatisation which the targeting of certain geographical areas or persons may reinforce.[12] In relation to targeted persons, the selection of those individuals must be linked to a genuine, objective and identifiable connection to serious crime and as such may not be based (directly/indirectly) on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. The Commission should consider appropriate safeguards for the protection of Art 21 CFREU in its implementation of the CJEU's findings, including adequate independent oversight of the objectivity of these retention schemes.

Recommendations:

- The Meijers Committee strongly opposes the circumvention of targeted retention through reliance on targeted access and emphasises the necessity of an "end-to end" system of safeguards.
- The Meijers Committee raises concerns relating to the "objective" and non-discriminatory nature of targeted retention regimes. It recommends the introduction of review and monitoring processes which focus on issues of discrimination and profiling.

2. Duration of data retention

A particular issue of the previous Data Retention Directive was the retention periods set out therein, whereby all categories of data to be retained could be kept for a period of no less than six (6) months but no longer than two (2) years.[13] The Court criticised the absence of reference to objective criterion with which to determine the relevant retention period within those parameters.[14]

The HLG Conclusions acknowledge the current divergences between retention periods in various Member States, but only within the context of ensuring cross border cooperation when retrieving retained data.[15] The HLG has recommended the establishment of minimum retention periods based on the type of data, subscriber information, IP

[12] Gavin Robinson, "Targeted Retention of Communications Metadata: Future-proofing the Fight Against Serious Crime in Europe?" (2023) 8 (2) European Papers 713, 726-727. Vanessa Franssen en Catherine Van de Heyning, 'Belgium's New Data Retention Legislation: Third Time Lucky, or Three Strikes and You're Out?,' in E. Kosta en I. Kamara (red.), *'Data Retention in Europe and Beyond: Law and Policy in the Aftermath of an Invalidated Directive* (Oxford University Press 2025), 257. Alena Birrer et al, 'The state is watching you- A cross-national comparison of data retention in Europe' (2023) 47 Telecommunications Policy 1, 10.

[13] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (2005) OJL 105/54, Art 6.

[14] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland* EU:C:2014:238, para 64.

[15] Case C-817/19 *Ligue des droits humains ASBL v Conseil des Ministres* EU:C:2022:491, para 196.

addresses, traffic data and location data.[16] The Meijers Committee wishes to stress the importance of complementary technical and organisational measures, including accurate and robust data filtering and labelling with regular oversight. Moreover, the HLG does not reference maximum periods of retention, which are of paramount importance to the right to privacy, data protection and the presumption of innocence.

Recommendation:

- The Meijers Committee welcomes the introduction of objective factors in the determination of minimum periods of retention. However, it stresses that these considerations must be equally extended to maximum periods of retention and accompanied by accurate and robust technical and organisational measures.

3. <u>The issue of decryption and "lawful access by design":</u>

The Meijers Committee welcomes the European Commission's plans to explore viable options for accessing data alternative to decryption but retains considerable concerns about the HLG's proposal on "lawful access by design".[17] In short, this pertains to access to data for the purpose of preventing, investigating and prosecuting criminal activities and threats to public security.[18]

The exact manner in which this "lawful access by design" would operate has not been specified yet, however, given that the concept is positioned under the sub-heading "Ensuring that evidence can be read: decrypting data", the Meijers Committee infers that this lawful access may include the creation of backdoors, or processes such as client-side scanning, as associated with the Proposed Regulation laying down rules to prevent and combat child sexual abuse ("CSAR"). [19]

The Meijers Committee echoes the statement of the European Data Protection Board: that in addition to decryption, measures like access by client-side scanning, fundamentally undermine the privacy and cybersecurity objectives which encryption safeguards. [20] Indeed, there are several identifiable risks posed by the concept of "lawful access by design", namely to cybersecurity, privacy and the freedom of expression.

---

[16] Concluding report of the High-Level Group on access to data for effective law enforcement, 34-35.
[17] Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, Recommendation Cluster 10 pg 20.
[18] Commission, "Roadmap for lawful and effective access to data for law enforcement" (Communication) COM (2025) 349 final, 2.
[19] Commission, 'Proposal for a Regulation laying down rules to prevent and combat child sexual abuse' COM (2022) 209 final, Recital 26; Art 10 (1).
[20] Statement 5/2024 on the Recommendations of the High Level Group on Access to Data for Effective Law Enforcement https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf, Section 3.

