Cybercrime@EAP III

Public/Private Cooperation under the Partnership for Good Governance with Eastern Partnership countries

2016/DGI/JP/3608
1 September 2017

Study on Liabilities of Internet Service Providers in the Eastern Partnership Region

Prepared by Council of Europe experts
under the Cybercrime@EAP III Project

www.coe.int/cybercrime

Partnership for Good Governance

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Contact
Cybercrime Programme Office of the Council of Europe (C-PROC)
Email cybercrime@coe.int

Disclaimer
This review has been prepared by independent Council of Europe experts Hein Dries-Ziekenheiner and Dave O'Reilly with the support of the Cybercrime Programme Office of the Council of Europe.
This document has been produced as part of a project co-funded by the European Union and the Council of Europe. The views expressed herein can in no way be taken to reflect the official opinion of either party.

Contents

1 Introduction

Cooperation between criminal justice authorities and private sector entities, including in particular service providers, is essential to protect society against crime. Such cooperation concerns primarily access by police and prosecution services to data held by service providers for criminal justice purposes, but also the sharing of information and experience, as well as training.

When it comes to access to evidence for the purpose of criminal investigations, the private business, including Internet Service Providers (ISPs), are expected to cooperate with the law enforcement without exceptions or concerns. This view, while it may be supported by the general legal framework, is more complicated in practice due to a multitude of factors, especially in the Eastern Partnership (EAP) region. For example, ISPs are also under other legal obligations, mostly sourced from the personal data protection legislation, to protect the privacy of their users; some sector-specific obligations, for example, require service providers to provide a certain level of consistent service. These requirements may often be at odds with the obligation to ensure cooperation with the law enforcement in the framework of criminal investigations. Electronic communications regulators in the EAP region, while being expected to be key players and facilitators of cooperation, are not always active of interested in resolving these conflicts of interest or serve as facilitators of public-private cooperation.

Even when every aspect of cooperation is laid out in law or regulations, there is always a practical side to cooperation. Non-cooperative business entities will relatively easily find ways not to cooperate in practice or delay the process so much that it becomes meaningless. Trust between the criminal justice system and the Internet industry is therefore a key factor, similar in importance to proper legislation or regulations. In this light, there can be genuine business interests and common goals that such entities can share with the law enforcement and cooperate with state authorities on a voluntary basis or as a matter of good business practice.

Taking into account the generally low level of understanding of the opportunities for cooperation with the private sector, the state agencies of the Eastern Partnership would greatly benefit from the extended overview of general liability framework applicable to the ISPs in the region, focusing on those regulations or practices that have potential relevance for investigation of cybercrime and access to electronic evidence in criminal cases.

2 Purpose and design of the study

Carried out under Result/Immediate Outcome 1 of the Cybercrime@EAP III project (*Analysis of current initiatives, challenges and opportunities regarding public/private cooperation in the Eastern Partnership region available*), this report offers insight into current problems and future opportunities for effective cooperation between the law enforcement in the EAP states and the Internet Service Providers.

The experts conducted desk research to understand the legislative and regulatory backgrounds of the various participant countries. This was followed by circulation of a questionnaire to the countries requesting clarifications and further information about legislative basis and practical matters. The experts analysed the responses and assembled this report.

3 Summary of recommendations

Recommendation 1: Information is not available about how well the arrangements for law enforcement access to ISP data are working in practice, but where practical shortcomings are identified, it may be advantageous for countries to consider less formal cooperation methodologies to address these. For example, if there are difficulties identifying which ISP to request data from, a single point of contact could be established for all ISPs to accept law enforcement access requests. The single point of contact can then work with the ISPs to route the request to the appropriate ISP for handling.

Recommendation 2: Upon receipt of a request from a competent authority, the scope and cost implications of the request may not be immediately apparent to either the ISP or the competent authority concerned. To prevent unnecessary discussion at the time of the request, it is recommended that countries consider putting in place, in advance, rules to govern the cost of handling law enforcement requests at an ISP.

Recommendation 3: The practice and use of legal interception should be subject to a transparent regime and to independent oversight in order for society to have insight into the balance struck between user privacy and protection and, on the other hand, the needs of the criminal justice authorities.

Recommendation 4: Rules for ISP liability for ISP content should be established that are horizontal and cover all types of content. In case such liability is made possible, it should be clearly addressed in criminal, civil (including copyright) and administrative law.

Recommendation 5: If liability for user content is provided for, the responsibilities for ISPs for blocking and takedown should be clearly defined and be based on a clear legal basis for all types of illegal content available.

Recommendation 6: Such obligations should be different depending on the type of service provided, and special care should be given to the legal basis for blocking of access to internet resources.

Recommendation 7: General obligations to monitor for certain types of illegal content should be avoided where possible, and be specific in relation to their goals and legal basis where they are imposed nonetheless.

