WP 29 contribution to scenarios proposed in the context of the Cybercrime@Octopus

The Article 29 Working Party ("WP 29") made best efforts to provide solid and constructive answers to the scenarios proposed by the Octopus Conference.

However, the scenarios are sometimes not specific enough to receive a concrete and precise answer. In particular, since the national context of the scenarios is not always specified, it makes it difficult to give an answer that could apply to the specific situation considering the different national legislation at stake. The WP 29 draws the attention to the fact that most of the scenarios submitted to its attention fall beyond its remits and mainly concern issues other than data protection.

For these reasons, the present document is only provided for discussion and cannot be considered as a definitive and final legal answer to the different scenarios proposed. It must be seen as a "non-paper for discussion only" as the result of the will of the WP 29 to provide its expertise to the debate and to remind the basic data protection principles that might interact with the application of the Budapest Convention.

Context

During the conference on the Budapest Convention held in Strasbourg on 19-20 June 2014, various scenarios regarding access to information by law enforcement authorities were presented in relation to transborder access to personal data.[1] These scenarios were intended to stimulate a discussion on the consequences of data protection legislation and principles when obtaining such data in criminal investigation.

In view of the plenary session of 2-3 December 2014, the WP29 shared with the Bureau of the Cybercrime Convention Committee (T-CY) a first assessment of the data protection implications of the various scenarios.[2]

At its plenary of 2-3 December 2014, the T-CY came to the conclusion that an additional Protocol on transborder access to data located in a foreign jurisdiction was not feasible in the current political context.

A new working group "on criminal justice access to evidence stored in the cloud, including through mutual assistance (Cloud Evidence group)" was set up. This group will take over the work on transborder access to data as well as the results of the T-CY assessment of the mutual legal assistance provisions of the Convention on Cybercrime adopted in December.

The WP 29 proposed to provide the T-CY with an in depth analysis of the scenarios. In this context, the present document is providing some elements of answers regarding the 18 scenarios proposed by the T-CY.

[1] The scenarios are available at http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@Octopus/cyber_COE_TB_Scenarios_june2014%20V5web.pdf

[2] See letter of the WP29 dated 28 November 2014 available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20141128__letter_of_the_art_29_wp_t-cy_on_the_cybercrime_scenarios___not_signed.pdf

General remarks

Before commenting on the specificities of the scenarios, we would like to make some general remarks.

Applicable law

The first step that needs to be taken when assessing the legality of access to personal data in a law enforcement context, both nationally and transborder, is to identify the applicable criminal (procedural) law. This can be different laws of different countries, since criminal (procedural) law and data protection law are triggered by different criteria[3]. In most cases, a good practice would be, as a second step, to inform, where known, the competent counterpart authority a priori or a posteriori.

From a data protection point of view, it is important to recall that the EU data protection legislation will be primarily triggered by the location, on the EU territory, of the establishment of the controller processing the data in the context of his activities[4]. Moreover, still from this point of view, the legislation and principles which should be respected by law enforcement authorities largely depend on the prior identification of the State where they are performing their activities. The Working Party therefore regrets that this information is, in most scenarios, not given. In any case, the legality of transborder access will be largely dependent on applicable national criminal law legislation (*i.e.* the existing bilateral or cooperation agreements, or the domestic legislation of the searching country or the one of the searched country).

One should remind that the Directive 95/46 was implemented by most Member States to apply its principles to police and law enforcement activities. Therefore, the level of protection granted by the Directive primarily aimed at covering the processing of data by the private sector. The police activities are however covered by the Convention 108 and the Recommendation 87(15), which is the minimum standard to the countries bound by the Convention.

Where data protection provisions may be similar in at least the European Union Member States following the implementation of Directive 95/46/EC and in the countries being subject to Council of Europe Convention 108 and recommendation 87(15), criminal law and criminal (procedural) law still largely differ. In our view, the first of data protection principles that law enforcement authorities wishing to access data have to ensure compliance with, is the principle of lawfulness of the data processing. For many of the scenario's, the discussion should focus on how to obtain data in a sovereign third country while respecting both the criminal (procedural) law of the searching and the searched State. Only if obtaining such data would be regarded as lawful, an assessment of the implications in terms of subsequent data protection requirements comes up. In this respect, compliance with the sovereignty principle and with existing Mutual Legal Assistance Treaties is crucial.

[3] For example, the law governing the law enforcement authorities is the one of the country of this authority, while national data protection law applies where the controller of the processing is established.

[4] See Article 4(1)a Directive 95/46/EC. It should be noted that even if the controller is not established on the EU territory, he will have to respect the EU data protection legislation if he makes use of equipment, automated or otherwise, situated on the territory of an EU Member State (Article 4(1)c of Directive 95/46/EC. See also the *Google vs. Spain* decision of the UECJ, C-131/12.

