Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Data retention in the States Parties to the Budapest Convention on Cybercrime

Survey report 2020

This project is funded by the European Union and the Council of Europe and implemented by the Council of Europe

Contact
Giorgi JOKHADZE
Project Manager
Giorgi.Jokhadze@coe.int
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania

Disclaimer

This document has been produced as part of a project co-funded by the European Union and the Council of Europe, with inputs from experts Hein Dries (Netherlands) and Marko Juric (Croatia). The views expressed herein can in no way be taken to reflect the official opinion of either party.

Table of Contents

1 INTRODUCTION 3

1.1 Background of the report 3
1.2 Data preservation versus data retention 3
1.3 Differentiating data retention regimes 5
1.4 Current legal frameworks on data retention 6

2 CURRENT SITUATION WITH DATA RETENTION 8

2.1 No retention, Targeted, Blanket retention 8
2.2 Type of data and retention regime 9
2.3 Retention time 10
2.4 (Carrier Grade) Network Address Translation 11
2.5 Safeguards in data processing: Territoriality, Other 12

3 ACCESS TO RETAINED DATA 15

3.1 Overview of the situation 15
3.2 Circumstances in which authorities are empowered to access retained metadata 16
3.3 Categories of persons whose data can be accessed 18
3.4 Authorisation procedure 19
3.5 Method of accessing data 21
3.6 Notification 21

4 OVERSIGHT 23

5 INTERNATIONAL COOPERATION 25

6 CONCLUSIONS 27

ANNEX I - QUESTIONNAIRE 28

ANNEX 2 DATA RETENTION DIRECTIVE 2006/24/EC (INVALIDATED): ART. 5 32

1 Introduction

1.1 Background of the report

This report describes the results of survey of States Parties to the Budapest Convention on Cybercrime (hereinafter: The Convention) to update chapter 4 of the 2012 Cybercrime Convention Committee (TC-Y) Assessment of data preservation provisions of the Convention. The present report specifically focuses on situation in the States Parties to the Convention in relation to data retention, conscious of the fact that further guidance has been sought from the court in several pending cases.

The information contained in this report is based on a questionnaire (attached as Annex I) that was sent to all States Parties to the Convention. The survey ran in February-March 2020 and 33 State Parties responded:

- Argentina
- Armenia
- Austria
- Belgium
- Bosnia and Herzegovina
- Cabo Verde
- Chile
- Costa Rica
- Czech Republic
- Denmark
- Finland
- Georgia
- Germany
- Ghana
- Greece
- Hungary
- Israel
- Italy
- Latvia
- Lithuania
- Luxembourg
- Moldova
- Morocco
- The Netherlands
- Panama
- Paraguay
- Philippines
- Poland
- Portugal
- Romania
- Serbia
- The Slovak Republic
- Spain
- Ukraine

1.2 Data preservation versus data retention

Firstly, it is important to note that the Convention does not mandate data retention, instead focusing on preservation of computer data that "has been stored by means of a computer system". Whereas the Convention addresses access to data, data retention allows for the storage of certain traffic data according to a (supra)national retention regime. The Explanatory Report to the Convention[1] draws a very specific line in this regard:

"Data preservation" must be distinguished from "data retention". While sharing similar meanings in common language, they have distinctive meanings in relation to computer usage. To preserve data means to keep data, which already exists in a stored form, protected from anything that

[1] Explanatory Report to the Convention on Cybercrime, section 151, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b

would cause its current quality or condition to change or deteriorate. To retain data means to keep data, which is currently being generated, in one's possession into the future. Data retention connotes the accumulation of data in the present and the keeping or possession of it into a future time period. Data retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe."

The EU had implemented a Data Retention Directive[2] which has, however, subsequently been declared void[3].

The difference between these two concepts still appears to remain the source of some confusion and it is therefore useful to repeat the explanation that was given by the TC-Y in 2012:[4]

"Expedited preservation and data retention are different concepts.

(..) The two are considered complementary measures that can be applied in parallel or in combination or separately for different purposes. For example:

- *A data retention obligation enhances the chances that historical traffic, location and subscriber data that are to be preserved are still available*
- *If the automatic retention period is about to expire, a preservation order would allow to safeguard specified data in a specific investigation beyond this period*
- *Retained data may only be accessed in relation to serious crime, while preservation orders may be issued and electronic evidence subsequently be obtained in relation to any crime. It has been underlined that in case of cybercrime it may not be known at the early stages of an investigation whether or not this is a case of serious crime.[5]*
- *While data retention obligations refer to providers of "publicly available electronic communications services or of a public communications network within their jurisdiction", preservation orders may be issued to any legal or physical person holding data.*
- *Article 29 and 30 Budapest Convention allow for international preservation requests also to countries without data retention obligation."*

The following table – also taken from the 2012 TC-Y report, further clarifies the distinction between (expedited) preservation and data retention obligations as they were intended in the data retention directive.[6]

	Expedited preservation	**Data retention (directive)**
Aim	Provisional measure to preserve volatile electronic evidence to allow for time for formal measures to obtain evidence	Ensure that data is available for investigation, detection and prosecution of serious crime
Specified/ Automated	Specific order for specified data	Automatic retention of data
Type of data	Any data (including content data)	Traffic and location data and subscriber information (not content data, nor destination IP addresses, URLs, email headers, or list of cc recipients)
Purpose limitation	Any crime involving electronic evidence	Serious crime

[2] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[3] Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014)

[4] T-CY(2012)10, Assessment report, implementation of the provisions of the Budapest Convention, Adopted by the T-CY at its 8th Plenary (5-6 December 2012), p. 75

[5] An investigation of an apparently minor fraud case may reveal that an IP address is linked to a major transnational criminal operation

[6] TC-Y(2015)7, p. 76

Addressee	Any physical or legal person (not limited to service providers)	Service providers
Time period	Flexible: 90 days (renewable)	Specific retention period (6 to 24 months - to be specified in domestic law)

1.3 Differentiating data retention regimes

By and large, data retention regimes can be differentiated across several criteria. For the purpose of this study, the following aspects were taken into account in order to compare data retention regimes:

- The type of data retained and its level of detail and/or selection criteria applied to the data to be retained
- The cases in which data is retained. This can relate to all data of a similar type, related to all users (often called "blanket data retention") or more specific data that relates to time periods, regions, specific (identified) users (suspects or direct contacts, for example) or specific other conditions ("targeted retention")
- The retention period during which this data is to be retained
- The type of crimes for which this data can be accessed
- The conditions applied to the retention obligation in relation to
    - Storage type (where is data retained)
    - Territoriality (where can the data be stored geographically)
    - Security and data protection conditions

Further to these, questions around the embedding of the regime in the laws of the state parties were asked in relation to:

- Method and safeguards surrounding access to data
- Criteria that apply to requests for access
- Oversight mechanisms and safeguards that are provided in relation to retained data and access requests
- International cooperation in cases related to retained data

The survey aimed to receive as much detail around the regimes in force, in relation to the above aspects. To allow for further analysis, the contents of the applicable regime was also requested, allowing for further analysis. In cases where the responses were unclear, further analysis was undertaken – in so far as possible given language and other constraints - in order to enhance the data set.

A clear understanding of the differentiation between the retention criteria and access criteria may be helpful to understand the method applied. The first relates to data that will be physically retained in the network or elsewhere. The second relates to the access to this data by law enforcement in the course of an investigation.

In relation to the latter is should also be noted that the questionnaire was limited to crime and criminal justice. Surveillance powers and related issues surrounding national security were explicitly not part of the scope.

1.4 Current legal frameworks on data retention

The 2012 report already contained a section on data retention that was updated in 2015.[7] As was stipulated in the 2015 assessment: many data retention regimes in operation in state parties to the convention were created using the (now defunct) data retention directive as a reference or model. The directive served as an outline for data retention regimes that apply in the EU as well as elsewhere, despite it being invalidated. This updated report also addresses the state of play that arose after the *Digital Rights Ireland* judgement in relation to data retention.[8]

However, in December 2016, the Court of Justice of the European Union (CJEU) found that EU law prevents its member states from "general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication", finding that it can only be legal in certain circumstances and "solely for the purposes of fighting serious crime" such as protecting national security.[9]

The Courts' decision stipulates that data retention is only allowed under EU law if a targeted approach is taken.[10] It could be read that the approach that the court has in mind is similar to the way the Convention implements data preservation. The Court, however, is not clear about the precise definition of targeted retention that would be acceptable. Practitioners take this term to mean that limitations are to be introduced in the data retained in relation to several aspects. Some argue for more and some for less of the following aspects of targeting to be applied:

a. Time (not all data is retained all the time)
b. Type of case and data (not for every type of criminal case can every type of data be retained or accessed)
c. Type of communications (not all aspects or all communications related data are retained)
d. Type of users in relation to whom data can be retained (only certain categories or types of users can be targeted)

Voicing privacy concerns in the digital era, privacy practitioners and civil society have resisted several implementations of data retention obligations, in view of their implications in relation to the right to privacy. Several EU member states have resorted to amendments and alterations of their data retention regime as a result of the aforementioned case law, as well as societal pressure.[11] It can be concluded that many member states are reluctant to fully abandon data retention.[12]

Regardless of the precise regimes that are in force in the EU, it can be said that in many countries the legal situation around a retention regime has become uncertain in many respects. As a result of the courts' decisions, a societal debate was often triggered in many countries, both in the EU and beyond, leaving data retention and its use for cybercrime investigations in a state of flux. On top of that, a case is currently pending in the CJEU regarding the French, Belgian and UK data retention regimes.[13]

---

[7] TC-Y(2015)7, Assessment report, Assessment report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime Follow up given by Parties, Adopted by the 13th Plenary of the T-CY (15-16 June 2015)

[8] Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014).

[9] Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016)

[10] In the judgement the Court argues that: "(..), Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary."

[11] For an early overview of the situation in 2017 see: https://fra.europa.eu/en/publication/2017/data-retention-across-eu

[12] Cf. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-frr-chapter-6-infosoc.pdf

[13] Cases concerning preliminary rulings requested by the French Council of State (joined cases C-511/18 and C-512/18, La Quadrature du Net and Others), the Belgian Constitutional Court (Case C-520/18, Ordre des barreaux francophones et germanophone and Others) and the UK Investigatory Powers Tribunal (Case C-623/17, Privacy International).