Recommendation 8: Independent oversight or judicial control should be provided for, in order to safeguard freedom of speech, where blocking or monitoring obligations are imposed.
Recommendation 9: Where there is not an authority responsible for oversight, countries should consider establishing, or assigning responsibility to, an agency for oversight of ISP's obligations to protect the confidentiality of their subscriber's communications.

Recommendation 10: It was noted that all participant countries for which information is available have legislation in place to protect secrecy of communication and confidentiality of subscriber identity. Conflicts will inevitably arise between the requirements of law enforcement for access to data and the ISPs obligation to protect the secrecy of subscriber communication. Countries should consider assigning authority to the agencies responsible for oversight to take an active role in such cases.

Recommendation 11: Countries should further consider assigning authority to the agencies responsible for oversight of ISPs to provide concrete guidance to all relevant parties on the interpretation, scope and application of proportionality measures.

Recommendation 12: Traffic data should be retained on a clear legal basis, both in relation to traditional (voice) services as well as in relation to data (internet) based services.

Recommendation 13: A clear definition of traffic data to be retained in case of Internet connection data should be provided.

Recommendation 14: An independent regulator should be considered in order to balance the needs of law enforcement, communications privacy and freedom of speech.

Recommendation 15: Notwithstanding their mandate, regulators should endeavour to co-operate with industry on a voluntary basis, preferably on the basis of clear and agreed terms (Memorandum of understanding).

Recommendation 16: Roles of the regulatory agencies in relation to both privacy and access to (content) data should be clearly defined, and provide clear powers to supervise these important areas. Regulators with this mandate should be relatively independent and not related, directly, or indirectly to law enforcement bodies or the executive branches of government.

Recommendation 17: Oversight on the law enforcement related obligations (access to data and interception) should not be enforced by law enforcement bodies themselves.

Recommendation 18: Given the large overlaps with the area of security, the development of a clear security policy, which outlines the role of the regulator and other inspections and government stakeholders in this area, is desirable.

Recommendation 19: Countries should consider development of coordination actions between ISPs, law enforcement and other competent authorities to enable simple reporting of illegal content and routing of complaints to the relevant authority or ISP.

Recommendation 20: Countries should consider putting in place fast/provisional takedown measures to enable blocking of illegal content pending receipt of appropriate legal process (e.g. court order).

Recommendation 21: When information has been provided it is noted that there are some cases where obligations have been put in place to prevent fraud or financial damage. Countries should continue to consider the use of obligations to prevent fraud in cases where ISP action is required to protect customers against certain types of fraud or financial damage, particularly in cases where coordinated action of multiple ISPs is required to achieve the desired effect.

Recommendation 22: There are significant advantages to information sharing between ISPs to prevent threats and incidents spreading from one ISP to others. It is therefore recommended that countries consider adopting an appropriate mechanism to share information between ISPs about on-going threats or incidents. In some countries there may be obligations to report such incidents to national CERTs but even in cases where there is no obligation to report there are advantages to informal information sharing of this type.

Recommendation 23: It is reasonable to expect that agencies receiving incident reports from ISPs are likely to be receiving these reports over an extended period of time. Providing feedback to reporting entities on their reports can help those entities to provide better reports in future. It is therefore recommended that countries consider adopting a practice of

providing feedback to reporting entities with whom on-going relationships are expected so that those entities can provide better reports in future if necessary.

Recommendation 24: Technological platforms are available to assist with confidential or anonymized information sharing about on-going incidents or threats. Countries should consider the use of such a platform by, for example, their national CERT if such exists and is operational.

Recommendation 25: ISPs and competent authorities have important information to share with each other regarding their perspectives on the matter of law enforcement access to data held by ISPs. Countries should consider ISP and competent authorities working to raise each other's awareness of the other's perspective in an appropriate forum.

4 Liability Framework

4.1 Introduction

This section describes the most relevant international law that serves a purpose in safeguarding freedom of speech, the right to private life and, on the other hand, the rights and obligations that exist for Internet Service Providers in relation to public authorities and their subscribers. These rules are often carefully balanced and require diligent implementation, due to, on the one hand, the positive obligation of states to safeguard fundamental Human Rights, and on the other, to provide effective (criminal) enforcement against all types of crime, including cybercrime and protect the rights of all citizens against any type of abuse.

A balanced implementation of these is often conducive to a fair and open discussion in relation to public private cooperation, especially if all relevant interests are weighed. This requires a thorough analysis of the interests involved, and was, hence, the goal of various questions of the questionnaire that was sent to EAP3 project countries. This sections aims to clarify the sources of (international and European) law that exist in order to facilitate a more careful analysis of the answers received.