Consent

Consent in a law enforcement context is not the same as consent in a data protection context. These notions therefore need to be carefully separated and can certainly not be regarded as interchangeable. To be clear:

As already mentioned in the letter of 28 November 2014, when it comes to data protection principles, consent must be freely given, specific and informed to be valid. Therefore, in a law enforcement context, it is very unlikely that a data processing can be legitimized on the basis of the consent of the data subject. The appropriate ground for the processing for a law enforcement authority would rather be found in the law governing their activities.

This means that in a law enforcement context, consent cannot serve as a valid legal basis to access personal data. Furthermore, Recommendation n° R (87)15 regulating the use of personal data in the police sector and adopted by the Committee of Ministers of the Council of Europe allows the collection of personal data for police purposes when necessary for the prevention of a real danger or the suppression of a specific criminal offence unless a specific national legislation provides otherwise. This would clearly cover most of the scenarios presented.

The meaning of the notion of *"consent of the person who has the lawful authority to disclose the data"* as mentioned by Article 32 b) of the Budapest Convention appears to be the core issue, since this notion has never received an unambiguous interpretation and can therefore receive several meanings[5]. The adoption of article 32 was rather controversial during the negotiation of the Convention[6]. The major issue with this provision of the Budapest convention is the lack of definition of the terms "consent" and "person who has lawful authority to disclose the data"[7].

The interpretation of the term "consent" as used in this provision is therefore not an issue that should only be solved on the basis of data protection law, should data protection law be considered as applicable to understand the meaning of this notion.

Data transfers

When discussing transborder access to personal data, it should be considered that an international transfer will take place when data stored in country A is accessed by country B. As long as country A and B are both EU Member States, this will not be an issue, since they will provide a similar (and

[5] See letter of WP 29 of 5 December 2013, pages 2-3.

[6] *"The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length.*
There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof." Convention on Cybercrime, Explanatory Note ¶ 293.

[7] See *eg.*, Prof. Ian WALDEN, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*, p. 8-9, electronic available at http://ssn.com/abstract=1781067.

adequate) level of data protection. This shall also be the case when data are transferred between Countries Parties to the Convention 108.

The situation is different with regard to third countries. Only under specific conditions it is allowed to transfer personal data from the EU to a public authority in a third country.

As any processing, a transfer should comply with all the data protection principles, including the principles of necessity, proportionality and purpose limitation. In addition, according to Article 25 of the Directive (if applicable to the law enforcement sector of the country concerned), the recipient also has to offer an adequate level of protection. If the European Commission takes a decision recognising the third country indeed has such an adequate level of data protection, transfers can take place without further restrictions.

Considering the adequacy decisions of the European Commission following article 25(2) Directive 95/46/EC only have effect to transfers to the private sector, the conditions of Article 26 to derogate from Article 25 principles need to be assessed. In a law enforcement context the derogations mentioned under paragraph 1 sub (d) and (e), seem particularly relevant. A data transfer to a non-adequate country could then take place on condition that:

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject;

The situation is different when data is transferred from the law enforcement authorities in an EU member state to law enforcement authorities in a non-EU country. In that situation, the provisions of the Framework Decision 2008/977/JHA on the protection of personal data processed in the context of police and judicial cooperation in criminal matters will apply. This legislation also states that a transfer of data to a third country may only take place if the Third State concerned ensures an adequate level of protection for the intended data processing an adequate level of data protection[8] except in exceptional situations, described in its Article 13(2) and (3). In particular, the transfer to a State that does not ensure an adequate level of protection for the intended data processing can take place if the national law of the Member State transferring the data so provides because of legitimate specific interests of the data subject or legitimate prevailing interests, especially important public interests.

With regard to the Parties to the Convention 108, the situation is similar. The Convention 108 is applicable to the processing of personal data in the private and in the public sector, including police and justice. With reservation of an adequacy decision, they should be no obstacle concerning the transfers of data between Parties (art. 12 Convention 108). Concerning the transfers to third countries, the additional protocol to Convention 108 regarding supervisory authorities and transborder data flows foresees that each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a state or organisation that is not Party to the Convention only if that state or organisation ensures an adequate level of protection for the intended data transfer (art. 2.1). In absence of an adequate level, the transfer is possible under the similar condition as for EU members (art. 2.2).

[8] See Article 13(1)(d)

Given the difficulty to assess whether a transfer to a third country, of personal data stored in Europe, is possible under the circumstances given in article 26 (1) d) and e), the use of existing tools to obtain personal data stored in another country, more specifically Mutual Legal Assistance Treaties, should be preferred. These treaties intend to ensure that the correct legal procedures are followed when obtaining (personal) data that is stored in an European Member State.

Nevertheless, it should be noted that the abovementioned exceptions cover most of the situations described in the scenarios so that the data protection legislation accompanies the work done by law enforcement authorities rather than being an obstacle.

The practice of Mutual Legal Assistance Treaties

We note that many delegations insisted during the Cybercrime@Octopus Conference that the mutual legal assistance procedures in practice do not always function in a satisfactory way. However, these dysfunctional practices do not justify the circumvention of applicable rules but rather call for their recast and improvement.