Whilst the Commission has stated that the cybersecurity of systems is paramount in the context of lawful access, how this security will be maintained and verified remains obscure. In Recommendation 26 of the HLG, it is suggested that there should be built-in lawful access obligations, including the access to encrypted data, for digital devices.[21]

Information security commonly refers to the confidentiality, integrity and availability of data during communication.[22] The Meijers Committee is concerned that the cybersecurity of systems will be put in jeopardy by lawful access by design and that confidentiality will be compromised. Weakening the encryption of digital communication does not only allow access by law enforcement authorities to sensitive data but may leave vulnerabilities exposed to any number of other actors, including members of organised crime.[23] In a Joint Statement from Europol and ENISA, the institutions confirmed that decryption may "increase the attack surface for malicious abuse, which, consequently, would have much wider implications for society."[24]

In *Podchasov v Russia* the ECtHR found that national law mandating the decryption of end-to-end encryption (E2E) was considered a disproportionate interference with the right to private life (Art 8 ECHR) when pursuing the objectives of protecting national security or preventing disorder and crime.[25] The importance of private communication and/or encryption cannot be overstated for the protection of private life. Moreover, the HLG's proposal that providers of encrypted services must be obliged to "find the means" to provide data upon request from law enforcement is highly problematic.[26] This could lead to divergent approaches by service providers, without due regard or respect for the privacy rights of individuals.

Furthermore, access to encrypted information may have severe effects on the right to freedom of expression enshrined in Art 10 of the ECHR and Art 11 of the Charter, respectively. Access by the Member States to "private" communications of its citizens may have pronounced "chilling effect" on freedom of expression and access to this information may also be mobilised to supress discourse and dissent. [27] Encryption of

---

[21] Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, Recomendation 26.
[22] Ot L. Van Daalen, " The right to encryption: Privacy as preventing unlawful access" (2023) 49 Computer Law and Security Review 1, 2.
[23] Ot Van Daalen , "The Governance Landscape" in *From Encryption to Quantum Computing* (T.M.C. Asser Press 2025), 119; Bert- Jaap Koops & Eleni Kosta, "Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark""(2018) 34 Computer Law & Security Review 890, 897.
[24] Europol;ENISA, 'On lawful criminal investigation that respects 21st Century data protection' (20 May 2016) < https://www.enisa.europa.eu/sites/default/files/all_files/2016-05-25_On_lawful_criminal_investigation_respecting_21st_century_data_protection-Joint_Europol-ENISA_statement.pdf> .
[25] *Podchasov v Russia* App no 33696/19 (ECtHR, 13 February 2024), paras 65;79.
[26] Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement ,9.
[27] Case C-203/15 *Tele2Sverige* EU:C:2016:970, 82. Joined Cases C-793/19 and C-794/19 *Spacenet* EU:C:2022:702, 56. *Big Brother Watch and others v. The United Kingdom* Application no 58170/13,

communication is key to the "right to whisper", constructed as a corollary right enabling individuals to decide to whom they wish to express themselves. [28] In addition, the risk to freedom of expression is exacerbated where data retention and access regimes are coupled with criminal-related or security-based labelling. The increasing classification of activists or protest movements as potential public order or security threats may facilitate their inclusion within targeted retention or access schemes, thereby deterring lawful expression, assembly, and association through stigma and heightened surveillance.

Recommendation:

- In light of the grave danger decryption poses to the right to private life, data protection and freedom of expression, and in compliance with the jurisprudence of the ECtHR, the Meijers Committee completely opposes the introduction of a regime mandating or permitting on a voluntary basis the decryption of communications or alternative processes with similar effects.

4. The rights of defence and evidence

In amongst this extended discussion of the regulation of data retention, it is important not to lose sight of the purposes of data retention and the role of data in the prosecution of crime. The Roadmap and Conclusions/Recommendations of the HLG show little consideration for the impact of data retention regimes on the rights of the defence and the role of retained data as evidence.