On the other hand, member states of the Convention have recognized the central role of data in almost all investigations of serious crime. This role makes it critical that relevant agencies can lawfully access data for the purposes of their investigations in cases where this is a proportionate and subsidiary measure. For example, child exploitation investigations often rely heavily on access to data, as perpetrators primarily share information online. Similarly, many CEO fraud (Business Email Compromise) cases involve almost entirely digital evidence related to Internet addresses and email.

This raises the question how a specific combination of targeting measures can be implemented in practice, in a way that is both meaningful as a tool to fight (cyber)crime whilst maintaining sufficient safeguards and a sufficient degree of proportionality in relation to user privacy.

This report intends to provide a snapshot of the current situation, in order to provide insight into implementation of data retention obligations with States Parties to the Convention in relation to data retained by Internet providers, telecommunications providers as well as any related services. It is primarily intended to provide an overview that is beneficial for the work of the 24/7 contact network that was created under Article 35 of the Convention and hence mainly serves to provide practical guidance. At the same time, however, this report provides an opportunity to draw some conclusions as to the impact of the CJEU cases in 2020.

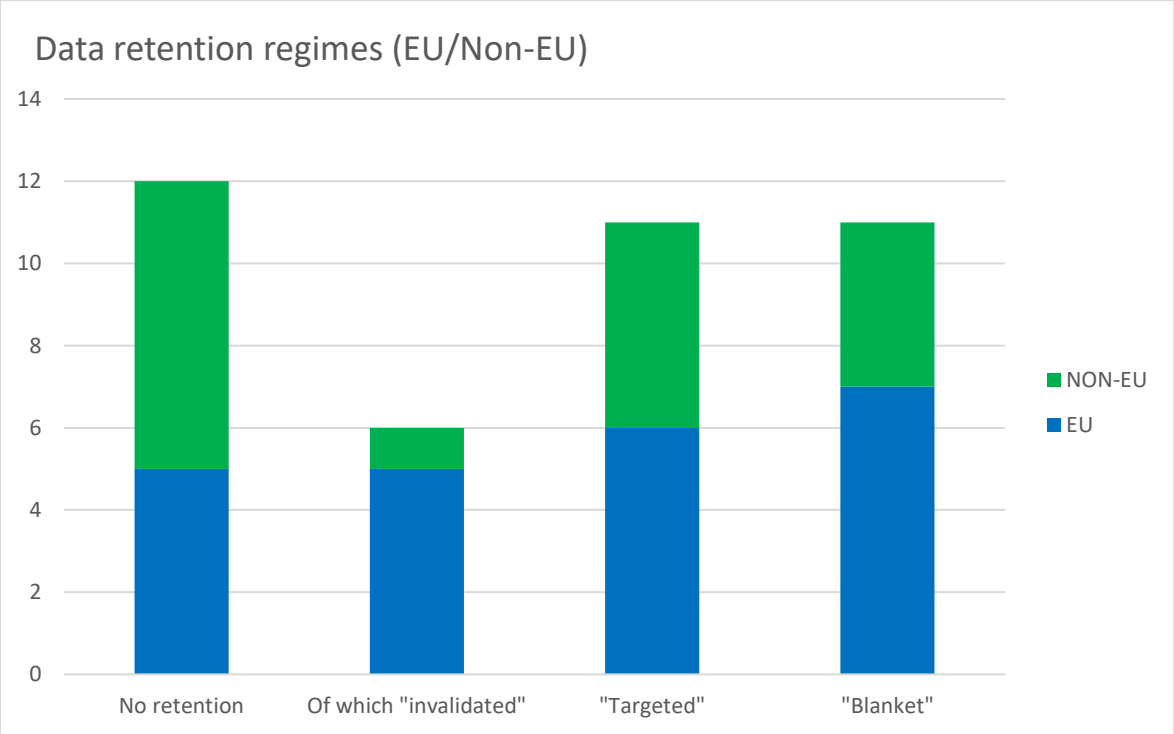
2 Current situation with data retention

2.1 No retention, Targeted, Blanket retention

In view of the Tele2/Watson case, member states were asked if they have a data retention regime in place and whether this is a targeted or "blanket" retention obligation, when they answer in the positive.

In the following graph the answers of the 33 state parties are represented in green (non-EU members) and blue (EU members). This subdivision was made in view of the fact that the Tele2/Watson case only applies directly in the EU.

The bars list the total number of state parties that have, respectively, no data retention regime in place (12), a so called "targeted" regime (11) and a so called "blanket" regime (10). Note that the category of invalidated retention regimes (5) is a subset of the total amount of countries without a retention regime.



A first observation from this data is that around two thirds of the respondent states have some form of data retention in place. From the 12 countries without data retention, several non-EU countries are working on implementing a form of data retention in the near future.

In the EU, however, where several data retention regimes have been invalidated both at the EU and national levels, the situation is made more complicated by the consequences of the Tele2/Watson judgement. 5 countries have seen their regime invalidated as a result.

The judgement provides only a limited insight into the actual requirements of a proportional and subsidiary retention regime. The main difficulty revolves around the "blanket nature" of the original data retention regime from the invalidated 2006/24/EC directive, which clearly proscribed that all data of a certain type should be retained for a certain retention period (between 6 months and 2 years).

In terms of targeting, none of the respondents indicated a type of targeting that is based on a form of "preselection" of data, meaning that instead of retaining traffic data from all users, some form of selection criterion would be used (such as type of service, person involved, time or location). This type of targeting is clearly not considered.

From a practical perspective this is perhaps understandable. In these investigations, more often than not, a crime is committed by an anonymous user that can only be identified through the use of previously retained data that can serve to link a specific IP address and connection time to a

specific user. This requires the retention, also of non-suspects data. Similarly, this data may also serve "à décharge" meaning that it is often used to identify innocent parties in order to focus an investigation on more relevant suspects.

Although the court clearly invalidates the Swedish and UK laws on data retention in the case, the "targeted" retention it introduces is also a source of controversy: a strictly targeted approach that limits itself to retention of suspects data in cases where a suspicion or order against a person exists is clearly not-fit-for-purpose when it comes to day-to-day cybercrime investigations.

On top of that, a case is currently pending in the CJEU regarding the French, Belgian and UK data retention regimes.[14] As a result 5 EU countries are making do without a data retention regime, out of the 33 respondents (which includes 18 EU members).[15] All of these 5 responding EU member countries saw their retention regime invalidated as a result of the CJEU judgements and/or local court actions.

Other EU countries have therefore sought to refine their regime more, and achieve a better balance between access criteria and safeguards. In these cases, countries sometimes resort to using the term "targeted" in reference to the revised legislation. A total of 11 respondents (6 of whom are EU members) refer to their retention regime as "targeted".

The remainder, perhaps in view of the absence of "preselection" criteria in the retention phase, refer to their regime as applying "blanket retention".

2.2 Type of data and retention regime

The attached questionnaire made a subdivision in several types of retained traffic data and the related retention period:

- Telephony data
- Internet data
- Location data
- Subscriber information

From analysis of the available data and the actual retention regimes in place, the image arises that the specific data to be stored, inside and outside of the EU is often based on the original EU data retention directive:

- For internet access the most common data stored are identifier, IP address and address allocation time. In some cases, the allocated TCP/UDP port number is also registered in order to overcome issues involving Network Address Translation.
- For telephony originating and destination telephone numbers together with connection times and relevant identifiers in mobile networks (IMSI, IMEI) are common.
- For location data a lot less information was given but Cell ID seems the most common.

All this data is then linked to the subscriber involved and thus is required to be linked (through the use of the relevant identifiers operational in the network) to the relevant subscriber data.

The 13 EU members out of the 33 respondents that have an active data retention regime, by and large, still apply the type of regime that was described in the data retention directive.

[14] Cases concerning preliminary rulings requested by the French Council of State (joined cases C-511/18 and C-512/18, La Quadrature du Net and Others), the Belgian Constitutional Court (Case C-520/18, Ordre des barreaux francophones et germanophone and Others) and the UK Investigatory Powers Tribunal (Case C-623/17, Privacy International).

[15] It should be noted that in Germany, whilst a regime is in place "de jure", it is not enforced by the supervisory authority (Bundes Netz Agentur) following a (regional) court case .

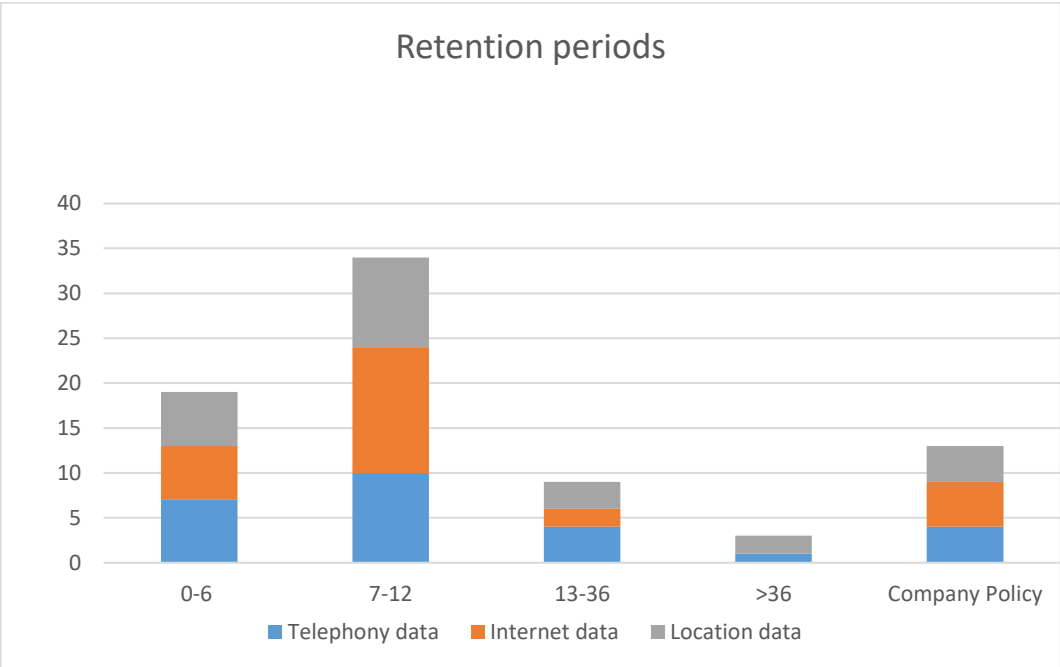
2.3 Retention time

For each of the categories of traffic data the retention period was asked. The following table outlines the answers received:

Data retention: retention times per type of data					
Retention period (months) Data type	0-6	7-12	13-36	>36	Company Policy
Telephony data	7	10	4	1	4
Internet data	6	13	2	-	5
Location data	6	10	3	2	4

Subscriber data usually has a retention period equal to, or longer than the longest retention period of any of the traffic data.

