Council of the European Union

Brussels, 22 May 2024
(OR. en)

9990/24

LIMITE

COSI 89
CRIMORG 78
ENFOPOL 248
IXIM 141
CT 61
CATS 43
CYBER 171
TELECOM 188
DATAPROTECT 213
COPEN 262
JAI 843

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	15043/23
Subject:	Digital files - state of play

Delegations will find in Annex 1 an overview of legislative files (either under negotiation or in implementation) that are dealt with outside JHA but have an internal security dimension. The purpose of this overview is to keep delegations updated about relevant legislative developments outside JHA.

Annex 2 contains a list of legislative files handled within JHA.

ANNEX 1

Legislative files with internal security relevance that are dealt with outside JHA

1. Artificial Intelligence (AI) Act

The proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) was submitted by the Commission on 21 April 2021. It was handled in the Working Party on Telecommunications and Information Society (WP TELECOM).

The Artificial Intelligence Act was adopted by the Council on 21 May 2024. One of the objectives of the Regulation is to ensure that AI systems placed or put into service on the Union market and used in the Union are safe and respect existing law on fundamental rights and Union values.

Relying on a risk-based approach, the Regulation sets out different obligations and requirements in particular for "high-risk AI systems". The use cases falling into the category of stand-alone high-risk AI systems are listed in Annex III of the Regulation. For the purpose of this document, three areas referred to in Annex III are particularly relevant: "biometrics, in so far as their use is permitted under relevant Union or national law" (point 1), "law enforcement in so far as their use is permitted under relevant Union or national law" (point 6) and "migration, asylum and border control management, in so far as their use is permitted under relevant Union or national law" (point 7).

Obligations and requirements for high-risk AI systems include, for example, a risk management system to be implemented throughout the lifecycle of the system, safeguards related to data sets, automatic recording of events ("logs"), information to users and transparency obligations, and human oversight. High-risk AI systems will also need to go through a conformity assessment procedure before they are placed on the market or put into service. Prior to deploying a high-risk AI system, the performance of a fundamental rights impact assessment is required for deployers that are bodies governed by public law, private actors providing public services and deployers that are deployers of high-risk AI systems listed in point 5 (b) and (c) of Annex III (Article 27).

Additional obligations have been introduced regarding the use of post-remote biometric identification by law enforcement authorities notably an authorisation, *ex ante* or *ex post* within 48 hours after the use, from a judicial or an administrative authority (Article 26 (10)).

In addition, the Regulation lists some prohibited AI systems such as real-time biometric identification for law enforcement in publicly accessible spaces (Article 5 (h)), which might only be used in limited and clearly defined exceptions and submitted to additional safeguards. Such safeguards include notably the need to obtain a prior authorisation by a judicial authority or an independent administrative authority. Additional monitoring and oversight measures as well as reporting obligations at EU level are also included. Other prohibited AI systems have been added to the list, such as "biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation certain characteristics", "systems for making risk assessments of natural persons in order to assess or predict the risk of a natural person to commit a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics" and "systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage"

Market surveillance authorities will play an important role in the implementation of the future Regulation. For example, when such authorities would have sufficient reasons to consider that an AI system presents a risk to the fundamental rights of a person, it would have to carry out an evaluation of that system to assess its compliance with the obligations and requirements laid down in the Regulation. They might also have to act upon a complaint made by a legal or natural person. For high-risk AI systems related to law enforcement, the market surveillance authority would either be the data protection authorities, or any other authorities designated pursuant to conditions laid down in Article 1 to 44 of Directive 2016/680 (data protection in the sector of prevention, investigation, detection, or prosecution of criminal offences, often called the "Law Enforcement Directive").

The Regulation will apply, for most parts, 24 months after the entry into force, except for the prohibited AI practices for which it will be after 6 months and 12 months for provisions concerning notifying authorities and notified bodies, governance, general purpose AI models, confidentiality, and penalties.

2. ePrivacy and lawful access to electronic evidence, including data retention

The proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (proposal for an ePrivacy Regulation) was published on 10 January 2017.

The Regulation will replace Directive 2002/58/EC (ePrivacy Directive) and specify the General Data Protection Regulation (GDPR). The objective is to reinforce trust in and the security and confidentiality of communications in the Digital Single Market (including content and metadata, e.g. sender, time and location of a communication), while providing flexible regulatory tools to enable innovation, defining clearer rules on tracking technologies such as cookies (including more user-friendly ways for users to express consent) and on spam. It applies to both natural and legal persons and also includes in its scope market players using the internet (e.g. 'over-the-top communication services', such as instant messaging apps and web-based email services), with the aim of ensuring a level playing field for companies.