The Commission's Roadmap and the Conclusions/Recommendations champion the use of decryption in criminal investigations, pointing to national efforts such as the EncroChat operation. In addition to the concerns highlighted in the above section, the use of decrypted data as evidence in criminal trials has garnered severe criticism across the Member States.[29]

The adversarial principle entails the ability of the individual concerned to examine all documents and observations submitted the court for the purpose of influencing its decision and to have the opportunity to comment on them.[30] It forms a fundamental part of the right to a fair trial both under Art 47 of the Charter and Art 6 ECHR.[31]

62322/14 and 24960/15 (ECHR, 25 May 2021) Joint Partly Concurring Opinion of Judges Lemmens Vehabović and Bošnjak, para 6-8.

[28] Lex Gill, 'Law, Metaphor and the Encrypted Machine' (2018) 55 (2) Osgood Hall Law Journal 440, 472. Concept coined by the LEAP Encryption Access Project.

[29] Vanja Bajović & Vesna Ćorić, "Encrochat and Sky ecc Data as Evidence in Criminal Proceedings in Light of the CJEU Decision" (2025) European Journal of Crime Criminal Law and Criminal Justice 235, 248.

[30] Case C- 300/11 *ZZ v Secretary of State Home Department* EU:C:2013:363 para 55.

[31] Case C-746/16 *HP v Prokuratuur* EU:C:2021:152, 43. *Ruiz-Mateos v. Spain* App no. 12952/87 (ECHR,23 June 1993), para 63.

Whilst the CJEU acknowledges that the admissibility of evidence is a matter of national law, the relevant rules must nonetheless align with the principle of effectiveness: the exercise of rights under EU law should not be rendered impossible.[32] Whilst admission standards primarily remain a matter of national law, the ECtHR's jurisprudence on the *fairness* of criminal trials in light of the unlawful interception of evidence should be born in mind: particularly, the need for additional corroborating evidence.[33]

A fortiori, the CJEU held that data obtained during unlawful general and indiscriminate data retention, must be excluded as evidence where the accused/defence does not have the ability to "effectively comment" on it, where the judge lacks the requisite knowledge of the field and where the data is likely to have a preponderant influence on the case.[34] In *MN*, this reasoning was extended to the issuance of European Investigative Orders, in the context of the sharing of decrypted data from the Encrochat Operation between the French and German Authorities.[35] The refusal by authorities to disclose key information on the functioning of Encrochat justified by "defence security" caused considerable issues in the ability of the defence to scrutinise the evidence for its lawfulness, reliability and accuracy.[36] Whilst the non-disclosure of evidence may be justified by the authorities, particularly in light of security concerns or the personal data of other persons contained in those datasets, the restriction of the rights of the defence must be strictly necessary and adequately counterbalanced.[37] This may include the involvement of the defence in the filtering of large datasets.[38]

The Meijers Committee wishes to highlight the importance of incorporating and developing the CJEU/ECtHR's safeguards further in the Commission's proposal. The ambiguity of the concept of an "effective comment" within the CJEU jurisprudence is a point of concern for the Meijers Committee as its restrictive interpretation may undermine the adversarial principle, and consequently, the right to a fair trial.

---

[32] Joined Cases C-339/20 & C-397/20 *VD;SR* EU:C:2022:703, para *105*.
[33] *Schenk v Switzerland* App no 10862/84 (ECHR, 12 July 1988), para 48.
[34] Case C-746/16 *HP v Prokuratuur* EU:C:2021:152, para 55. Joined Cases C-339/20 & C-397/20 *VD;SR* EU:C:2022:703 ,para 106. C-670/22 *MN* EU:C:2024:372, para 105. Adam Juszczak and Elisa Sason, "Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?" (2021) 4 EUcrim 238, 251.
[35] C-670/22 *MN* EU:C:2024:372, para 105. JJ Oerlemans & D.A.G. van Toor, "Legal aspects of the EncroChat Operation: A Human Rights Perspective"(2022) 30 European Journal of Crime, Criminal Law and Criminal Justice 309, 315. Vanja Bajović & Vesna Ćorić, "Encrochat and Sky ecc Data as Evidence in Criminal Proceedings in Light of the CJEU Decision" (2025) European Journal of Crime Criminal Law and Criminal Justice 33 (2025) 235, 253.
[36] Radina Stoykova, "Encrochat: The Hacker with a warrant and fair trials?" (2023) 46 Forensic Science International: Digital Investigation 1, 7.
[37] Van Mechelen and Others v the Netherlands App. nos. 21363/93, 21364/93, 21427/93 and 22056/93 (ECtHR 12 April 1997), para. 58. Rowe and Davis v. The United Kingdom App. 28901/95 (ECtHR, 16 February 2000), para. 61.
[38] *Sigurður Einarsson and Others v. Iceland* App no. 39757/15 (ECHR, 4 June 2019), para 90.

