Council of European National Top-Level Domain Registries

Brussels, Belgium
23 June 2020

CENTR Board statement on the Inception Impact Assessment on the Europol Regulation

Introduction

CENTR is submitting the following feedback on the Inception Impact Assessment on the Europol Regulation (hereinafter the 'Inception Impact Assessment') that aims to revise the mandate of Europol, the agency that supports the cooperation between law enforcement authorities in EU member countries (hereinafter 'the Agency').

CENTR is the association of European country code top-level domain (ccTLD) registries. All EU Member State and EEA country ccTLDs (such as .de, .no, and .nl) are members of CENTR.

CENTR members represent the industry that is at the core of the public internet, safeguarding the stability and security of the internet as we know it today. The majority of European ccTLDs are SMEs or non-profit organisations, providing an internet infrastructure service in the interest of and in close cooperation with their local internet communities (i.e. registrars, end-users, rightsholders but also in cooperation with CSIRTs and law enforcement authorities).

ccTLD registries maintain a registration database that is used to collect and access the contact information of domain name holders (the so-called WHOIS database). In addition, Domain Name System (DNS) operators such as ccTLD registries are responsible for the resolution of domain name queries when a website in their domain name zone is requested.

As "private parties" responsible for managing WHOIS database who are directly affected by the planned reform of the Agency, CENTR members ask the European Commission to take into consideration and adequately assess the impact of the anticipated legislation on ccTLD operators.

CENTR recommendations

1. Threat of proliferation of data access requests across the EU

The Inception Impact Assessment considers the need to increase the capacity of the Agency "to gather and process data available in the online environment, including data requested and obtained directly from private parties, notwithstanding Europol's obligation to notify the relevant national competent authorities of the Member States as soon as these are identified", in order to more effectively fulfil its primary role in countering terrorism and serious crime across borders.

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium

Phone: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org

www.centr.org

The need for law enforcement to access data held by private parties across the EU has been the focal point of the proposal for a Regulation of the European Parliament and of the Council on the European Production and Preservation Orders for electronic evidence in criminal matters (COM/2018/225 final - 2018/0108 (COD) (hereinafter the e-Evidence Proposal). The e-Evidence proposal is currently under review by the co-legislator: the European Parliament.

The Rapporteur of the European Parliament for the e-Evidence Proposal has stated in the Draft Report[1], after consulting a large majority of stakeholders, including judiciary, data protection and fundamental rights experts, as well as service providers, that the framework suggested in the e-Evidence proposal that allows inter alia foreign law enforcement authorities **"to directly address service providers in cross-border situations without automatically involving the authorities of the other affected State(s)**[...] **would deprive States from their fundamental responsibility to ensure the respect of fundamental rights on their territory** and would, **at the same time, deprive data controllers from their obligation to respect the laws of the country where they are established**"[emphasis added].

In its discussions, the European Parliament has identified numerous concerns from a fundamental rights perspective[2], as well as the burden on SMEs[3] when numerous law enforcement authorities are mandated with direct access to data held by private parties without any procedural guarantees. Therefore, considering these concerns and the ongoing work of the co-legislators on the e-Evidence proposal, pursuing another legislation with a similar aim before concluding the negotiations of the earlier proposal would be detrimental to the rules of a democratic society, as well as to the legal clarity of the operators.

It is necessary to consider the negotiations on the e-Evidence proposal as a priority, before enlarging the scope to a supranational law enforcement authority's ability to request direct access to personal data from private parties, like ccTLD registries.

2. Possible accreditation authority role of the Agency

The European Commission's Work Programme 2020 suggests strengthening "the Europol mandate in order to **reinforce operational police cooperation**"[emphasis added]. The Inception Impact Assessment acknowledges the need for the Agency to provide stronger support for the work of national law enforcement authorities.

CENTR welcomes the goal of increased operational police cooperation as expressed in the Inception Impact Assessment and further operational support the Agency could provide for EU law enforcement authorities.

Considering the fact that the WHOIS database for enforcement purposes "may be of relevance for criminal proceedings as they can provide traces allowing for identification of an individual or entity involved in criminal

[1] European Parliament's Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Rapporteur MEP Birgit Sippel, 24.10.2019

[2] European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 6th Working Document on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 1.04.2019.

[3] European Parliament's Committee on Civil Liberties, Justice and Home Affairs, 3rd Working Document on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 13.02.2019.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

activity"[4], and due to occasional difficulties in obtaining access to non-public WHOIS records as expressed by the law enforcement community, the Agency could play a more central role in operational cooperation during cross-border investigations when several Member States are involved. In particular, the Agency's invigorated role could be reflected by allowing the Agency to give assurance to ccTLDs that individual national law enforcement agencies that approach them for access to non-public WHOIS are legitimate. This approach is already in line with the European Data Protection Supervisor's assessment[5] that the Agency could take on a "law enforcement accreditation role" by certifying EU law enforcement agencies approaching TLD registries as legitimate law enforcement agencies, already under its currently valid legal basis.

ccTLD operators have well-established information channels to their local law enforcement authorities, meaning that the mutual trust has been established by long-standing practice and network-building. National law enforcement authorities are also the primary contact point for ccTLDs in case of criminal activity involving domain names.