The file is being negotiated in the Working Party on Telecommunications and Information Society (WP TELECOM). On 10 February 2021, Coreper adopted a negotiating mandate on this legislative proposal. As far as JHA is concerned, the Council mandate includes important access to electronic evidence and data retention aspects (Article 2(2)(d) - scope; Article 6(1)(d) - opening for data processing for law enforcement and public security purposes; Article 7(4) - explicit provision on data retention; Article 11 - exceptions to the obligations and rights provided for in the instrument).

Since May 2021, the Parliament and the Council have been discussing the proposal at technical level. No compromise between the Parliament and the Council has been found so far.

3. Data Act[1]

The Commission submitted the proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) on 23 February 2022. The Data Act entered into force on 11 January 2024 and will become applicable in September 2025.

The new rules enable users of connected products to access the data generated by these devices, and to share such data with third parties. Public sector bodies will be able to access and use data held by the private sector to help respond to public emergencies such as floods and wildfires, or when implementing a legal mandate where the required data is not readily available through other means. The Data Act also includes safeguards against unlawful requests by third-country authorities to transfer or access non-personal data held in the EU, ensuring a more reliable and secure data-processing environment. Finally, the Data Act introduces measures to promote the development of interoperability standards for data-sharing and for data processing services, in line with the EU standardisation strategy.

In Article 1(6) of the Data Act it is made clear that this Regulation does not affect Union or national legal acts providing for the sharing of, access to and the use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the execution of criminal penalties, or for customs and taxation purposes, or international cooperation in that area. This Regulation does not affect the competences of the Member States concerning public security, defence or national security, or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and the maintenance of law and order.

[1] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)

4. European Digital Identity (revision of the eIDAS Regulation)[2]

The Commission submitted the proposal for a Regulation establishing a framework for a European Digital Identity (European eID) on 3 June 2021. The initiative amends the eIDAS Regulation from 2014, which laid the necessary foundations for safely accessing services and carrying out transactions online and across borders in the EU.

In the Council, the examination of the proposal was carried out in the Working Party on Telecommunications and Information Society (WP TELECOM). The revised regulation was published in the Official Journal on 11 April 2024, entered into force on 1 May 2024 and will be fully implemented by 2026.

Under this Regulation, Member States will provide citizens and businesses with digital wallets that will link their national digital identities with proof of other personal attributes (e.g. driving licence, diplomas, bank account). Citizens will be able to prove their identity and share electronic documents from their digital wallets. These new European digital identity wallets will also enable all Europeans to access online services with their national digital identification, which will be recognised throughout Europe, without having to use private identification methods or having to share unnecessary personal data. In addition to public services, very large online platforms designated under the Digital Services Act and private services that are legally required to authenticate their users will have to accept the EU digital identity wallet for logging into their online services.

[2] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

5. European Media Freedom Act (EMFA)[3]

The proposal for Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act, EMFA) and amending Directive 2010/13/EU was submitted by the Commission on 16 September 2022. It was handled in the Audiovisual and Media Working Party. The EMFA was published in the Official Journal on 17 April 2024 and entered into force on 7 May 2024.

On the substance, the EMFA Regulation, based on Article 114 TFEU (approximation of laws for the achievement of the internal market objectives), aims at establishing a common framework for media services in the internal market. It builds on the 2018 Audiovisual and Media Services Directive (AVMSD) and amends certain provisions of this directive. The EMFA covers complex and sensitive areas with links to other policy areas such as Rule of Law and Justice and Home Affairs, and it is the first time that the EU aims at legislating in the fields of media freedom, media pluralism and editorial independence.

The first part of the Regulation contains safeguards for and duties of media service providers. In particular, Article 4 of the Regulation deals with the rights of media service providers, including the protection of the confidentiality of journalistic sources. This Article is particularly relevant for the law enforcement sector, as it contains limitations to the detention, sanction, interception and inspection of media service providers, editorial staff or persons with regular or professional relationship with them who might have information related to or capable of identifying journalistic sources or confidential communications. It also contains specific provisions applicable to the deployment of intrusive surveillance software on devices used by media service providers, editorial staff or persons with regular or professional relationship with them.

[3] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).