Also, there may be situations where these procedures may not be sufficient, namely in cases where it is unknown where the data are located, such as the deepweb, or when there is uncertainty where the processing takes place. It is however unarguable that only because it is unknown where data are processed, the data protection principles can be ignored when it cannot be deduced which data protection regime would be applicable. Fundamental rights in Europe need to be respected. Therefore, in these situations, it needs to be assumed that the data could be processed in any of the other Parties' jurisdiction and thus, it is our view that it would be the most appropriate solution if the searching Party respects the Party that has set the highest data protection standards to ensure that the data protection law of the searching Party is not violated. In this respect it would be advisable if all States Party to the Budapest Convention would also ratify Convention 108 and its additional Protocol and transpose it's principles into their national law. To the extent that countries are already Party to Convention 108, they should ensure its provisions are respected.

Analysis of the scenarios

Scenario 1

In a kidnapping case being investigated by European country A, ransom notes are coming from an email address that originates with a US provider. Country A wants to know the accountholder's information.

An IP address is considered personally-identifiable information by Country A.

A is not permitted to provide personally-identifiable information directly to US providers because they are private parties, not governmental parties. The notes threaten to kill the victim in two days if conditions are not met.

Should A be permitted to send the information to the US provider because it is an emergency (and because identifying an accountholder would be only the start of the investigation)?

If yes, may A's law enforcement authorities send it immediately, or must it undergo data protection review? If it must undergo data protection review, what would the review entail? Should A be required to establish procedures for emergency data protection review?

The competent authority in Country A has to rely on national law and existing cooperation agreements to assess the conditions under which the IP address was obtained. Once the IP address was collected, it is to the national law of/bilateral or multilateral agreement concluded by Country A to establish the conditions under which such a data can be transferred to the US provider, which is a private party.[9] It is up to national legislation to provide a specific procedure to submit such requests to a data protection review[10].

As to the right for the private entity to provide such information to the competent authorities of a third country, it is to the national legislation of the US to establish the cases when such a transfer outside the US is authorised.[11]

Scenario 2

A teenager who is close to her parents telephones them to say that she is walking home from a party but then disappears. The police would like to examine her numerous social-networking accounts, which are run out of several different countries. The distraught parents cannot find her passwords. The girl is not an adult under the law of her country. Should her parents be permitted to give consent to the police to search the account?

The question of accessing a social network account by the police does not appear to be a matter of consent for the following reasons:

Depending on national law, the police can access the information that has been made publicly available by a subscriber of a social network. This is confirmed by article 32 a) of the Convention on Cybercrime which states *"that a Party may, without the authorisation of another party, access publicly available (open source) stored computer data, regardless of where the data is located geographically."*

Second, as already stated, consent if not the appropriate legal basis for the processing of personal data by law enforcement authorities.

Depending on what is meant by "searching the account", an appropriate legal basis should exist to process personal data by the police: the domestic law regulating the collection and use of personal data by the police.[12] Again, reference to the Recommendation R (87) 15 can be done in this respect.[13]

---

[9] WP 29 already noted that in the field of police, the Recommendation No. R(87) 15 is to be considered part of the standard level of data protection to be ensured" (see WP 29 letter of 28 November 2014). In this respect, one can read that article 5.3.ii of the Recommendation R(87) 15 states that *"5.3.ii. Communication to private parties is exceptionally permissible if, in a particular case:*
a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if
b. the communication is necessary so as to prevent a serious and imminent danger."

[10] It is not clear in this case what is understood as a "data protection review". This could be better defined in the further discussions.

[11] At the same time, the situation in the US regarding request to provide data stored in another country by a private entity is subject to discussion in a case involving Microsoft and its cloud services; see: http://www.duquesneadvisory.com/US-jurisdiction-over-emails-in-Dublin-can-Microsoft-win-in-the-Court-of-Appeals_a293.html

[12] Where the Convention 108 is applicable, it should be reminded that article 5 a) states that personal data undergoing automatic processing shall be obtained and processed fairly and lawfully. The national legislation

Scenario 3

Investigators in Country A are investigating a massive fraud. Several hundred people lost all their savings when they tried to purchase certain items using an Internet service originating in Country B. The items were never delivered. A founder of the group who has administrator privileges on its website, hosted in B, is arrested while on vacation in A. He wants to cooperate with the authorities of A to disclose IP addresses of participants, financial documents, the network tools that were used, and similar evidence. Such cooperation would reduce his prison sentence and his attorney is advising him to cooperate. The authorities want the disclosures in order to shut down the network and locate unknown victims.

Scenario 3 cont'd

The Article 29 Working Party states that consent is freely given only in the absence of several factors, including "significant negative consequences." Should the arrested man and his counsel be allowed to consider his cooperating to reduce his prison sentence? Would it violate the arrestee's human rights to deny him the possibility of reducing a prison sentence? What about the rights of the victims to possible restitution?

Similarly, the Article 29 WP letter discusses what constitutes "consent" or "lawfully obtained credentials" under EU data protection law. Criminal law inside and outside the EU may define "consent," "lawfully obtained credentials," and other terms differently than data protection law does.