In the countries where there is a data retention regime, the most common retention regime dictates a retention time of **12 months** across all types of data.[16] In some cases the retention time is shorter, whilst longer retention periods are much less common.



Differentiation in the retention period, based on data type is seen only in 4 countries, only 2 of which are EU members. In these cases, the retention of Internet related data is shorter whereas telephony and location data are kept longer.

The limited use of differentiated retention periods is surprising given the need for a targeted approach that appears to follow from the Tele2/Watson judgement. From a privacy perspective one could argue that internet related data is particularly intrusive. In potential it is registered at many more destinations and relates to many personal interest and /or contacts. At the same time, convergence of services and the advent of many over-the-top internet services may make that this differentiation is less frequently chosen.

Lacking targeting based on retention periods and data type, the question can be asked how targeting can be implemented otherwise, without turning to a "preselection" of data to be retained.

Further targeting could also - for example - be related to specific data types. One can imagine, for example, that certain Internet related traffic data is more invasive than others, especially in relation to Internet access.

[16] Only in one case does the category of 7-12 months retention list a 9-month regime.

In that category a distinction could be made between traffic data reflecting the originating IP address used for a connection versus the IP addresses or even URLs (domain names and directories) that were visited on websites. Whereas the first is usually sufficient to trace back the user of an IP address at a given moment in time (sometimes including some extra information related to NAT), the second and third type of data will also form a picture of the users online behaviour and interests. Some argue that this type of data is no longer traffic data, yet pertains to content.

Article 5 in the invalidated directive originally read that only in a limited number of cases was the destination of internet related communications to be retained. In many data retention regimes the same or similar wording is still found:

> *Concerning Internet e-mail and Internet telephony:*
>
> (i) *the user ID or telephone number of the intended recipient(s) of an Internet telephony call;*
>
> (ii) *the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;*

This means that only for those specific media (VOIP and email) did the directive ever mandate the registration and retention of the destination of internet related traffic data.

In relation to internet related data, the study therefore asks if the data retention regime still required providers to keep track of this "destination" data. If there is a requirement to retain destination data, it is asked if there is a requirement to store this data at the level of either IP address or URL or otherwise.

Out of all 21 respondents (out of which 14 are EU members) with an operational data retention regime, 5 (of which 3 EU members) replied that some form of internet destination data (either at the level of IP addresses connected to, or even URLs) is part of the regime.

A further study of the regimes of the countries concerned, however, found that in three cases of these five, the law in force does not appear to contain such a requirement. These three members are all EU member and the regime described above (from the invalidated directive) seems to be in force: only the IP address allocated by the internet provider (source address) is to be retained, not the addresses that will be connected to (IP nor URL).

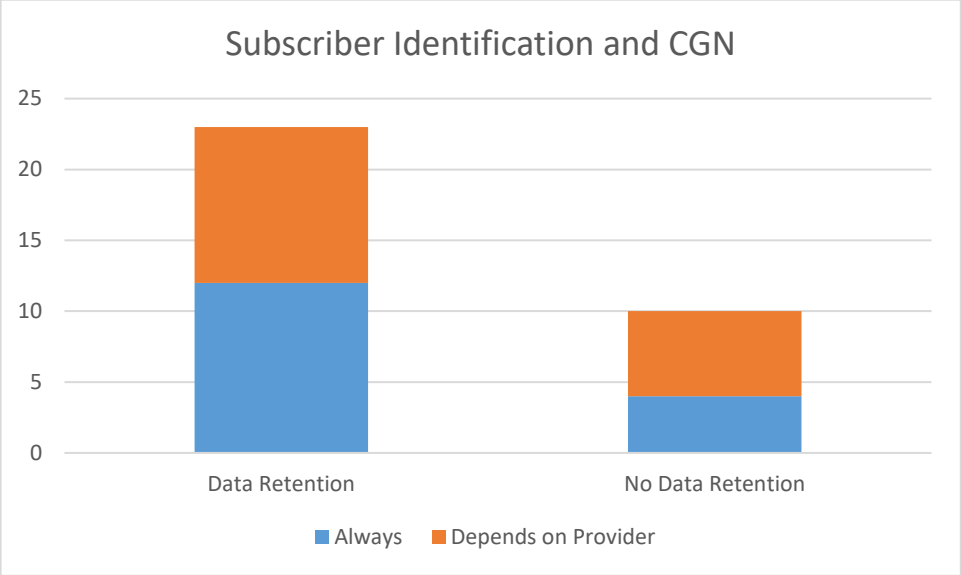
The remaining two responses were not investigated further, due to language constraints and/or the limited data provided.

2.4 (Carrier Grade) Network Address Translation

A specific problem that has arisen since the advent and invalidation of the data retention directive is network address translation. If a applied at the scale of a carriers network, the result of this technology is that a large number of users will share a single public IP address.[17] The only identifier that will set users of this single address apart, in these cases, will be the port number that is allocated to the device by the service provider next to the address. Together with a precise time of usage of this IPv4 address/port combination, there is still a possibility to identify the source of a communication at the level of an individual end user device.

Many countries indicate that the technology is used on their territory and that it is most prevalent in mobile networks. Due to the relative scarcity of IPv4 addresses on these networks and the relatively short time of TCP-IP connections that are established (addresses are often allocated for a short period of time only in order to save channel capacity on the radio) the technology is not free of challenges, as the next graph indicates.

[17] For a full explanation of the technical aspects of NAT and user identification see, for example, Wikipedia: https://en.wikipedia.org/wiki/Network_address_translation and Report for the EC, Allocation and Use of IP addresses, https://op.europa.eu/en/publication-detail/-/publication/5c8dc87f-6732-4a18-9d02-328658c27cf4



All the 23 respondents that have indicated having a data retention framework indicate that CGN is in operation in networks in the country. However, almost half of them (11) replied that identifying subscribers or suspects is often dependent on the specific network and service providers involved and the logging that is available on their network.

A similar picture arises in countries that work without a legal data retention regime: half (5) of the total of 10 respondents to the questionnaire that had answered this section indicate that CGN may lead to problems in identifying the subscriber behind an IP address.

An important observation is that after analysis of the underlying acts and administrative decisions, only 5 countries with a legal regime for data retention mention source ports as an identifier that is to be retained under the regime.

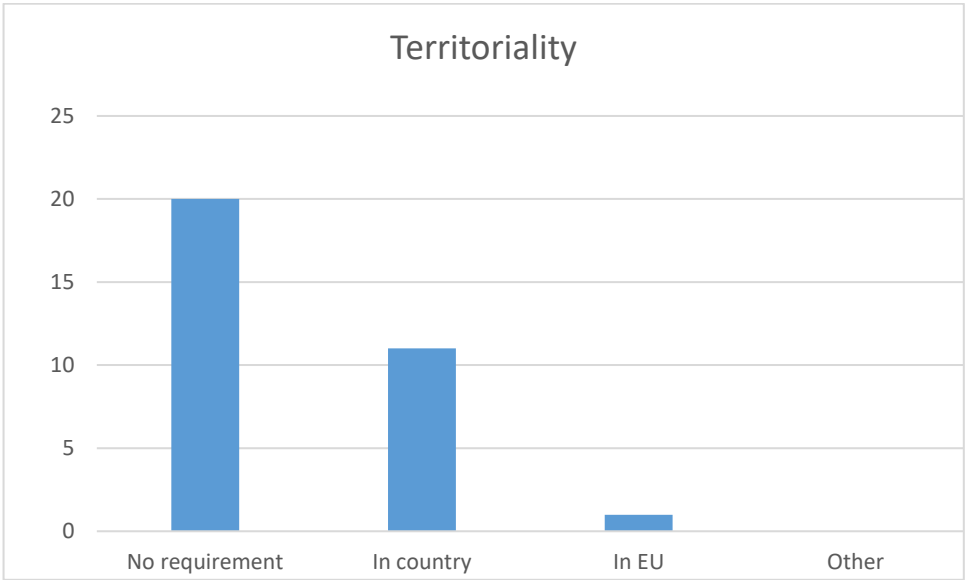
A noteworthy best practise was found in Finland, where CGN is limited to 64 users per IP address. If, in case an investigation does not produce an IP port number, yet does relate to several IP addresses, this will greatly limit the privacy impact and will enable easier cross-referencing of IP address use across several timeframes.

In several other countries the legislation in force appears to indicate that port ranges are allocated to users in order to ease the identification of subscribers on the basis of IP/port and time combinations.

2.5 Safeguards in data processing: Territoriality, Other

In the Digital Rights Ireland case, one of the safeguards that is mentioned by the court is the territoriality of the processing of traffic data. Indeed, the processing on a state's territory maximises the control it has over the processing, origin and access to the data.

The questionnaire reveals that a majority of state parties, however, do not have such requirement.



Further safeguards could relate to the security and standards that regulate the processing of the data itself. Although very specific standards and safeguards were created in relation to data retained for the purpose of criminal justice[18], the majority of the responding state parties have opted for a more limited regime that either applies requirements of the data protection domain or that attaches to the security requirements present in the telecommunications domain.