The detention, sanction, interception, and inspection of media service providers, editorial staff or persons with regular or professional relationship with them are prohibited unless the following cumulative conditions are provided: i) it is provided for by national law or Union law; (ii) it is in compliance with Article 52(1) of the Charter and other Union law; (iii) it is justified on a case-by-case basis by an overriding reason of public interest and is proportionate; and (iv) it is subject to prior authorisation by a judicial authority or an independent and impartial decision-making authority or, in duly justified exceptional and urgent cases, is subsequently authorised by such authority without undue delay. In addition, the deployment of intrusive surveillance software can only be carried out for the purposes of investigations of one of the aforementioned persons for offences referred to in Article 2(2) of Council Framework Decision 2002/584/JHA (European Arrest Warrant) punishable in the Member State concerned by a custodial sentence or a detention order of a maximum period of at least three years or for other serious crimes punishable in the Member State concerned by a custodial sentence or a detention order of a maximum period of at least five years, as determined by the law of that Member State. Furthermore, such surveillance measures or the deployment of intrusive surveillance software must be regularly reviewed by a judicial authority or an independent and impartial decision-making authority in order to determine if the conditions are still met.

The EMFA Regulation shall apply, for most parts, from 8 August 2025. In particular, Articles 4(1) and (2) shall apply from 8 February 2025.

6. Digital Services Act (DSA)[4]

Following the entry into force of the DSA on 16 November 2022, all platforms had to publish the number of monthly users by 17 February 2023, and this must now be updated every six months.

Based on the information received, on 25 April 2023 the Commission made the first decisions as to designating 19 entities as a very large online platform (VLOP) or very large online search engine (VLOSE). Following the designation decisions by the Commission, the entities in question had until the end of August to comply with the obligations under the DSA, including carrying out the first annual risk assessment exercise. On 20 December 2023, the Commission designated 3 additional platforms as VLOPs.

To allow for the supervision and enforcement of the DSA, Member States had to designate their digital services coordinators (DSCs) by 17 February 2024, the general date of entry into application of the DSA. DSCs can request access to VLOPs' and VLOSEs' data, order inspections and impose fines in the event of an infringement. They are responsible for certifying 'trusted flaggers' and out-of-court dispute settlement bodies.

On 20 October 2023, the Commission published a Recommendation for Member States to coordinate their response to the spread and amplification of illegal content, such as terrorist content or unlawful hate speech, before it can lead to a serious threat to public security. The aim was for Member States to support the Commission in ensuring full compliance by VLOPs and VLOSEs with their new obligations under the DSA, ahead of the deadline for Member States to play their role in the enforcement of the DSA. With the Recommendation, the Commission was encouraging Member States to designate an independent authority to be part of a network of prospective DSCs, ahead of the legal deadline. The Recommendation also recalls powers to tackle illegal content conferred on Member States by various EU legal instruments, such as the Regulation on addressing the dissemination of terrorist content online (TCO), in force since June 2022.

---

[4] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

Legislative files handled within JHA

1. JHA digital files under negotiation

File	State of play
Regulation laying down rules to prevent and combat child sexual abuse	No Council position yet
Regulation laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679	No Council position yet
Regulation on the collection and transfer of advance passenger information (API) for the prevention, detection, investigation and prosecution of terrorist offences and serious crime	First reading agreement, awaiting formal adoption following lawyer linguist scrutiny
Regulation on cybersecurity requirements for products with digital elements (Cyber Resilience Act)	First reading agreement, awaiting formal adoption following lawyer linguist scrutiny
Regulation amending Regulation (EU) 2019/881 as regards managed security services (Cybersecurity Act)	First reading agreement, awaiting formal adoption following lawyer linguist scrutiny
Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (Cyber Solidarity Act)	First reading agreement, awaiting formal adoption following lawyer linguist scrutiny

2. JHA digital files in implementation

Adopted legislative act	State of implementation
Regulation (EU) 2017/2226 of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011	EES is expected to be in operation in 2024
Regulation (EU) 2018/1240 of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226	ETIAS is expected to be in operation in 2025
Regulation (EU) 2019/816 of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726	ECRIS-TCN is expected to be in operation in 2025
Regulation (EU) 2019/817 of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 and Council Decisions 2004/512/EC and 2008/633/JHA	2024: European Search Portal (ESP) 2025: Common Identity Repository (CIR), Shared Biometric Matching Service (sBMS) 2026: Multiple Identity Detector (MID)
Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online (TCO Regulation)	The TCO Regulation has applied since 7 June 2022
Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)	By 17 October 2024, Member States must adopt and publish the measures necessary to comply.

Adopted legislative act	State of implementation
Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (e-evidence)	The e-evidence Regulation will apply from 18 August 2026.
Regulation (EU) 2023/2844 of the European Parliament and of the Council of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation	The Regulation will apply from 1 May 2025.
Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation)	In force. By 26 April 2025, eu-LISA has to report for the first time about the development of the router, and Europol about the development of EPRIS.
Regulation (EU) 2024/1307 of the European Parliament and of the Council of 29 April 2024 amending Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse	In force until 3 April 2026.