*If criminal law and data protection law would yield different results, which law governs? What if a country with inadequate data protection laws is involved?*In case there is an establishment of the company in the EU, the data protection regime of the place of the establishment of the company will be applicable.[14] The principles of the Directive 95/46 will have to be respected, and in particular the lawfulness of the disclosure of the data. This would lead to two verifications:

First of all, the question of the delegated powers of the founder arrested to reveal these data should be verified with *i)* the bylaws of the company and *ii)* with the law applicable to the governance of the company, which is in principle the company law of the state of incorporation of the company. If the applicable law and the bylaws allow the founder of the group to reveal such data, it should be checked whether the EU data protection law is applicable.

Second, if the voluntary disclosure of information for judicial cooperation is allowed by the applicable law, then the disclosure to the competent judicial authorities is subject to the legal conditions set in the law. If the voluntary disclosure of data by a founder for judicial cooperation purposes is not permitted by the applicable law, then the competent authorities will have to identify the appropriate channel of cooperation with the authorities of country B.

Regarding the question concerning the consent and the definition of it, we refer to the general introductory remarks relating to the interpretation of consent in the context of data protection law. The existence of different meanings of the term consent in two different laws (*i.e.* criminal law and data

regulating the police activities should therefore provide the appropriate legal basis for such a processing to take place.

[13] See article 2.1 of the Recommendation.

[14] WP 29 Opinion 8/2010 on applicable law, WP 179.

protection) will not prevent both laws to apply. In this specific scenario, the consent at stake in terms of data protection law is the consent of the data subjects (*i.e.* the persons whose data are processed by the company) and not the consent of the natural person, founder of the company.

Finally, if the data are to be transferred to a country with no adequate protection in the meaning of Directive 95/46 and Convention 108, the derogations provided in these texts should apply, as mentioned in the general introductory remarks. In the scenario, should Directive 95/46 apply in this case, Article 21) d provides that a transfer is allowed when it is "necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims".

Scenario 4

Police-to-police passage of information is favoured by law enforcement because it can keep an investigation moving, even though it may be foreseen that a formal mutual legal assistance request may be needed to obtain evidence that is usable at trial.

Is police-to-police passage of data impermissible if the data would go to a country judged to have inadequate data protection rules by EU standards?

The principle remains that data transfers should only take place where the receiving State provides for an adequate level of protection except in limited and enumerated situations (see development in general remarks).

If the data was received by the police authorities of a State from another State bound by the Framework Decision, according to the Framework Decision 2008/977[15], further transfer to a third Country is authorised under specific conditions[16]. One of these conditions is that the third country ensures an adequate level of protection for the intended data processing[17].

By way of derogation, data can be transferred to a country that does not ensure an adequate level of protection if:

a) the national law of the Member State transferring the data so provides because of:

(i) legitimate specific interests of the data subject; or

(ii) legitimate prevailing interests, especially important public interests; or

[15] The Framework Decision is not applicable to domestic use of data: see Article 1.2 of the Framework Decision.

[16] According to Article 13.1 of the framework decision, Member States shall provide that personal data transmitted or made available by the competent authority of another Member State may be transferred to third States or international bodies, only if:
(a)it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
(b)the receiving authority in the third State or receiving international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
(c)the Member State from which the data were obtained has given its consent to transfer in compliance with its national law; and
(d)the third State or international body concerned ensures an adequate level of protection for the intended data processing.

[17] See article 13.1 of the Framework Decision.

(b) the third State or receiving international body provides safeguards which are deemed adequate by the Member State concerned according to its national law.

Should the Framework Decision not be applicable to this case[18], the Additional Protocol to the Convention 108 regarding supervisory authorities and transborder data flows, provide that a transfer of data to a third country that does not ensure an adequate level of protection can take place under conditions similar to the conditions stated by the Framework Decision.

Scenario 5

A group has collected and posted public information, including home address, photographs, children's schools, etc, about a group of policemen from Country A. While the information is public, it gives a very complete picture of the policemen's lives when the information is aggregated. They are frightened for themselves and their families. There are no explicit threats of violence but an investigation is opened. The website is hosted in the US to take advantage of a) US Constitutional hurdles to searches by the US government and b) difficulties of cooperation between EU countries and the US. The police in A, a civil-law country that is a Party to the Budapest Convention, have arrested someone who wants to cooperate voluntarily and seems to have the lawful authority to consent to disclosure of data from the website. The police in A know that the US is a Party to Budapest and would like to do a search of the website pursuant to Article 32 b. Data protection authorities in A tell the police in A that they must follow the suggestion of the Article 29 Working Party and, therefore, apply US law in determining whether they have valid consent under the Budapest Convention.[19]

Scenario 5 cont'd

The police and justice authorities swiftly become confused about US law. It is not statutory but case law; they are unfamiliar with the distinction between the law of US states and US federal law; they don't know which federal district is relevant to the place where the website is hosted; and, while they know which federal circuit to research, they are unaware that a leading case on consent has just been decided in a different federal circuit court.