The privacy domain typically involves requirements related to:

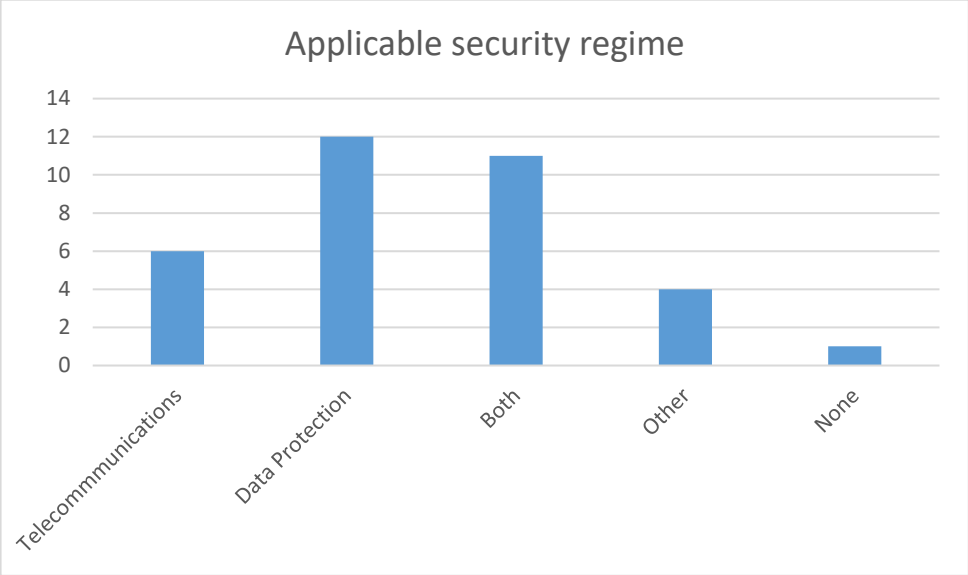
- Lawfulness, transparency and fairness of the processing
- Purpose of the processing and access
- Data Minimisation
- Data accuracy
- Retention periods and deletion of data
- Integrity and confidentiality of the data
- Accountability

Furthermore, requirements from the telecommunications domain typically involve:

- Integrity and confidentiality requirements related to the networks involved
- Application of security measures
- Various requirements based on operating permits and/or general authorization schemes
- Specific rules related to processing of traffic and location data[19]

In many cases state parties chose to apply one or both of these generic regimes to the processing of traffic data that is the subject of a data retention regime. In 4 cases other, sometimes slightly more specific regimes apply, either in lieu of, or next to the generic regime(s) that stem from the data protection and telecommunications act:

[18] Cf. ETSI standard TF 102656, available at https://www.etsi.org/deliver/etsi_ts/102600_102699/102656/01.03.01_60/ts_102656v010301p.pdf
[19] CF the ePrivacy directive EU/2002/58.


Applicable security regime
14
12
10
8
6
4
2
0
Telecommmunications
Data Protection
Both
Other
None

3 Access to retained data

3.1 Overview of the situation

It is clear that both the data retention itself as well as their accessing interfere with fundamental human rights, most notably the rights to privacy and data protection. In such circumstances, rules of international law require that adequate conditions and safeguards be implemented at the national level.

Nevertheless, the scope of those conditions and safeguards is not completely harmonized. This is due to the fact that different international treaties are applicable to various parties of the Budapest Convention. Since the Budapest convention is a treaty which is open to accession also to states which are not members of the Council of Europe, some of its parties need to adhere to human rights standards which are different from the European ones. In general, we find it useful to differentiate between those countries which are (1) member states of both the European union and Council of Europe, (2) those which are members of the Council of Europe only, and (3) those countries which are members of neither the European Union nor the Council of Europe.

Of the member states in the third category, we note that they are from different continents, and consequently different regional treaties are applicable to them. Therefore, the following legal instruments can be applicable here:

- Charter of Fundamental Rights of the European (EU Charter)
- European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)
- International Covenant on Civil and Political Rights (ICCPR)
- American Convention on Human Rights (ACHR)
- African Charter on Human and Peoples' Rights (ACHPR)

In the context of this report, we received 34 replies, 10 of which (29,5%) from non-European states.

It might be useful to consider the following mapping of countries which submitted their replies to this questionnaire and applicable human rights treaties:

	EU	ECHR	ICCPR	ACHR	ACHPR
Argentina			✓	✓	
Armenia		✓	✓		
Austria	✓	✓	✓		
Belgium	✓	✓	✓		
Bosnia and Herzegovina		✓	✓		
Cabo Verde			✓		
Chile			✓	✓	
Costa Rica			✓	✓	
Czech Republic	✓	✓	✓		
Denmark	✓	✓	✓		
Finland	✓	✓	✓		
Georgia		✓	✓		
Germany	✓	✓	✓		
Ghana			✓		✓
Greece	✓	✓	✓		
Hungary		✓	✓		
Israel			✓		
Italy	✓	✓	✓		
Latvia	✓	✓	✓		

Lithuania	✓	✓	✓		
Luxembourg	✓	✓	✓		
Moldova		✓	✓		
Morocco			✓		
The Netherlands	✓	✓	✓		
Panama			✓	✓	
Paraguay			✓	✓	
Philippines			✓		
Poland	✓	✓	✓		
Portugal	✓	✓	✓		
Romania	✓	✓	✓		
Serbia		✓	✓		
The Slovak Republic	✓	✓	✓		
Spain	✓	✓	✓		
Ukraine		✓	✓		

Looking from a formal perspective, different states are under different legal regimes when it comes to the international protection of human rights and freedoms. Therefore, we recognize that conditions and safeguards applied in one country might be different from the other, since different national laws must satisfy different requirements under international law.

However, in broader sense, what we witness in recent years is increased internationalization in the collection, use and especially exchange of metadata between law enforcement agencies of different states. Therefore, there is also some merit in global outlook on these issues, in which binding international rules from one region are viewed at least as a good policy in other regions, if not as a binding law itself.

Moreover, it is not uncommon that highest courts take into account case-law from the counterparts in other jurisdictions, which also contributed to the globalization of key legal issues.

3.2 Circumstances in which authorities are empowered to access retained metadata

Currently there are no universally applicable rules in international law which would require a state to restrict access of its law enforcement authorities to retained data only in cases pertaining to some (serious) criminal offences. Still, we witness a clear trend moving in that direction in the European union law, as well as in the application of the ECHR.

For member states of the European union, 2006 Data Retention Directive[20] stipulated in its Article 1 that it "*aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available* ***for the purpose of the investigation, detection and prosecution of serious crime****, as defined by each Member State in its national law*" (emphasis ours). Although this directive was invalidated in 2014, the requirement that retained data should be used only for proceedings related to serious offences was accepted and further emphasized by the Court of Justice of the EU (CJEU).

Firstly, CJEU criticised Data Retention Directive in the *Digital Rights Ireland* case on the basis that, while recognizing that access to data should be limited to cases connected with serious crime, it nevertheless failed to "*lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be* ***sufficiently serious to justify such an interference***" (emphasis ours). The CJEU did not it consider it satisfactory that Data Retention Directive referred

[20] Data Retention Directive was invalidated in 2014

only to "serious crime" and left it to the member states to define the scope of these offences in their national laws.[21]

Secondly, in *Tele 2 / Watson*, dealing with national legislation mandating data retention, CJEU concluded that given "*the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data**, only the objective of fighting serious crime is capable of justifying such a measure***" (emphasis ours).[22]

Therefore, it follows clearly that parties to the Budapest Convention which are also member states of the European Union should limit access to retained data only to cases pertaining to serious criminal offences. However, notwithstanding criticism of the CJEU in *Digital Rights Ireland,* due to the lack of harmonization regarding the notion of "serious offence" there still remains a margin of discretion for member states of the EU in defining what is to be considered serious offence.

Turning now to broader international legal framework, we emphasize that under ECHR every interference with the right to private and family life, home and correspondence (protected under Article 8) must (1) pursue legitimate aim, be (2) in accordance with the law and (3) necessary in a democratic society.

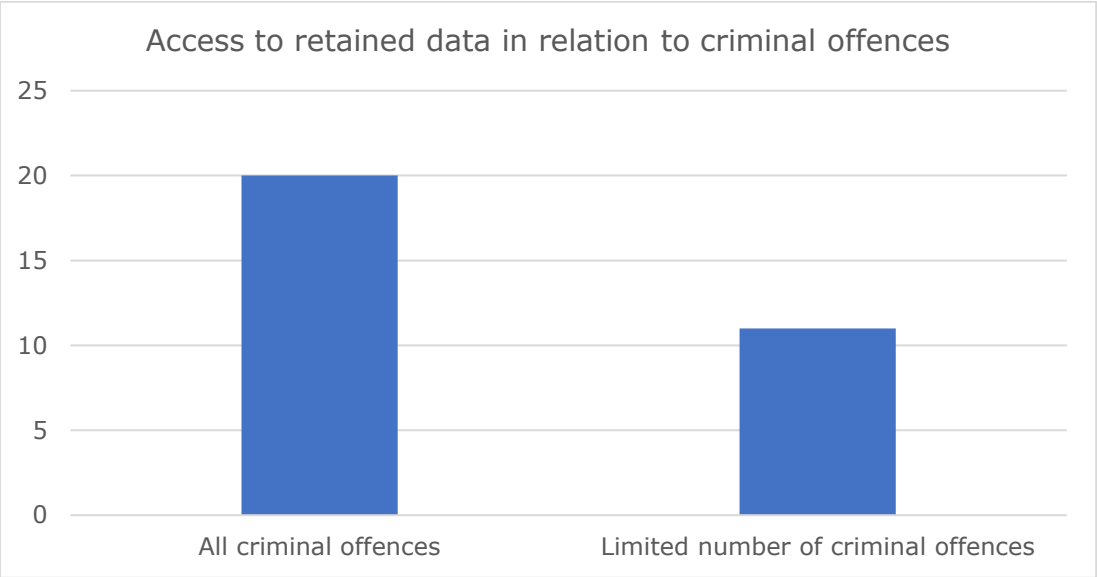
Although the European Court of Human Rights (ECtHR) is yet to face cases concerning retention of communications data generally, and conditions for lawful access to such data more specifically, there is no doubt that the requirement of necessity of democratic society encompasses the application of the principle of proportionality, application of which should take into account the gravity of offences in relation to which access is requested. This is particularly true if access to retained subscriber, traffic and location data is viewed in analogy to surveillance of content data, where the ECtHR has developed an extensive practice which considers the gravity of an offence as one of the factors to be considered when addressing compliance of national law with the ECHR.[23]

This analogy between content data and metadata is not misplaced, since it is increasingly accepted that collection and use of metadata can give rise to serious concerns in the context of human rights. This is explicitly recognized by the CJEU, which explained in *Digital Rights Ireland* that "*those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*".[24]

Moving our focus outside Europe,[25] we note that the most universally accepted instrument on human rights – ICCPR – regulates protection of privacy broadly in line with European solutions. Still, due to the fact that individuals have only limited possibilities to claim protection under the ICCPR, and that the enforcement mechanism is not on the same level as with the ECHR and the EU law, general principles defined in its Article 17 are not so developed in practice (especially in comparison with ECHR and other regional human rights treaties). Therefore, while there are various opinions and commentaries on this issue, we lack specific and binding legal rules applicable to present issues (access to retained data) under the ICCPR.