Considering the existing well-established connections between ccTLDs and their national authorities, this additional accreditation scenario could potentially be relevant in cross-border investigations if the pool of querying law enforcement agencies approaching ccTLDs were to rise significantly. This situation will create additional overload and burden on technical operators like ccTLDs in responding to data access requests by multiple law enforcement agencies and authorities. By taking on the role of "law enforcement accreditor", the Agency could improve police cooperation and unburden technical operators from the difficulties of verifying cross-border law enforcement authorities[6].

Mindful of the EDPS advice, the Agency could take on a role of "accreditation authority" of EU law enforcement authorities across the EU in cross-border investigations of serious crime in order to facilitate access to the WHOIS database in time-sensitive cases.

3. Involvement of national authorities and rule of law

As stated above, the Inception Impact Assessment expresses the Agency's inability to process personal data received directly from private parties upon their initiative beyond the purpose of identifying and notifying the competent authority in the Member State. The Inception Impact Assessment also notes that "while, **the rules currently in place aim at ensuring that the information is obtained in full respect of the requirements of the applicable criminal procedure law and under other control of national authorities**[...], the current legal framework limits de facto the Agency from cooperating effectively with entities like[...] online service providers and non-governmental organisations"[emphasis added].

National law enforcement authorities remain the primary contact point for ccTLDs in case of criminal activity involving domain names under their respective zones.

National law enforcement authorities are rooted in their local jurisdictions, meaning they are subject to national criminal procedural law and rule of law safeguards, usually deriving from national constitutions. These are designed to allow individuals and private (and public) entities to access justice in case of misconduct, including by law enforcement. It is unclear from the Inception Impact Assessment what judicial guarantees would apply in cases of

[4] Recital 18 of the e-Evidence Proposal

[5] European Data Protection Supervisor's letter to Europol's consultation on law enforcement access to WHOIS database

[6] CENTR Comment on the Proposal on e-Evidence. Available here: https://centr.org/library/library/policy-document/centr-comment-on-the-proposal-on-e-evidence.html

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

personal data violations when accessing personal information held by private parties like ccTLD registries. According to the current legislative basis[7] of the Agency, the appropriate venue for the right to lodge a complaint against the Agency in the case of unlawful data processing is the European Data Protection Supervisor, with the further right to a judicial remedy before the Court of Justice of the European Union. It is, therefore, essential to make sure that the right to **judicial remedy** is adequately reflected in the updated Europol's mandate and to check **whether in the new framework the venues mentioned above are still effective and appropriate** and with a sufficient legal basis considering the subsidiarity principle of the EU.

An appropriate framework with a functioning judicial remedy is also needed to **ensure legal clarity for technical operators** like ccTLDs and to make sure that any mandated action by law enforcement is adequately rooted within the local jurisdiction where the technical operator is established.

Any additional direct data collection from private parties by the Agency, if deemed to be necessary and proportionate in a democratic society, should be conducted in cooperation with the national law enforcement authorities, under judicial oversight according to the limits of national jurisdiction of the affected Member State.

4. Necessity and proportionality of the Agency's data access requests to private parties

The Agency is already subject to an autonomous regime on personal data protection and processing. Specific provisions are included in its currently valid legal basis allowing the Agency "to process all personal data received to identify the links between multiple crimes areas and investigations", without limits to one crime area[8], as well as a broad possibility for the Agency to gain computerised access to EU, national or international information systems in order to retrieve and process personal data if that is necessary for the performance of its tasks[9].

ccTLDs welcome the necessity to consider data protection safeguards and mechanisms when opting for direct data access requests to private parties or querying databases like the WHOIS database, as indicated in the Inception Impact Assessment. Considering the role of ccTLDs as predominantly data controllers under the GDPR, ccTLDs are subject to data protection obligations in collecting and processing personal data, such as data minimisation and anonymisation efforts. Private parties, like ccTLDs, should be able to raise objections to data access requests by the Agency when the justification for the data access request is not sufficiently clear, and they should be able to require additional information in order to respond to the data access request.

It is necessary to make sure that any data access request from a law enforcement authority, including the Agency, directed towards private parties, like ccTLDs, should only concern the information that is strictly necessary to achieve legitimate purpose. Blanket, vague and broad data access requests directed towards private parties, like ccTLDs, affect technical operators disproportionately, creating organisational overload and a burden on the operators.

[7] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

[8] ibid

[9] Article 17(3) ibid.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org