Recently, there have been daily postings of photos of children of these police officers on their way to school, but no explicit threats. Since the authorities are increasingly worried that there may be a tragedy at any time, what should they do?

They have been advised by the US government that this is probably not an emergency, so they have decided not to apply for help from the US provider on an emergency basis.

If country A implemented either the framework Decision or the Convention 108, the reception of the information from a third country like the US is not an issue regarding EU data protection law, since principles on transborder transfer of data are only applicable in case of transfers outside of a country where Convention 108, Directive 95/46 or Framework Decision is applicable. The data processed received by the police authorities will of course have to comply with the national data protection

[18] Because the Searching State is not bound by the Framework Decision or because the data were not originally obtained from another States bound by the Framework Decision.

[19] It should be reminded that data protection authorities do not have the power to give instruction to the police in the context of criminal investigations.

principles applicable to them, if any. Nevertheless, depending on what type of request the authorities in country A want to address to authorities in the US[20], the existence of a MLAT (*e.g.* the cybercrime convention) between country A and the US should be the sole legal channel to be followed, and the circumvention of the said MLAT should not be a valid option. In the context of a MLAT, the lawful authority to disclose/delete/block the data would be the competent authority designated by the searched state. Besides, the fact that there are difficulties of cooperation between the EU and the US should not justify any circumvention of existing agreements.

Finally, application of the article 32.b of the Cybercrime convention (access with the consent of the person with the lawful authority to disclose the data) would only be possible if the term "consent" of this article is interpreted in a way that allows the hosting provider to validly consent to the communication of the data. In this regard, as already stated in previous letters and to comply with data protection requirements, the Article 29 Working Party reminds that the term "consent" used in Article 32(b), can be interpreted as referring to the consent of the competent public authority rather than the consent of the controller or the consent of the data subjects.

That should be checked by the provider and should not be the responsibility of the police authorities in charge. It should also be reminded that article 35 of the Cybercrime convention provides that the Parties shall appoint a point of contact, of which one of the tasks shall be the provision of legal information and collection of evidence.

Scenario 6

Often computers inside a country are networked with computers outside it. As long as they have a valid legal basis for a domestic search, an increasing number of countries (including EU countries) permit themselves to search foreign networked computers. This permission is based on statutes or court decisions but also on frustration with mutual legal assistance. If such practices violate data protection law, may a country carry out such networked searches?

See above our development on Article 32(b) of the Budapest Convention.

Since the permission is based on a court decision or on a statute and circumvents the application of the Cybercrime convention, such a solution violates the Budapest Convention.

Therefore, such an (illegal) access could violate the domestic data protection legislation of the searched party.

That would be the case, *eg.,* if the data controller is established in the searched country since, and is subject to the Directive 95/46, since the presence of an establishment in an EU country triggers the application of the Directive.[21]

[20] It is not clear according to the scenario what would be the request addressed to the US: reception of the identity of the persons storing the data on the server, deletion of these data, ...

[21] One should note that, Yahoo! , a US base company, was imposed a fine by a Belgian Criminal Court for failing to identify the users of a number of webmail accounts to the Belgian public prosecutor. Yahoo! argued that an international treaty existed between Belgium and the US which should be followed to search information from a US company. The Court of First Instance decided that Yahoo! was an electronic communication services provider (ESP) within the meaning of the Belgian Code of Criminal Procedure and that the obligation to cooperate with the public prosecutor applied to all ESPs which operate or are found to operate on Belgian territory, regardless of whether or not they are actually established in Belgium. This first decision was overturned by the Court of Appeal, on the ground that the Code of Criminal Procedure was to be read in the

In this specific context, the risk of violation of EU data protection law has already been raised by the WP 29 in its Opinion on cloud computing[22].

It should also be reminded that, besides the potential breach of data protection legislation of the searched country, and if article 32 b is not applicable to this scenario, Article 3 of the Budapest Convention makes illegal access a criminal offence and Articles 4 and 5 make it a criminal offence to commit data or system interference. In case the national legislation implementing the Budapest Convention considers that access by a foreign law enforcement authority violates these provisions, the access might be considered as illegal in the searched country on this basis.

Scenario 7

Mr A cyberstalks Ms B. Becoming nervous about being discovered, he asks the relevant provider to delete a certain posting. He tells the provider that B is his mistress and it would be embarrassing and destructive of his private life if his wife became aware of the posting. The provider rejects the request, so A applies to his data protection authority. Without consulting B, the data protection authority orders the provider to delete the posting. Law enforcement is eventually alerted by B. When law enforcement seeks the posting from the provider, it is irretrievable. Is the data protection authority liable for damages or some type of sanction because it acted without obtaining the full facts, particularly by not consulting B?

The data protection authorities, when issuing an order to delete data, should apply the national data protection legislation. For example, article 6.1 e) (data retention), article 12 b (right of erasure and rectification) and article 14 (right to object) might be appropriate legal basis to ask the controller to delete data relating to a data subject.