In the questionnaire, we sought information about scope of power to access retained data under national law. The distribution of answers is in the graph below:

[21] Digital Rights Ireland, para 60.
[22] Tele 2, para 102
[23] See for instance in *Roman Zakharov v Russia*, para 243 et seq.; *Iordachi and others v. Moldova*, para 41 et seq.
[24] Digital Rights Ireland, para 27.
[25] For broad analysis of applicable legal framework on international level see, inter alia, St. Vincent, Sarah, International Human Rights Laws Concerning Systematic Government Access to Communications Held or Transmitted by the Private Sector, in: Fred H. Cate, James X. Dempsey (eds), Bulk Collection: Systematic Government Access to Private-sector Data.



In short, the majority of states which retain metadata allow access and use by the law enforcement in relation to any criminal offence; states which limit the use of these data to some scope of criminal offences represent approximately one third within the responses we received. Moreover, 9 states which are members of the European Union still use metadata for investigations of all criminal offences, without regard to their seriousness.

Within the states which do restrict access, the states rely on the criterion of seriousness of offence, viewed in terms of the penalty prescribed in law, sometimes combined with enumerating additional offences which are considered serious due to some other factors (see for instance in Czech Republic, Slovakia, Finland). Majority of states which restrict access in this way include all criminal offences defined in the Budapest Convention within the list of offences for which access is possible.

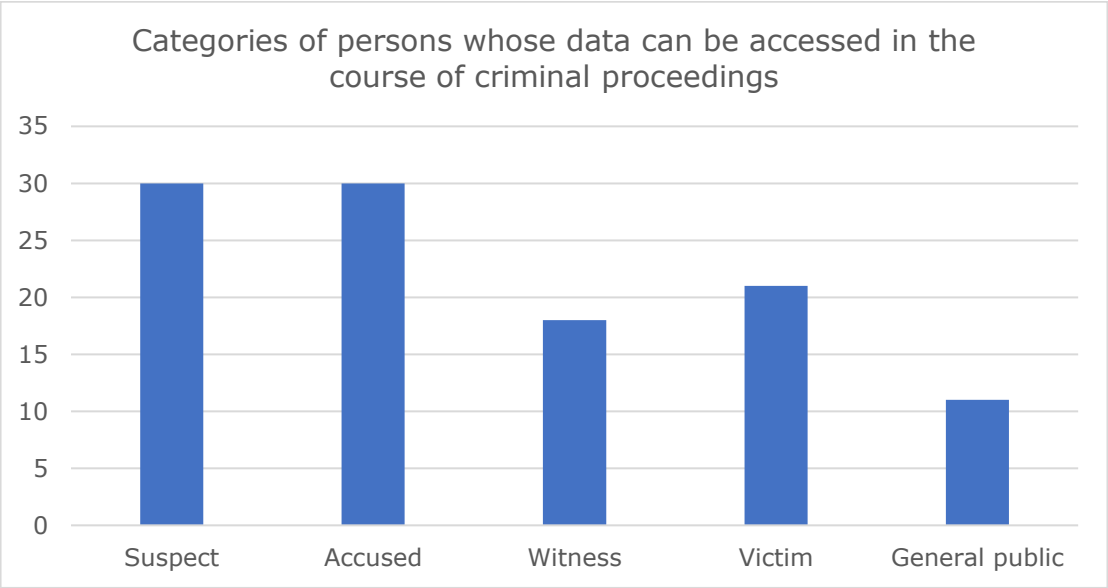
In Denmark, there is a differentiation between traffic and location data, with the former available for limited number of offences and the latter for all criminal offences.

3.3 Categories of persons whose data can be accessed

Foreseeability regarding scope of power to access data, in relation to persons (potentially) affected is one of the criteria to be considered when assessing compatibility of national law with international human right requirements. Recognizing that different states have different approaches in this regard, in the questionnaire we asked respondents to provide us with the information about categories of persons whose retained data can be accessed in the course of criminal proceedings, and the following options were offered: Suspect, Accused, Witness, Victim, Members of the general public, Other.

We emphasize once again that the purpose of this report was to analyse access to data in the context of criminal proceedings. Therefore, answers of some parties which offered additional explanations about possibilities of accessing data in the context of police duties and powers, as well as in intelligence and security operations, were not considered in this analysis.

The answers we received can be summarized as follows:



Almost all the surveyed countries allow access to retained data of persons who are, depending on the stage of criminal proceedings, considered as either suspect or the accused. A majority of states also allows accessing witness's or victim's data, with some differentiation between states for which such access is possible *ex lege* and others where it requires consent of the person affected. Finally, a minority of states also allows their law enforcement authorities to access data of persons from the public, namely those who do not fit in one of the aforementioned categories.

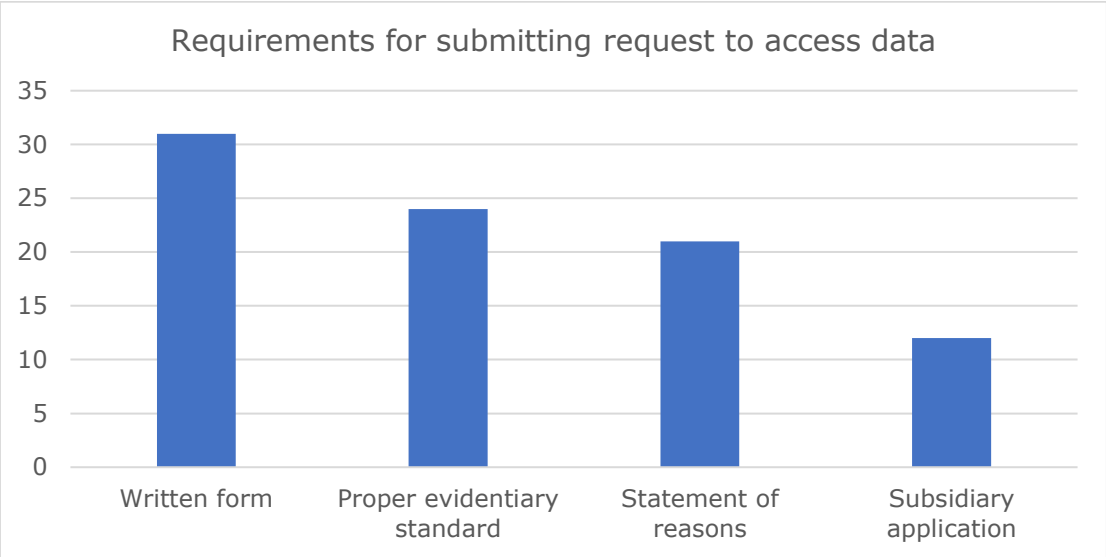
3.4 Authorisation procedure

The authorisation procedure is one of the important guarantees against arbitrary and unlawful intrusions in the private sphere of individuals. In this context, we analysed formal and substantive requirements applicable to request to access data in every country, authorising body and requirements regarding the decision which authorizes access in the final turn.

Regarding the formal and substantive requirements for a request to access data under national law, the following options were offered:

- It must be in written form,
- It must show reasonable suspicion or satisfy some other evidentiary standard,
- It must contain statement of reasons,
- It must explain why the measure cannot be achieved using less intrusive means,
- Other (please explain).

The distribution of answers is as follows:



To begin with, we note that most countries implement more than one of the abovementioned requirements. Almost all countries require that an order to request data is submitted to the authorizing body in written form, with only one country reporting the possibility of submitting an oral request, and this only in urgent cases.

Similarly, most countries require that explanations regarding reasonable suspicion or other legal standard applicable under national law are provided already in this phase.

In more than half of the countries require statement of reasons demonstrating the need to access data is mandatory.

Finally, approximately one third of the surveyed countries allow access to data as a subsidiary measure, to be used in those cases where the aim pursued cannot be achieved using less intrusive means.

The most important insight regarding this issue is that most countries indeed have formal procedures in place, typically contained in codes on criminal procedure and laws regulating telecommunications / electronic communications. On the other hand, it is also obvious that only approximately one third of the surveyed countries allows access to metadata as a subsidiary measure, which is a standard usually applied in relation to interception of content data.

Therefore, it seems evident that, notwithstanding recognition in the case-law of CJEU that use of metadata is in a sense comparable to interception of content, most countries still differentiate in substantive requirements between access to content and metadata.

Turning now to the authorising body, the following options were offered in the questionnaire:

- Investigator,
- Prosecutor,
- Court,
- Investigating judge,
- Police officer,
- Other (please explain).

On the basis of answers received, it is obvious that most countries place the final decision on granting access with the judicial bodies (court or investigating judge). Only a minority of countries report possibility of accessing data on the basis of (solely) investigator's or prosecutor's request.

There are also countries where authorizing body is different, dependant on the kind of information sought. For instance, in Chile subscriber information can be accessed with a prosecutor's order, while access to traffic data requires a court order. Similarly, in Italy a differentiation exists between static and dynamic IP addresses.

Also, some countries report that in urgent cases it is possible to access data on the basis of investigator's order, with subsequent judicial authorization. For instance, in Denmark, in urgent situations where the purpose of the specific limitation might otherwise be endangered if the police

were to await the ruling of the court, the police are authorised to access data immediately, and the similar approach is followed in Luxembourg and The Czech Republic as well.