Recommendation:

- In the view of the Meijers Committee, the ability to comment effectively should include at a minimum: meaningful information on the method of intercepting the data, the involvement of the defence in the filtering of the intercepted data, data provided in a readable format and the possibility of analysis and observations by a digital forensic expert.

5. The use of Artificial Intelligence in Data Processing:

The Meijers Committee further draws attention to the Roadmap's projections on retained data should be further processed. The Commission advocates for the use of Artificial Intelligence (AI) to perform tasks such as "data filtering, correlating evidence from massive amounts of data...getting access to encrypted data ...and forensic analysis".[39] The Commission states that AI applications used for these purposes should be "accurate, transparent" and in full compliance with the Regulation laying down harmonised rules on artificial intelligence ('The AI Act') and the data protection and privacy legal frameworks.[40] However, in spite of this assurance of compliance, the framing of the AI applications in the Roadmap raises several issues under the EU's AI Act.[41]

Firstly, the involvement of AI applications in the processing of evidence may include tasks such as "correlating evidence" and "forensic analysis" according to the Roadmap. Whilst these tasks do not exactly correspond to the notion of an AI system "evaluating the reliability of evidence" classified as a high-risk AI system under Annex III Art 6 (c) of the AI Act, the use of AI to extract the "relevant" data from the datasets will inevitably prejudice the further evaluation of evidence by law enforcement authorities. In the absence of human oversight, the correlations drawn from the datasets may be inaccurate, incomplete and biased.

Secondly, the Commission's proposal for investment in AI applications to identify investigative leads from large amounts of data could (depending on its manifestation), fall within the prohibited practice found in Annex III Art 5 (d) AI Act, which involves the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a crime based on profiling or otherwise

[39] Commission, "Roadmap for lawful and effective access to data for law enforcement" (Communication) COM (2025) 349 final, 13.
[40] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L2024/1689. Commission, "Roadmap for lawful and effective access to data for law enforcement" (Communication) COM (2025) 349 final, 13.
[41] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (2024) OJ L 2024/1689.

assessment of their personality traits and characteristics. Alternatively, it could fall within the category of high-risk applications employed by law enforcement authorities for assessing the risk of offending/re-offending, not solely on the basis of profiling of natural persons.[42] This distinction is dependent on the data and corresponding algorithm in use. The extremely large amounts of non-content data indicated for retention and the corresponding task of identifying "investigative leads" could lead to the "prediction" of certain individuals committing criminal offences.

Thirdly, the Commission's suggestion that AI applications be used to "get access to encrypted data" has not been addressed at present under the AI Act or Law Enforcement Directive. Hence, further clarification is needed from the Commission on the compliance of such AI applications with EU law.

On a fundamental level, automated analysis of data containing precise information about the private life of individuals and its compatibility with Art 7 and 8 of the Charter will depend on their pre-determined models and criteria and on the databases used for processing.[43] The Court expressly precluded the use of AI as constituting pre-determined criteria, due to its adaptive nature which may change the assessment criteria and weighting of the criteria. [44] Drawing on the Court's reasoning laid down in *La Quadrature du Net*, any automated processing should be non-discriminatory, reviewed regularly, and should be accompanied by oversight and verification by non-automated means.[45]

Finally, such use of mass pre-emptive data surveillance would negatively affect the presumption of innocence, which flows from Article 48(1) of the Charter, as it can be interpreted as viewing large groups of individuals as 'suspect', regardless of whether there is a reasonable suspicion against them.[46] Moreover, when eventually used in a criminal process, it risks shifting the burden of proof (an important aspect of the presumption of innocence) to the individual.