According to the conditions laid down in Article 14 of Directive 95/46/EC (right to object), DPAs should ask the data subject to submit legitimate grounds relating to his/her particular situation to justify the request. As regards the specific right to rectification or erasure (article 12 b), such a right is

---

light of the law on Electronic Communications of 13 June 2005 that defines an ESP as a company offering services consisting in the transmission of signals on electronic communication networks. Therefore, according to the Court, Yahoo! was not an ESP since it provided a webmail service. In January 2011, the Belgian Supreme Court reversed the Court of Appeal's decision considering that, according to the principle of autonomy of criminal law, the concept of electronic communications services provider in the Belgian Code of Criminal Procedure was to be interpreted autonomously. On the basis of this decision, non-Belgian providers operating in Belgium via the internet may be required to disclose personal data of their customers in the context of criminal investigations conducted in Belgium. (see https://www.huntonprivacyblog.com/uploads/file/Belgian_Yahoo_Case.pdf

[22] Opinion 05/2012 on Cloud computing, WP 196: *"There is a risk that personal data could be disclosed to (foreign) law enforcement agencies without a valid EU legal basis and thus a breach of EU data protection law would occur"* (page 5); *"Access to personal data for national security and law enforcement purposes: It is of the utmost importance to add to the future Regulation that controllers operating in the EU must be prohibited from disclosing personal data to a third country if so requested by a third country's judicial or administrative authority, unless this is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority"* (page 21). See also WP29's comments to the LIBE Committee's vote on 21 October 2013 (comments published on 11/12/2013)/Access by public authorities and data transfers to third countries; WP222/Statement on the results of the last JHA meeting/ 17 September 2014; Working Document on surveillance of electronic communications for intelligence and national security purposes/5 December 2014, Page 52, 6.1.1.

limited to situations where the data is incomplete, inaccurate or kept too long taking into account the purpose of the processing.

Moreover, by taking such a decision, the data protection authority might also take into account any data retention legislation that might impose the service provider to retain data for a certain period of time. In this context, the deletion of the data should not be possible. Therefore, is it unlikely that the decision of the data protection authority would be considered illegal. On the contrary, if the service provider retains the data for a longer period than the period necessary to achieve the purpose of the processing, it might be in breach of the data retention principle mentioned above.

If, for any reason, one might prove that the data protection authority acted in violation of the law, the national law on liability of the public authorities might provide for a remedy. Of course, this issue has to be solved in contemplation of the applicable national law.

Scenario 8

In a serious criminal investigation, Country A seeks preservation of data from Country B. Both are Parties to Budapest. However, unknown to law enforcement authorities in A or B, the data protection authorities in B have ordered the provider to delete the same data that Country A is seeking. The provider has not acted yet, so this is still an open question.

Should the data be preserved or deleted?

In this case, the provider has received two contradictory decisions: a criminal order to preserve the data and a decision to delete them. Obviously, this has to be resolved on the basis of the national law referring to situations where two different authorities issued two diverging decisions[23].

In terms of data protection law, the setting of a retention period implies that the data processed is retained for the time necessary for the purpose pursued and would never prevent a law enforcement request to be processed.

Besides, the deletion of the data processed ordered by a data protection authority is not incompatible with the preservation of the same data, offline or in a specific file, for the sake of criminal law requirements. Indeed, in the context of criminal law, the preservation of data means, in principle, storing a copy of a data set, while deletion under data protection law leads to the erasure of the data at stake. following the DPA's request. It shall therefore be possible for the provider to conciliate the preservation order and the decision of the data protection authority.

[23] This can be submitted to a judge who will assess the case on the basis of all relevant legislations (without limiting to data protection law or criminal law).

Scenario 9

During criminal investigations your law enforcement agency has acquired via an "informant" knowledge of the username, login and password of an e-mail account in which e-mails were present containing information on drug trafficking to your country, including details of modus operandi and dates of smuggling these drugs into your country. The data is not stored in your country. Urgent action is required. What options:

1. A prosecutor issues a production order to a foreign service provider requesting email data related to a specific email account?

2. The prosecutor instructs the police to access the email account via "webmail"?

The solution to this question depends on national legislation and national case-law. Indeed, if a law enforcement authority have the legal power to request a foreign provider to disclose data stored in another country, one will still have to verify that such a transfer of data does not violate the data protection law of the country where the data are processed by one establishment of the provider. Option 1 is similar to the context already mentioned in the Yahoo! and Microsoft cases mentioned above. In the Belgian Yahoo! case, such a production order was accepted by the Belgian Supreme Court. Therefore, the production order was validated by a judge and should be considered as legal under the data protection legislation, under the exceptions to the principles that the Member States can adopt to safeguard "the prevention, investigation, detection and prosecution of criminal offences"[24].

As to option 2, if the national law provides for the possibility to authorise the access of a suspect's email account by the police, the reasoning will be the same.

However, depending on the national legislation of the searched country, the intrusion into the email account might amount to a data interference, which should be considered as a criminal offence under domestic law, according to Article 4 of the Budapest Convention.