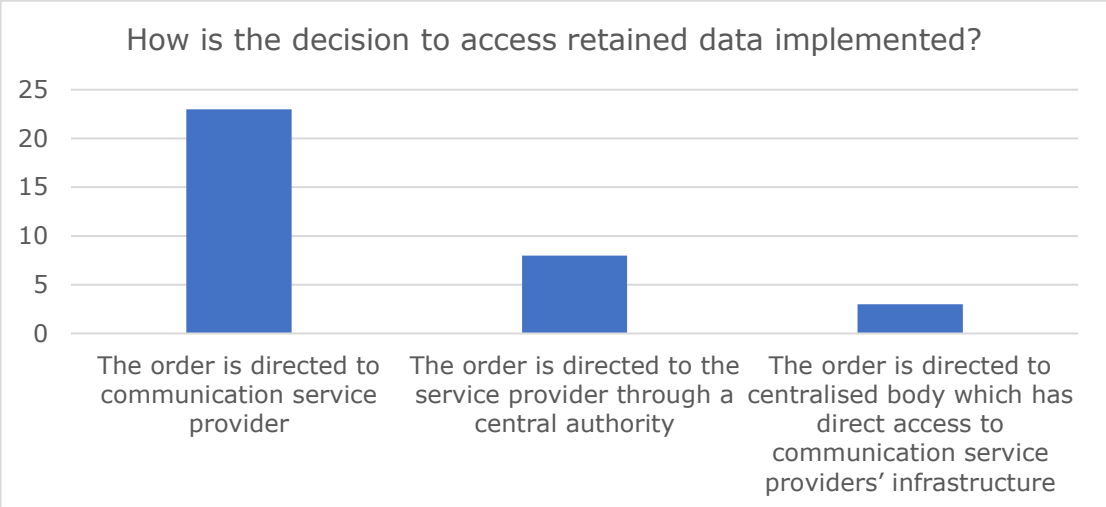
3.5 Method of accessing data

Next, we analysed how is the decision to access retained data is implemented. The following options were offered in the questionnaire:

- The order is directed to communication service provider, who is then obliged to deliver data;
- The order is directed to the service provider through a central authority and/or to a single point of contact at the provider;
- The order is directed to centralised body which has direct access to communication service providers' infrastructure, and the data is then retrieved by this body;
- Other (please explain).

This issue is important since the possibility of accessing data directly, without involvement of the service provider, gives rise to the additional threat of abuse. As explained by ECtHR in *Zakharov* case, "*the requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of interception*".[26] On the contrary, if it is technically possible to access data without proper legal authorization, it is necessary to implement additional safeguards in order to ensure adequate protection of human rights.

In response to the questionnaire, we received the following answers (summarized):



Majority of states report that the method of accessing data is either by requesting them from the service provider directly or through the central authority (sometimes both options are available). On the other hand, only three countries reported the existence of direct access with the possibility of retrieval of information from the provider's infrastructure.

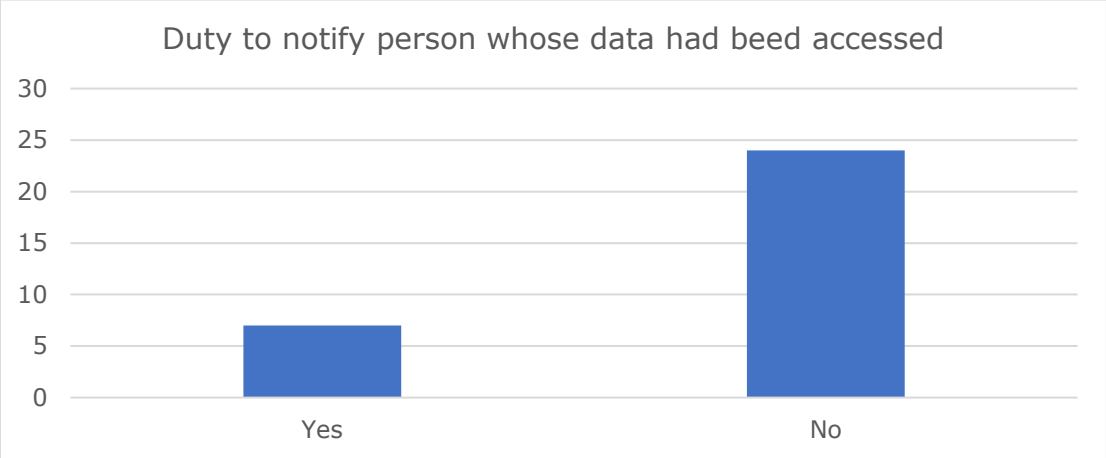
3.6 Notification

As elaborated by the ECtHR (although admittedly in the context of interception of content), notification of persons who were under surveillance is an important safeguard against abuse since it allows those persons to seek further remedies. While it is accepted that in certain cases notification can be delayed for operational and other reasons, the ECtHR nevertheless takes the position that "as soon as notification can be carried out without jeopardising the purpose of the

[26] *Roman Zakharov v Russia, para 269.*

restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned".[27]

On the basis that we consider use of metadata, in line with CJEU's legal position, to be comparable with the interception of content, we sought to establish the position of countries surveyed regarding obligation to notify. We received the following answers:

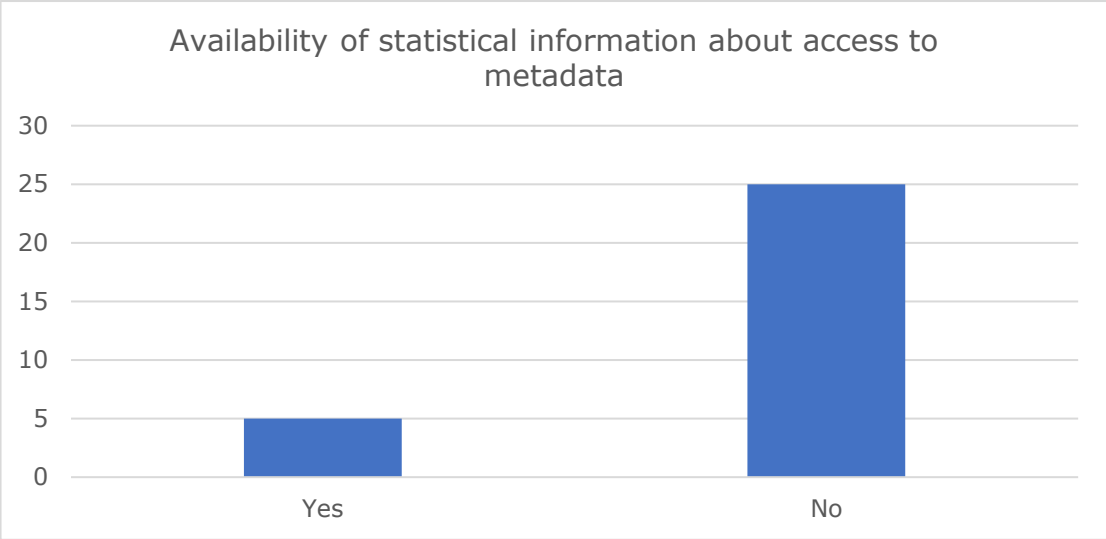


In short, some obligation to notify exists in 7 of the surveyed countries, while the other report that no such duty is present in their law.

[27] *Roman Zakharov v Russia*, para 243.

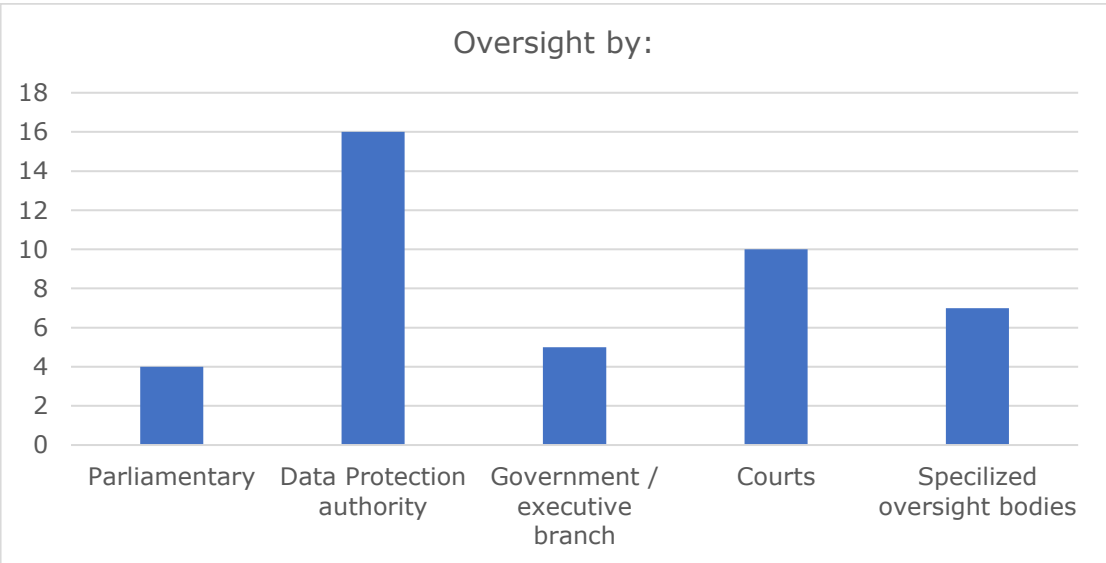
4 Oversight

Proper oversight mechanisms are necessary for any surveillance system, including access to retained metadata. Therefore, in the questionnaire we sought to obtain information about oversight applied in every country. The first criterion we used was the public availability of statistical data about cases involving use of metadata. On the basis of the answers received, we see that only a minority of countries makes such information publicly accessible; in a majority of them, this information is not open to the public.



