Council of the European Union

Brussels, 16 November 2023
(OR. en)

15043/23

LIMITE

COSI 221
CRIMORG 185
ENFOPOL 489
IXIM 213
CT 180
CATS 67
CYBER 291
TELECOM 336
DATAPROTECT 310
COPEN 395
JAI 1482

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	8875/23
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 is being handled in the Working Party on Telecommunications and Information Society (WP TELECOM).

The Council reached a general approach on the proposal on 6 December 2022[1]. Trilogues took place on 14 June, 18 July, 2 and 3 October and 24 October 2023. The objective is to reach an agreement with the Parliament by the end of the year. The negotiations are intense given the complexity, importance and sensitivity of the instrument.

One of the objectives of the proposal is to ensure that AI systems placed on the EU market and used in the EU are safe and respect fundamental rights and EU values. Relying on a risk-based approach, the proposal sets out various obligations and requirements, in particular for high-risk AI systems. The use cases falling into this category are listed in Annex III to the proposal and include biometrics (point 1), law enforcement (point 6) and migration, asylum and border control management (point 7). The obligations and requirements for such 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. Several exemptions are provided for law enforcement authorities throughout the proposal, for example as regards human oversight and the 'four eyes principle' (Article 14), to accommodate confidentiality and operational needs. The extent of those exemptions and possible additional safeguards are currently under discussion.

[1] 14954/22.

The proposal also lists in Article 5 some AI systems, such as real-time biometric identification for law enforcement in publicly accessible spaces, which are either prohibited or may only be used exceptionally and under certain conditions. The Parliament added to the list of prohibited use cases AI systems used for predictive policing, systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage, systems used to infer emotions of a natural person in the areas of law enforcement and border management, and biometric categorisation systems that categorise natural persons according to sensitive or protected attributes.

The Council's general approach provides for the explicit exclusion of use of AI systems for military, defence or national security purposes from the scope of the Regulation. The Council's position also explicitly states that the use of AI systems for military, defence or national security purposes is excluded regardless of the type of entity carrying out activities for the excluded purposes. The Parliament did not provide for the exclusion of national security in its position.

Issues related to national security, prohibited use cases, possible exceptions and other provisions related to law enforcement access and use of certain AI systems will be discussed at the upcoming trilogue on 6 December 2023.

2. Data Act

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 Council's mandate for negotiations with the European Parliament was confirmed in Coreper on 22 March 2023 and a first trilogue took place on 29 March 2023. Political agreement at first reading was reached on 28 June 2023, and was formally approved by the European Parliament on 9 November 2023. Once the Council also approves the text in the coming days, the Regulation will be adopted, will enter into force on the 20th day following its publication in the Official Journal and will become applicable 20 months after the entry into force.

The concerns pertaining to the JHA community are mostly addressed in Article 1(4) of the Council's mandate. While the Commission proposal states that the Regulation will not affect legal acts in the area of prevention, investigation, detection or prosecution of criminal offences, or in the area of defence and national and public security, the Council's mandate adds that voluntary arrangements for the exchange of data between private and public entities are also unaffected by the Regulation. Article 27 provides for rules on the prevention of unlawful intergovernmental access and sets out a framework for the provision of data to countries with which there are specific arrangements in place.

3. European Digital Identity (revision of the eIDAS Regulation)

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. The revised Regulation aims to ensure universal access for people and businesses to secure trustworthy electronic identification and authentication by means of a digital wallet.

In the Council, the examination of the proposal was carried out in the Working Party on Telecommunications and Information Society (WP TELECOM). On 6 December 2022, the Council adopted its general approach regarding the framework for a European Digital Identity.
The Parliament adopted its position on 16 March 2023, and the negotiations started thereafter.

Further to the general approach reached under the Czech Presidency in December 2022, the Swedish Presidency held negotiations with the Parliament on 21 March, 23 May and 28 June 2023. After obtaining a further Coreper mandate on 27 October 2023, the Spanish Presidency held a fourth and final trilogue on 8 November 2023, successfully concluding the negotiations.

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.

4. 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.

5. Media Freedom Act

On 16 September 2022, the Commission presented a proposal for a Regulation establishing a common framework for media services in the internal market (European Media Freedom Act, EMFA). The aim of the proposal is to improve the internal media market. From a law enforcement perspective, the proposal defines the concept of 'serious crimes' by reference to some of the criminal offences listed in Article 2(2) of Council Framework Decision 2002/584/JHA. In addition, Article 4(2)(c) provides for a prohibition on deploying spyware in any device used by media service providers, unless certain conditions are met (e.g. justified on grounds of national security or in the case of serious crimes investigations).

In the Council, the negotiations are taking place in the Audiovisual and Media Working Party (AVMWP). While the leading Parliament Committee is CULT, LIBE has exclusive competence on Articles 4(2) and 20(3).

The first trilogue with the Parliament was held on 19 October 2023. Two further trilogues will take place on 29 November and 15 December, where Article 4 will be discussed. The Presidency aims to reach a political deal on 15 December 2023.

The co-legislators aim to conclude a first reading agreement before the next European Parliament elections.

6. Digital Services Act (DSA)[2]

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 whether entities are to be designated 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.

To allow for the supervision and enforcement of the DSA, Member States have 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 will be responsible for certifying 'trusted flaggers' and out-of-court dispute settlement bodies.

On 20 October 2023, the Commission published a Recommendation[3] 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 is 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 is encouraging Member States to designate already now 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.

---

2 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), (OJ L 277, 27.10.2022, p. 1).

3 Commission Recommendation of 20.10.2023 on coordinating responses to incidents in particular arising from the dissemination of illegal content, ahead of the full entry into application of Regulation (EU) 2022/2065 (the 'Digital Services Act'), C(2023) 7170 final.

ANNEX 2

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 on automated data exchange for police cooperation ('Prüm II'), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818	Trilogue phase
Regulation on the collection and transfer of advance passenger information (API) for the prevention, detection, investigation and prosecution of terrorist offences and serious crime	Awaiting EP position (expected December 2023)
Regulation laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679	No Council position yet
Regulation 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	Negotiations have been concluded, awaiting final approval by EP
Regulation on cybersecurity requirements for products with digital elements (Cyber Resilience Act)	Trilogue phase
Regulation amending Regulation (EU) 2019/881 as regards managed security services (Cybersecurity Act)	Coreper mandate for negotiations was approved on 15 November 2023
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)	No Council position yet

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	Entry into operation: 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
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