Scenario 10

During criminal investigations into a child pornography case your law enforcement agency detects servers on which there were very violent child abuse images. Via a bulletin board on the servers it is even possible to "order" the execution of "hands on" sexual child abuse and the recording of the abuse in images which are to be sent to the person placing the order. The location of these servers is unknown ('hidden services').

a) A search of so-called TOR (The Onion Router) servers that were known NOT to be located in your country is ordered with the consent of a magistrate.

b) Digital copies of the incriminating information to be used in the criminal case later on are made in the process of search and seizure of the TOR servers, and the data on the servers is destroyed.

The first search performed in order to locate the server is not a matter of data protection. Even more, the search and storage of data should be made in accordance with the national procedural law.

[24] See article 13, 1, d of the Directive 95/46.

Even if the data processed on the server were subject to data protection legislation, the exception provided by the Directive or the Convention 108 in the context of law enforcement[25] will authorise the law enforcement authorities to access the data.

The processing of data in the context of a specific investigation is subject to the applicable national criminal procedural legislation. Once the data located and the data controller identified, it should be ensured that the applicable data protection legislation is complied with.

Scenario 11

Mr A, who was a resident but never a citizen of Country 1, was tried and convicted by Country 1 for complicity in the murder of 3,000 people in Country 2. He served a prison sentence in Country 1, he had no relatives, and he's dead.

Should data protection rules prevent his digital personal criminal records[26] from being made available to foreign prosecutors who are conducting related investigations?

If his personal criminal records should be unavailable for data protection reasons, what is the public interest being protected?

Here again, the potential application of data protection rules to the concerned data[27] would not impair the sharing of information in the context of criminal and police cooperation[28].

If the information is shared among countries subject to the Framework-Decision 2008/977, some restrictions to onward transfers may apply and specific conditions as to the processing of the data will have to be met [29].

Among others, as always, the Convention 108 and the Recommendation (87) 15 should also be complied with, and the principles provided therein on international transfer of data should be followed[30].

Scenario 12

Transborder access to data in another Party with consent (Article 32b) A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.

As a reminder, the adoption of article 32 was rather controversial during the negotiation of the Convention[31].

[25] See article 13. 1 d) of Directive 95/46 and 9.2 of Convention 108.
[26] We assume that here, the correct term that was intended to use is "personal criminal records".
[27] Knowing that some countries do not provide for protection of personal data of deceased people.
[28] See article 13. 1 d) of Directive 95/46 and 9.2 of Convention 108.
[29] Such as, *eg.*, the principles of lawfulness, proportionality, purpose limitation (article 3), the right of rectification, erasure, and blocking (article 4) or the conditions relating to automated individual decisions (article 7).
[30] See in particular article 5.4 of the Recommendation 87 (15).

The major issue with this provision of the Budapest convention is the lack of definition of the terms "consent" and "person who has lawful authority to disclose the data"[32].

The following scenarios address these issues and shall be examined hereunder.

Scenario 13

Transborder access to data in another Party with consent (Article 32b Budapest Convention) A suspected drug trafficker is lawfully arrested while his/her mailbox hosted in another country – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b.

It should be checked whether the national applicable legislation allows for such procedure and, if that is the case,the derogations to data protection referring to criminal purposes, as provided *eg*.in Directive 95/46, Convention 108 or framework Decision 2008/977, will apply accrodingly.

However, the Article 29 Working Party recalls that consent is not the appropriate legal basis for the processing of data by law enforcement authorities[33] in compliance with data protection requirements.

Considering the above, in situations where the data controller is likely to be established in another jurisdiction, it is our view that it would be the most appropriate solution if the searching Party respects the conditions of the Party that has set the highest data protection standards to ensure that the data protection law of the searched Party is not violated[34].

In any case, we advise that, as soon as the data controller is identified, the fundamental data protection rules are respected *a posteriori*[35] and that the competent counterpart authority is informed of the access made to data.

---

[31] *"The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length.*
There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof." Convention on Cybercrime, Explanatory Note ¶ 293.

[32] See *eg*., Prof. Ian WALDEN, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent,* p. 8-9, electronic available at http://ssn.com/abstract=1781067.

[33] The question whether the term "consent" as mentioned in Article 32 b of the Budapest convention refers to the consent of the data subject, the data controller, or the consent of the law enforcement authority remains the core issue to be solved for a correct and unambiguous application of Article 32 of the Budapest Convention, which would be compliant with all fundamental rights.

[34] See WP 29 letter of 28 November 2014.

[35] The transmitting Party should check (see WP 29 letter of 5 December 2013):

- that the data processing is lawful, i.e. compliant with national legislation and, if relevant, international agreements,

Scenario 14

Transborder access to data with consent but not necessarily in another Party

A suspected drug trafficker is lawfully arrested while his/her mailbox that is likely to be hosted abroad – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device.

If the suspect voluntarily consents that the police access the account but if the police are NOT sure that the data of the mailbox is located in another Party, may the police proceed and access the data?

See above.