One reason for the lack of proper information might relate to the fact that many states do not use any method of accessing data through central contact point or authority. Therefore, it is possible that information about the number of cases where metadata were used is not available to state bodies (since it would require collecting metadata from all service providers in a country). However, this also brings us to the next issue, which is effectiveness of oversight. Namely, if such data are not available and open to scrutiny, then it is more difficult to gain complete picture about the functioning of the system.[28]

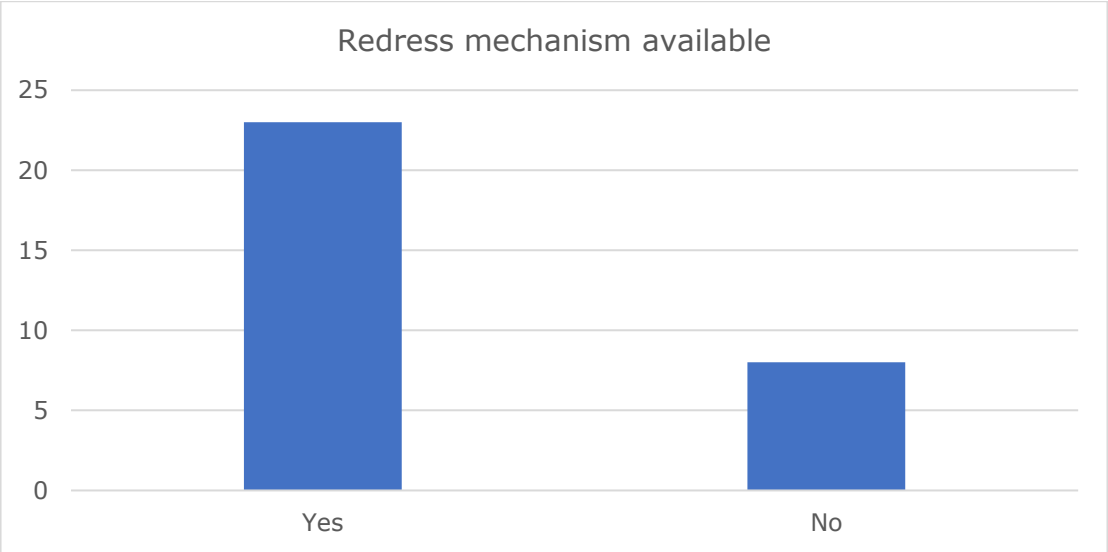
Also in this context, it is relevant what bodies within the state have the competence to perform oversight. The countries surveyed reported the following:



[28] This is in line with the approach taken by the ECtHR in *Youth Initiative for Human Rights v. Serbia*, where the Court considered failure to deliver statistical information about the number of people who had been subjected to electronic surveillance by state intelligence agency.

Once again, we note that many countries report that more than one body exercises oversight. For instance, in Belgium House of Representatives (Parliament) will receive yearly anonymised statistics on access to retained data; The Commission for the Protection of Privacy has the additional competence in oversight, and courts perform oversight in concrete cases.

We also note that many countries report oversight by their data protection authorities. The role of the courts is usually limited to an *in concreto* review in particular cases, and specialized bodies / functions take several different forms (internal control, *sui generis* entities, …).



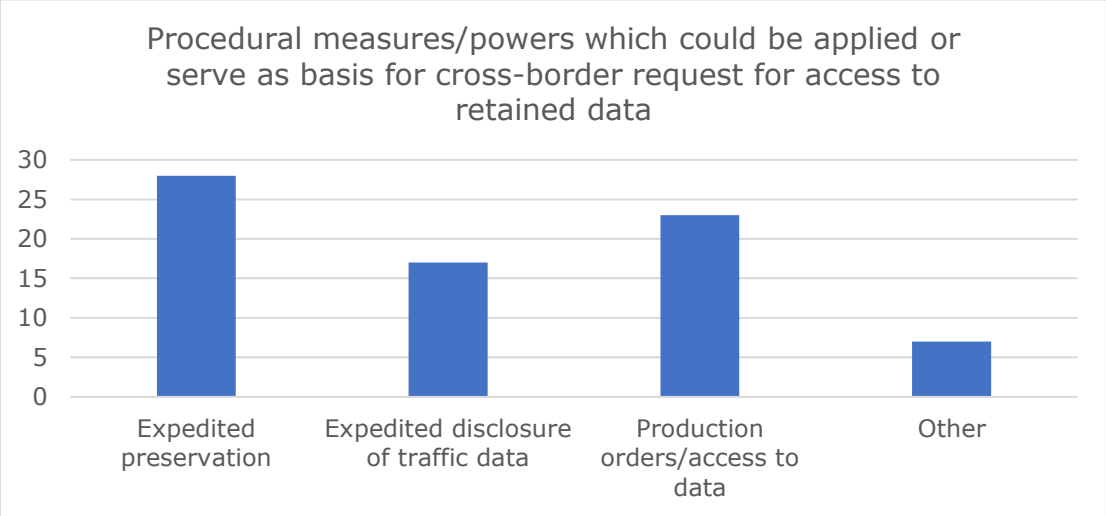
Finally, most countries report that individuals whose data have been accessed do have some redress mechanism available under national law. However, there seem to be many different mechanisms here, including i.e. the following: initiating criminal proceedings against responsible persons in cases of illegal access to data (Bosnia and Herzegovina, Costa Rica, Czechia, Greece, Moldova, Philippines, Slovakia, Spain), initiating proceeding before data protection authority (Chile, Bosnia and Herzegovina, Cabo Verde, Ghana, Hungary, Italy, Lithuania, Morocco, Serbia, Spain), liability for damages caused through an error or negligence in the exercise of public authority (Finland), administrative complaint (Netherlands).

5 International cooperation

In the final part of the questionnaire, we sought information about mechanisms for international cooperation regarding exchange of retained data. Firstly, we analysed the procedural measures/powers which could be applied or serve as basis for cross-border request for access to retained data. The following options were offered:

- Expedited preservation (Art. 29 Budapest Convention),
- Expedited disclosure of traffic data (Art. 30 Budapest Convention),
- Production orders/access to data (Art. 31 Budapest Convention),
- Other (please specify).

We received the following replies (aggregated):



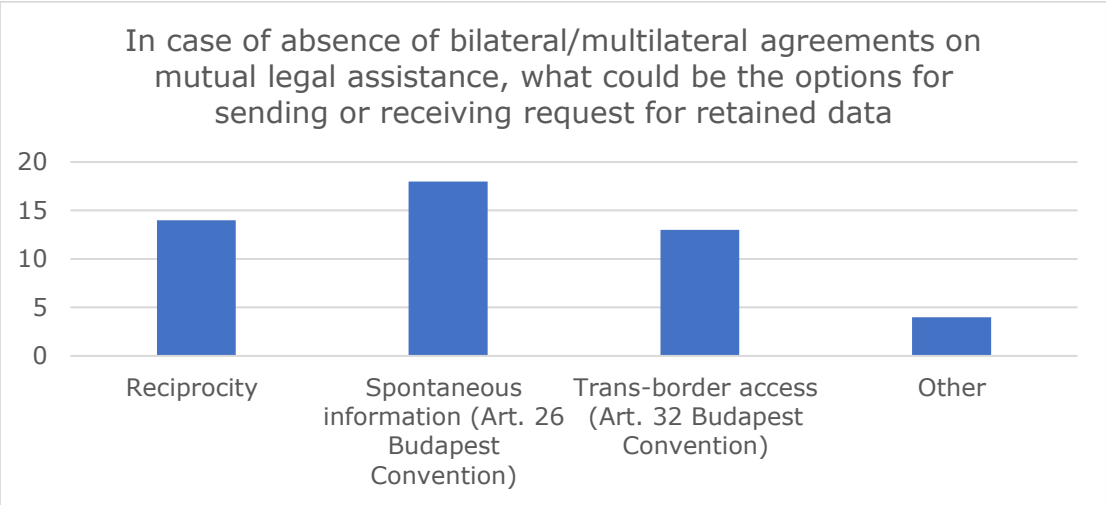
We can see from the graph above that most of the surveyed countries implement expedited preservation of data as well as access to data through the production order. Expedited disclosure of traffic data, in line with Article 30 of the Budapest convention, is possible in approximately half of the surveyed countries.

Next, we looked what would be the possible basis for sending or receiving request for retained data, in case of absence of bilateral/multilateral agreements on mutual legal assistance.

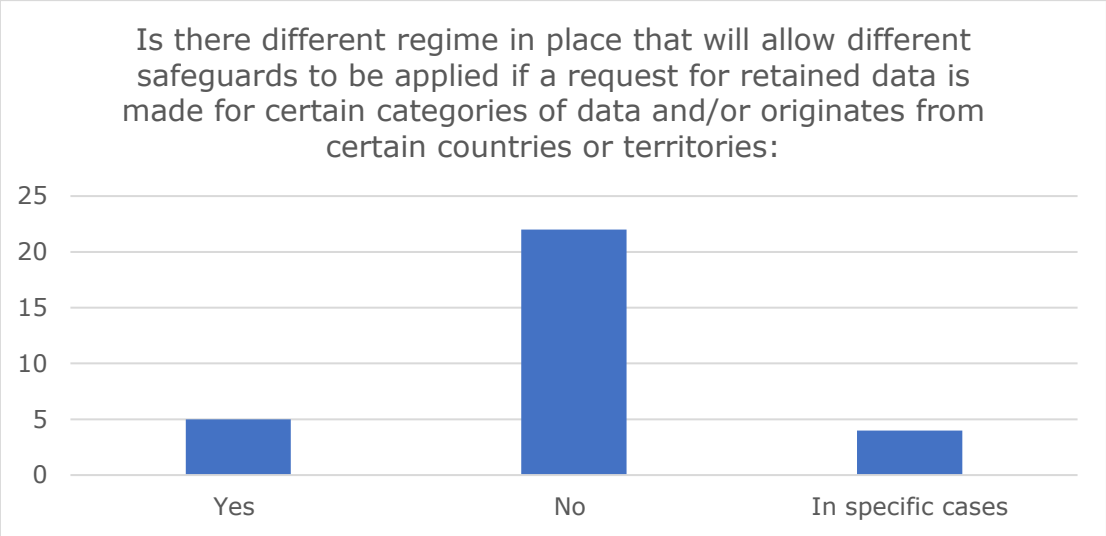
The following options were offered:

- Reciprocity,
- Spontaneous information,
- Trans-border access,
- Other.