Recommendations:

- The Meijers Committee recommends that the use of Artificial Intelligence in filtering and correlating evidence from datasets should be critically examined due

[42] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (2024) OJ L 2024/1689, Annex III 6 (d).
[43] Case C-817/19 *Ligue des droits humains ASBL v Conseil des Ministres* EU:C:2022:491, para 103.
[44] ibid, 194.
[45] ibid, 124. Joined Cases C511/18, C512/18 and C520/18 *La Quadrature du Net and Others* EU:C:2020:791, para 172. Sarah Eskens, "The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of La Quadrature du Net and others and Privacy International"(2022) 8 (1) Data Protection Law Review 143, 151.
[46] Julia Wojnowska-Radzinska Implications of Pre-emptive Data Surveillance for Fundamental Rights in the European Union, 2023, Brill/Nijhoff, par. 5.4; Antonella Galetta, 'The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?' (2013) European Journal of Law and Technology, Vol. 4, No. 2; Jonida Milaj, Jeanne Pia Mifsud Bonnici, 'Unwitting subjects of surveillance and the presumption of innocence' (2014) Computer Law & Security Review 30.

to its potential non-compliance with the AI Act, Art 6 ECHR, Art 48 Charter and Art 21 Charter and CJEU case law.

- The Meijers Committee recommends that any automated processing by way of AI must be subject to oversight and verification by non-automated means.
- The Meijers Committee requests that the Commission explain its proposal to use AI to "get access to encrypted data" and to demonstrate its compliance with EU law and the jurisprudence of the CJEU/ECtHR.

Conclusion:

Whilst the Meijers Committee appreciates the importance of data retention in effective law enforcement, it stresses the need for careful attention to be paid to extensive and interconnected EU fundamental rights such as the right to privacy, data protection, cybersecurity, freedom of expression, right to non-discrimination and the rights of the defence in future frameworks. An approach emphasising efficiency and effectiveness in data retention should not come at the expense of safeguards afforded to individuals. In light of the current information available on the Commission's Roadmap on lawful and effective access to data, the Meijers Committee offers the following recommendations for any future proposals:

1. The Meijers Committee strongly opposes the circumvention of targeted retention through reliance on targeted access and emphasises the necessity of an "end-to end" system of safeguards.
2. The Meijers Committee raises concerns relating to the "objective" and non-discriminatory nature of targeted retention regimes. It recommends the introduction of review and monitoring processes which focus on issues of discrimination and profiling.
3. The Meijers Committee welcomes the introduction of objective factors in the determination of minimum periods of retention. However, it stresses that these considerations must be equally extended to maximum periods of retention and accompanied by accurate and robust technical and organisational measures.
4. In light of the grave danger decryption poses to the right to private life, data protection and freedom of expression, and in compliance with the jurisprudence of the ECtHR, the Meijers Committee completely opposes the introduction of a regime mandating or permitting on a voluntary basis the decryption of communications or alternative processes with similar effects.
5. The rights of defence should be central to and robustly safeguarded within proposed data retention frameworks. In the view of the Meijers Committee, the ability to comment effectively as part of the adversarial principle should include at a minimum: meaningful information on the method of intercepting the data, the involvement of the defence in the filtering of the intercepted data, data provided in

a readable format and the possibility of analysis and observations by a digital forensic expert.

6. The Meijers Committee recommends that the use of Artificial Intelligence in filtering and correlating evidence from datasets should be critically examined due to its potential non-compliance with the AI Act, Art 6 ECHR, Art 48 Charter and Art 21 Charter and CJEU case law.
7. The Meijers Committee recommends that any automated processing by way of AI must be subject to oversight and verification by non-automated means.
8. The Meijers Committee requests that the Commission explain its proposal to use AI to "get access to encrypted data" and to demonstrate its compliance with EU law and the jurisprudence of the CJEU/ECtHR.