Fast and furious law enforcement access to digital evidence : The E-Evidence-package and its implications for Switzerland

Giulia Canova, le 7 décembre 2023

The recently adopted E-Evidence package will allow law enforcement authorities in EU member states to directly request data from a service provider in another EU member state. This article provides an overview of the new EU-wide rules and discusses potential implications for Switzerland.

After five years of negotiations, on 13 June 2023 the European Parliament adopted a legislative package for cross-border access to electronic evidence from online service providers (e.g. telecom companies, online-platforms, social media providers). From 2026 on, national law enforcement authorities in EU member states will be able to directly request certain data from service providers located in another member state, on a legally binding basis.

The introduction of the initial proposal sparked quite a debate about cross-border access to data stored by private service providers and there were strongly divergent views on almost everything despite the fact that there is a need to tackle the issue. The rules are developed to facilitate and accelerate access of law enforcement authorities to electronic evidence outside their own territory. As data has become an essential source of evidence (not only in cases of cybercrime but for quite any type of criminal offence), law enforcement authorities are increasingly relying on the collection of data in criminal investigations. A substantial part of the relevant data accrues by the widespread use of online services (instant messengers, social media, e-mail services, cloud data storage, etc.) and is stored by the providers collecting data about their users. With the data in the hand of private service providers, authorities see themselves increasingly forced to request data from private companies.

In practice, there are two major obstacles limiting access to data from service providers : First, service providers are often located in another state, and as a consequence, subject to foreign jurisdiction. Due to the principle of territoriality, authorities are not entitled to execute investigative measures in foreign territory. Coercive cross-border access to data is thus only possible based on mutual legal assistance measures, which are considered too slow and complicated. Second, direct non-coercive requests to online service providers in another state are only possible based on the voluntary cooperation of the provider, leading to uncertainty and unpredictability.

The E-Evidence package has been designed to tackle these issues by providing legally binding instruments for direct cross-border access to data without the procedure of mutual legal assistance. This article will give a short overview of essential rules of the E-Evidence package and discuss what implications the new regime could have for Switzerland.

New instruments : European Production and Preservation Orders

The E-Evidence-Package consists of a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and a complementary Directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. The Regulation lays down binding rules to obtain data from service providers, whereas the Directive obliges all service providers offering services in the Union to designate an establishment or appoint a legal representative for the receipt of, compliance with and enforcement of the orders. By this mechanism, also non-European service providers active in the European market will have to comply with orders from law enforcement authorities of member states.

The Regulation introduces two new legal instruments : a “European Production Order” and a “European Preservation Order”. By these instruments, competent judicial authorities in member states will be able to directly request a service provider (or its legal representative) in another member state to produce or preserve certain data necessary as evidence in criminal proceedings.

Subject to European Production or Preservation Orders are all service providers in the Union that offer :

- Electronic communication services (such as instant messengers like Whatsapp, Telegram, etc.);
- Internet domain name and IP numbering services ;
- Or other information society services enabling communication of users (such as social media networks like Facebook or TikTok, online marketplaces like Amazon, Ebay, etc.) or services enabling storage of data (such as cloud computing services).

The Regulation applies to European service providers that offer such services in more than one member state ; as well as to non-European service providers that are active in the EU market and are obliged to appoint a legal representative in a Member State. Similar to the GDPR which requires the establishment of legal representatives for non-European organizations processing personal data of data subjects in the Union, the E-Evidence-Package requires

the establishment of legal representatives for non-EU providers offering services in the Union. By building on this concept, the Regulation and Directive aim to develop extraterritorial effects. The relevant factor determining the scope of the Regulation is the offering of services in the Union, regardless of where the service provider's data is stored or where its servers are located.

By this mechanism, the Regulation will oblige the most important service providers, including WhatsApp, Google or Meta, to directly cooperate with national authorities.

Categories of data, access requirements and duty of cooperation

The legal framework differentiates four categories of data, considering the varying sensitivity of the data. The categories of data covered by the Regulation include :

- subscriber data (relating to the identity of the user, e.g. name, date of birth, billing and payment data, etc.);
- data requested for the sole purpose of identifying the user (IP addresses, logs and access numbers together with technical identifiers);
- traffic data (relating to the provision of a service, e.g. the geographic location of the device used, date, time, duration, etc.);
- content data (text, video, voice, images, sound, etc.).

Depending on the category of data, the requirements for cross-border access to the data differ, both with regards to both the authority that may issue an order and the underlying criminal offence. In that regard, it is important to note that the Regulation lays out rules on how to access the data, but it does not impose a general obligation of data retention or specific data retention periods for service providers, which remain to be regulated by specific European data retention legislation and national law. The Regulation sets rules for the access or acquisition of data as evidence, but not obligations to retain data in general.

To obtain subscriber data or data requested for the sole purpose of identifying the user, a European Production order may be issued for all criminal offences by a judge, a court, an investigating judge or a public prosecutor.

To obtain traffic data or content data, the requirements are higher, and a European Production order may only be issued by a judge, a court or an investigating judge (i.e. the authorization of a public prosecutor does not suffice). It may only be issued for criminal offences punishable by a maximum custodial sentence of at least three years.

In general, for all data categories the issuance of a European Production Order is only allowed if necessary and proportionate for criminal proceedings. In addition, the order to obtain data may only be used under the condition that a similar order could have been issued under the same conditions in a similar domestic case.

To issue a European Preservation Order, the requirements are less strict, as this instrument does not (yet) include access to the data. A Preservation Order may be issued for data of any category by a judge, a court, an investigating judge or a public prosecutor and for all criminal offences.