We received the following aggregate answers:



Finally, there is the issue of conditions and safeguards applicable to a request for retained data is made for certain categories of data and/or originates from certain countries or territories. Distribution of answers is the following:



6 Conclusions

A closer look at the data types and retention periods reveals that there appears to be considerable uncertainty as to the way in which a sufficiently balanced ("targeted") regime can be achieved. On the one hand, few countries have chosen to create a regime whereby targeting based on the user, the time or the location is used as a preselection criterion for the data that will be retained. This is understandable given the crime involved: telephony, location and internet access data are used in a wide variety of investigations. Selecting the data that could be relevant to such an investigation in order to make the data set more "targeted" appears impossible from a practical perspective.

It is perhaps telling that the responding 5 EU members with an invalidated data retention regime have not come up with a way of achieving more "targeted" retention regimes. And instead this study reveals that the label of "blanket" versus "targeted" retention is applied to largely similar regimes. In other words: similar laws are qualified as either "targeted" or "blanket" by the responding state parties. In several cases countries began to describe their regime as "targeted" (usually after adjusting parameters such as types of data, safeguards and retention periods) yet have virtually similar regimes to other countries, who's regime is declared as being a "blanket retention" regime (whether or not it saw changes further to the Tele2/Watson case).

It would, perhaps, be best to forego these labels altogether and judge each regime on its merits. In relation to the data involved further balancing is often achieved by:

- A careful consideration of the retention periods and data categories.
- A differentiation of retention periods based on the intrusiveness and impact on privacy of the related data.
- A further fine tuning of the way data retention can be utilised in the case of carrier grade NAT (such as by limiting the number of users per IP or allocating distinct port ranges).
- Applying a better, more specific regime that applies to the process of retention and access itself, rather than generic requirements from the Telecommunications and Data Protection domains.

Further to this, the Tele2/Watson case provides many pointers both in relation to the data to be retained, as well as the safeguards that exist in relation to access and usage of the data.

In terms of procedural safeguards, we noted that surveyed countries need to adhere to relatively non-harmonized set of conditions under rules of international law. Most guidance here is provided under the EU law as well as under the ECHR. On the other hand, countries which rely on the ICCPR as the main human rights instrument are not provided with detailed requirements in terms of protecting fundamental rights and freedoms in the context of data retention. In such circumstances, it would be best to follow best policies from other countries, especially once which operate under EU law and the ECHR.

In terms of conditions, the most pressing issue is that the majority of countries still allow use of retained data in proceedings pertaining to any criminal offence. This is not in line with the trend in the EU law and ECtHR's jurisprudence, which seek to limit application of surveillance to a range of serious offences.

Next, we note significant differences in terms of substantive requirement to access metadata. While almost all states require written order, only about one third of them allow access only as a subsidiary measure.

Another issue which should draw attention is the obligation to notify persons concerned. It appears that only a minority of states uses this important safeguard. In the context of oversight, most countries report different mechanisms which are used to achieve this goal. However, statistical information about access to metadata by law enforcement authorities is mostly unavailable, which also reduces possibility of proper oversight.

In sum, we can conclude that regulation and practice of data retention in Budapest Convention member states remains a work in progress. Yet, the focus on defining targeted approach to data in line with recent jurisprudence as well as putting into action all relevant safeguards is the way forward to keep the data retention a viable and relevant option for cybercrime investigations.

ANNEX I - Questionnaire

Questionnaire – data retention study
The current questionnaire was created to update chapter 4 of the 2012 TC-Y assessment of data preservation provisions of the Budapest Convention on Cybercrime (hereinafter: The Convention). It was created to provide a good overview that is beneficial for the work of the 24/7 contact network that was created under the Convention and mainly serves to provide practical guidance.

Current legal framework: data retention
Blanket retention is defined, in this questionnaire, as the retention of all traffic data (irrespective of the categories of data, users and use case) in relation to all subscribers on the network.
Targeted retention means that limitations are put in place in relation to the types of (use) cases, the type of user, the type of communication and the type of data to be retained, and hence not all data is retained at some point in time.

1. A. Do you currently have a legal regime that requires the blanket, or targeted retention of certain types of traffic data?
    a. Blanket
    b. Targeted
    c. No data retention at all
    d. Other: (please specify)

–

– B. If you answered b: please specify the way that targeted data retention was implemented.

–

2. Please specify what data is retained according to this legal regime and specify the precise data and applicable retention period in the following table.

Category	**Data**	**Retention period**
Internet access	*For example: IP address, TCP port number, connection date, connection time, username or identifier etc.*	*For example: 6 Months*
Telephony	*For example: incoming and outgoing numbers etc.*	
Location Data		
Subscriber information		
Other (please specify, if not covered above)		

–

3. Please indicate if your retention regime includes the following data related to internet access services:
    a. Data pertaining to sites visited at the level of URLs
    b. Data pertaining to sites visited at the level of IP addresses
    c. Other data pertaining to internet usage (please specify):

–

4. A. Please indicate if Carrier Grade NAT is common in your country (in this IPv4 addressing scheme one public IP address is shared between numerous subscribers and a mapping is made from the single public address to the TCP/IP port number to identify the individual connection at the gateway):
    a. Yes
    b. No

    B. Please indicate if you are able to identify an end user if given a TCP/IP port number, time and date of an internet connection:
    a. Yes
    b. No
    c. Depends on the service provider involved (please specify if more information is available)

–

5. How and where is subscriber and traffic data to be retained:
    a. In provider infrastructure
    b. In a government owned system

c. Other (describe):

6. Is there a requirement for retained data to be stored and processed in your own country or any specific territory (such as "in the EU"):
    a. In the country
    b. In a specified territory (please specify):
    c. None of the above
    d. Other (please specify):

7. A. Please describe the relevant data protection standard that applies to retained data:
    a. Data protection law
    b. Telecommunications law (ePrivacy directive or other/similar)
    c. Specific protection requirements
    d. Other (please specify)

B. Please provide a short overview of the main requirements of the applicable regime (if other than data protection law based on the GDPR).

C. Please provide a link to the legal framework or a copy of the relevant legal regime.

Access to retained data

8. Please list all national statutes (acts) which regulate access to retained data

9. A. Is it possible to access retained data for:
    a. All criminal offences, or
    b. Some limited number of criminal offences

B. If you answered "b", please explain whether it is possible to access retained data when investigating offences defined in the Budapest Convention, namely:
    c. Illegal access
    d. Illegal interception
    e. Data interference
    f. System interference
    g. Misuse of devices
    h. Computer-related forgery
    i. Computer-related fraud
    j. Offences related to child pornography
    k. Offences related to infringements of copyright and related rights
    l. Dissemination of racist and xenophobic material through computer systems
    m. Racist and xenophobic motivated threat
    n. Racist and xenophobic motivated insult
    o. Denial, gross minimisation, approval or justification of genocide or crimes against humanity
    p. Other offences not covered by the Budapest Convention (please specify)

10. Categories of persons whose data can be accessed in the course of criminal proceedings according to your national law include:
    a. Suspect
    b. Accused
    c. Witness
    d. Victim
    e. Members of the general public
    f. Other persons (please explain)

11. Please explain what is the form and content of a request to access retained data:
    a. It must be in written form
    b. It must show reasonable suspicion or satisfy some other evidentiary standard
    c. It must contain statement of reasons
    d. It must explain why the measure cannot be achieved using less intrusive means
    e. Other (please explain)

12. Which authority approves requests to get access to retained data:
    a. Investigator
    b. Prosecutor
    c. Court
    d. Investigating judge
    e. Police officer
    f. Other (please explain)

13. What are the legal requirements for decision granting access to retained data?
    a. It must be in written form
    b. It must contain statement of reasons
    c. It must explain why the measure cannot be achieved using less intrusive means
    d. Other (please explain)

14. How is the decision to access retained data implemented?
    a. The order is directed to communication service provider, who is then obliged to deliver data
    b. The order is directed to the service provider through a central authority and/or to a single point of contact at the provider
    c. The order is directed to centralised body which has direct access to communication service providers' infrastructure, and the data is then retrieved by this body
    d. Other (please explain)

15. Does the national law require authorities to notify the persons affected that their retained communication data have been accessed?
    a. Yes
    b. No

    If yes, please explain how is the obligation to notify defined in national law (i.e., when should it be done, what is the scope of notification, …)

Oversight mechanism

16. Are the statistics about access to retained data by various law enforcement agencies available to the public?
    a. Yes
    b. No

    If yes, please provide statistics for the last available year
17. Which bodies perform oversight over the functioning of the whole retention / accessing system:
    a. Parliament /parliamentary committees
    b. Data protection authority
    c. Government / other executive bodies
    d. Courts
    e. Specialized bodies tasked with oversight function
    f. Other (please explain)

18. Please explain how your national oversight system functions (which bodies have competence, what is the scope of their competence, …)

19. In cases of illegal processing of retained data and / or accessing them contrary to the law, does the national law contain specific redress mechanism:
    a. No
    b. Yes (please specify)

International cooperation

20. Please provide some details regarding the regime that applies to requests for the above data in cross border investigations, both in terms of sending or receiving requests:

A. What are the procedural measures/powers which could be applied or serve as basis for cross-border request for access to retained data:
    a. Expedited preservation (Art. 29 Budapest Convention)
    b. Expedited disclosure of traffic data (Art. 30 Budapest Convention)
    c. Production orders/access to data (Art. 31 Budapest Convention)
    d. Other (please specify)

B. In case of absence of bilateral/multilateral agreements on mutual legal assistance, what could be the options for sending or receiving request for retained data:
    a. Reciprocity
    b. Spontaneous information (Art. 26 Budapest Convention)
    c. Trans-border access (Art. 32 Budapest Convention)
    d. Other (please specify)

C. Is there different regime in place that will allow different safeguards to be applied if a request for retained data is made for certain categories of data and/or originates from certain countries or territories:
    a. Yes
    b. No
    c. In specific cases (specify):

Please ensure that full text of all applicable provisions of national statutes is provided either as a URL or as an annex to your reply. Please provide an English translation where available.

ANNEX 2 Data retention directive 2006/24/EC (invalidated): Art. 5

Article 5

Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;
(ii) the name and address of the subscriber or registered user;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;
(ii) the user ID and telephone number allocated to any communication entering the public telephone network;
(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;
(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;
(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;
(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;
(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;
(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;
(2) concerning mobile telephony:

(i) the calling and called telephone numbers;
(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;
(iv) the IMSI of the called party;
(v) the IMEI of the called party;
(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;
(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;
(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.