Scenario 15

Transborder access to data without consent A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device or the police has obtained the access credentials during a lawful search. The suspect does not consent. Can the police access the account under domestic procedural rules even if the data are likely to be located in another State?

See above as well.

The Article 29 Working Party believes that uncertainty with respect to location does not allow for contravening the binding rules that are applicable with respect to fundamental rights' protection in the Member States and to ignore their jurisdiction.

Indeed, should the controller's establishment be located in another jurisdiction, and the data need to be transferred from a law enforcement authority located in an EU Member State to a third party, Article 13 of aforementioned Framework Decision or Convention 108 would apply laying down the conditions for such transfer[36].

For these safeguards to apply, it is necessary that the jurisdiction of the relevant Member State is respected. The solution proposed under this alternative scenario would lead to ignoring this national jurisdiction together with the principle of national sovereignty.

- that the request is made for specified, explicit and legitimate purposes and that the data will be processed only for the purpose mentioned in the cooperation agreement (fight against cybercrime in this case),
- that only data that is accurate, complete and updated, as well as adequate, relevant and not excessive in relation to this purpose is transmitted,
- that any further processing for a different purpose, transmission to another authority, agency or body, is authorized by the sending State and subject to strict conditions (see page 1 as regards conditions for derogations from data protection principles),
- that the data will not be retained longer than necessary for the purpose pursued,
- that transmissions and receptions of personal data are logged or documented,
- that security of the data processing is ensured,
- and finally, that an independent supervisory authority5 is responsible for checking that these requirements were respected in both the transmitting and the receiving Party.

[36] See developments under Scenario 4.

Scenario 16

Transborder access to data without consent in good faith or in exigent or other circumstances 1. Your are in country A and doing a search without consent in a well-known provider in your own country A. Without your knowledge, the provider has changed its network architecture and moved the data to country B. 2. In an emergency situation (e.g. a kidnapping investigation), law enforcement has lawfully acquired the access credentials to an email account under a domestic procedure and uses the credentials to search the account.

We refer to the response of the WP 29 in the letter of 5 December 2013 in this respect regarding the case of a transborder access without consent in good faith.

The response to this scenario is rather similar to the one given regarding scenario 15. Here again, we advise that, as soon as the data controller is identified, the fundamental data protection rules are respected *a posteriori*[37] and that the competent counterpart authority is informed of the access made to data.

Scenario 17

Transborder access by extending a search from ones territory to another territory

A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device or the police has obtained the access credentials during a lawful search.

The suspect does not consent. Can law enforcement search the device and extend it to data hosted abroad under domestic procedural rules (e.g. domestic court order)?

The Article 29 Working Party draws the attention to the fact that this would enable a law enforcement authority with lawful access[38] to a specific computer system to access data stored in another computer

[37] The transmitting Party should check (see WP 29 letter of 5 December 2013):

- that the data processing is lawful, i.e. compliant with national legislation and, if relevant, international agreements,
- that the request is made for specified, explicit and legitimate purposes and that the data will be processed only for the purpose mentioned in the cooperation agreement (fight against cybercrime in this case),
- that only data that is accurate, complete and updated, as well as adequate, relevant and not excessive in relation to this purpose is transmitted,
- that any further processing for a different purpose, transmission to another authority, agency or body, is authorized by the sending State and subject to strict conditions (see page 1 as regards conditions for derogations from data protection principles),
- that the data will not be retained longer than necessary for the purpose pursued,
- that transmissions and receptions of personal data are logged or documented,
- that security of the data processing is ensured,
- and finally, that an independent supervisory authority5 is responsible for checking that these requirements were respected in both the transmitting and the receiving Party.

[38] Considered lawful according to the national legislation of the searching country.

system even if the latter is not within the jurisdiction of the requested Party, provided the data is accessible from or available to the initial system and located in a Party or in an unknown location[39].

The Article 29 Working Party recalls that such an access would breach the principle of territoriality and sovereign jurisdiction of the requested Party (the Party on whose territory or within whose jurisdiction the data is located). In case the searching Party does not recognise the right to protection of one's personal data as a fundamental right, such an access could violate of the rights guaranteed in the EU Charter of Fundamental Rights and the European Convention of Human Rights.

Furthermore and in addition to the lack of clarity regarding the compliance with the aforementioned data protection requirements, this option seems to run contrary to the current prerequisite for the application of Article 32 b) of the Cybercrime Convention, namely the need to obtain the "lawful and voluntary consent of the person who has the lawful authority to disclose the data".

Scenario 18

Power of disposal as connecting legal factor in situations where territoriality cannot be determined A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device or the police has obtained the access credentials during a lawful search. The suspect does not consent. It is not known where the data is located. The data may be moving or fragmented over different locations/jurisdictions. Or the provider doesn't know where the data is located. Can the police carry out the search under domestic procedures (possibly with a court order) since territoriality cannot be determined based on the fact that the suspect is under the jurisdiction of the police and has the power to dispose of the data?

See scenario 15.

[39] See WP 29 letter of 5 December 2014.