Both European Production Orders and European Preservation Orders are legally-binding for the service providers affected in the case. Upon receipt of a Production Order, the service provider is obliged to respond within 10 days, or 8 hours in emergency cases. In case of non-compliance with a valid Order, the respective service provider risks pecuniary penalties of up to 2% of the worldwide annual turnover. Thus, in contrast to the current approach (mutual legal assistance or voluntary cooperation), the new instruments will indeed provide very fast access to data ; with potential furious effects for service providers in view of the risk of sanctions.

The sticking point : involvement of the enforcing state

The new instruments enable national law enforcement authorities (from the “issuing state”) to directly issue orders to service providers in other member states, without prior authorization of the authorities where the provider is located (in the “enforcing state”). Contrary to the traditional system of mutual recognition, where a judicial authority in a state may issue an order which must then be recognized and executed by a judicial authority in the other state, the new rules allow authorities to directly issue an order to a service provider in the other state. The new system bypasses the judicial control of the enforcing state to whose jurisdiction the service provider is subject. This absence of prior authorization by the enforcing state has been the thorny issue in the negotiations. The initial proposal did not provide for a notification mechanism or authorization procedure by the enforcing state and was based on the idea of absolute mutual trust between member states. Undoubtedly, such a direct cooperation system would significantly fasten cross-border access to data. However, by skipping the assessment of the enforcing state that the request does not violate fundamental rights or principles of criminal law, the direct cross-border access system risks losing a crucial layer of control (for a detailed analysis see Albus 2023).

After lengthy negotiations about the role and degree of control of the enforcing state in the

access system, the legislators compromised on a notification mechanism of the enforcing state. Whenever a Production Order for traffic or content data is issued to a service provider, the issuing authority is obliged to notify the enforcing authority (at the same time the order has been transmitted to the service provider). The enforcing authority then assesses the order and has the possibility to raise grounds for refusal (due to immunities, privileges, conflicts with the freedom of press or freedom of expression etc.). Thus, the enforcing state has some degree of judicial control to safeguard fundamental rights, but only regarding traffic or content data.

Implications for Switzerland

The EU-wide rules for cross-border access apply to all service providers offering their services in the European market. Non-European service providers are subject to the rules if they are active in more than one European member state. Outside the European market and for law enforcement authorities from non-EU member states, the rules do not take direct effect. Swiss law enforcement authorities will not be allowed to issue legally binding access requests to providers established (or with a legal representative) in the EU. In turn, service providers established in Switzerland will not be subject to access orders unless they are also ordering services in more than one European member state. The Swiss messenger application Threema for instance, which offers its services also in the European market (thus also held to comply with the GDPR), would have to designate a legal representative in the EU responsible for compliance and enforcement of access orders.

Overall, the legislation is not having direct impact on criminal proceedings in Switzerland. The E-Evidence package is to be regarded as set of internal EU-wide rules to harmonize judicial cooperation between European member states. Still, the new facilitated access regime to evidence within the EU raises the question as to whether there is need for Switzerland to regulate access to data stored by service providers and adapts its current law. The issue gains importance because service providers in Switzerland could expose themselves to the risk of criminal liability under Article 271 of the Swiss Criminal Code if they disclose data to foreign authorities and thus contribute to activities on behalf of foreign states (as noted in the recently published report on the E-Evidence-Package of the Federal Office of Justice; for a critical summary on the issue see also www.swissprivacy.law/233).

Under the existing legal framework, Swiss authorities do not have the power to authoritatively request access to data controlled by providers outside the Swiss territory. Investigative measures to obtain data from service providers outside Switzerland must be requested over

international mutual legal assistance in criminal matters. Under Swiss law, direct requests to providers without mutual legal assistance are only allowed on the basis of Article 32 lit. b of the Convention on Cybercrime and under the requirement that the provider voluntarily discloses the data (see also the Decision of the Federal Supreme Court of Switzerland 141 IV 108, consideration 5.10, as well as the commentary on the provision in the Online Kommentar).

International legally binding access requests beyond voluntary cooperation of the provider would require a legal basis in (bilateral or multilateral) international treaties. To enable cross-border access as made possible in the E-Evidence-package, Switzerland would have to negotiate exceptions to the system of mutual assistance with the European Union or individual states. According to the report on the E-Evidence-Package, Switzerland will have to react to the new European rules, at least to avoid conflicts of law. A more far-reaching approach would be to adapt similar (national) regulation linking to the E-Evidence-Package and to build bridges to other legal systems by the means of international treaties (as mentioned in the report on the E-Evidence-Package).

Certainly, binding rules for access requests to service providers would be desirable in terms of legal certainty and clarity. Today, law enforcement authorities often depend on good will of providers and their willingness for cooperation. However, with a view to fundamental rights and data protection, there is good reason for caution in regulating direct access requests from foreign authorities. By skipping the process of mutual assistance, authorities risk losing control over the disclosure of data to foreign authorities. Additionally, by imposing binding rules to providers to disclose data, the responsibility for evidence gathering shifts somewhat to service providers, and with that to private companies which are not primarily driven by fundamental rights considerations or the rule of law. Thus, the new E-Evidence-Package should prompt Switzerland to reflect on law enforcement access to data stored by service providers and what consequences direct access instruments might have on fundamental rights of individuals. At the moment, this debate is still in its infancy in Switzerland, but should be conducted sooner rather than later as the relevance of data in the hand of providers will continue to grow.

Proposition de citation : Giulia CANOVA, Fast and furious law enforcement access to digital evidence : The E-Evidence-package and its implications for Switzerland, 7 décembre 2023 *in* www.swissprivacy.law/271

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.