4.2 General liability framework for ISPs

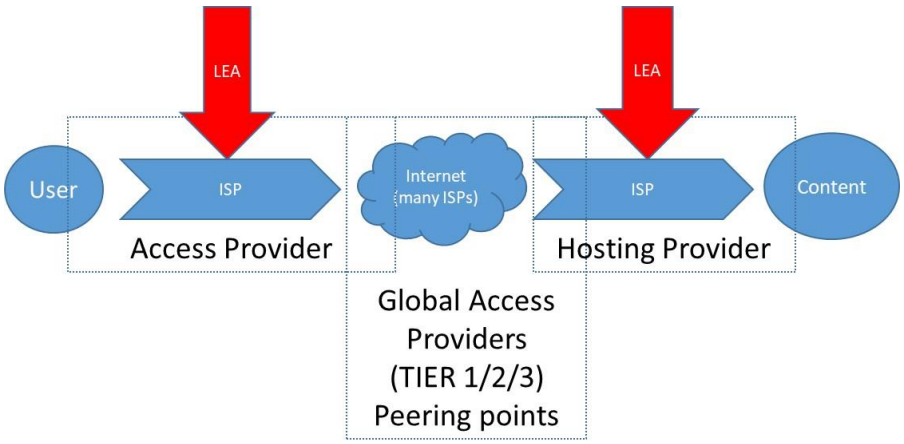
4.2.1 Introduction

This study analyses the applicable liability framework for ISPs in relation to the EU "ecommerce" directive of the year 2000 and the associated liability regime for internet Service Providers. In order to offer internet services, in 2000, the European Union (EU) developed a balanced regime that deals, in a horizontal fashion, with the liability of intermediary services that transport or store data. The regime is described in detail in directive 2000/31/EC: Directive on Certain Legal Aspects of Information Society Services[1] also referred to as the e-Commerce Directive.
The technical and business role that an intermediary plays in providing these services is critical in the way they are legally treated. For the purposes of this directive European law distinguishes three distinct roles:

- Mere conduit (Art. 12)
- Caching (Art. 13)
- Hosting (Art. 14)

A diagram outlining the role of these various providers in relation to Law Enforcement Authorities (LEA) describes the situation as follows:

[1] The relevant text of this Directive is attached as Annex II to this report.



Note that in practice large Internet providers are responsible for carrying traffic across the globe. Although they may be seen as access providers, they are often not the first port of call for LEA requests since they do not have easy access to individual users and user details. Except for some specific circumstances, the use of LEA powers against caching services is also virtually unheard of and does not play a large role in practise.

Mere Conduit

Providers that exclusively transport data, or in other words, act as a conduit for data that is transported in their networks, are called "mere conduit" providers. They have protection from liability relating to the meaning or content of that data as long as they strictly keep to this role: a party that exclusively transports internet traffic and does not select or modify the content or destination cannot be held liable for any aspect of the content.

There is one exception to this rule: when a court, or authority, in specific circumstances, can dictate that certain content should be blocked or made inaccessible. Hosting and Caching are described separately in the following paragraphs.

Hosting and caching

With caching and hosting providers, a new issue is introduced which is the level of knowledge of the provider concerning the illegality of specified content and is a further factor in determining whether the liability protections can be invoked. In these cases the provider is only protected from liability if the operator has no "*actual knowledge*" about illegal content that is stored or cached using their services. In any case, the protection fails if service providers do not act expeditiously to remove disputed content, once they have actual acknowledge of its existence and proof that it is located on their services.

Actual Knowledge

Actual knowledge is a higher level than simple knowledge. When an ISP receives information from a complaint about possible illegal content, it does not, in every cases, have the necessary information to decide if that specified content is likely to be illegal in all situations. For example, in cases relating to breach of copyright allegations, the illegality of the content may be a matter for a court to decide, on the basis of the law, the contract between two parties or the time of creation of a work. The regime does not pretend to put intermediaries in a position to judge such disputes and in those cases, is intended to maintain immunity against prosecution relating to illegal content, until actual knowledge of illegality is present with the intermediary. Therefore, even if specific content might be the object of a dispute

between parties, this does not mean an intermediary service has actual knowledge of its illegality.

Note that the exclusion of liability that is described in this directive is horizontal: it concerns any type of liability for the content on the intermediary's network. The term liability refers to civil, administrative and criminal liabilities (amongst others) which are all covered by the regime at the same time.

Freedom of Expression

One of the most important aspects of this regime is that it safeguards the freedom of expression for users of these services since it minimizes the "chilling effect" of extended liability regimes for intermediaries. In other regimes where intermediaries are directly liable for content, intermediaries are likely to start disallowing content that is considered risky, or possibly illegal. Without liability protection, it will be in their interest to limit or filter provocative content, thereby creating a negative, chilling effect on the freedom of expression online. For signatories of the Convention for the Protection of Human Rights and Fundamental Freedoms CETS 005 (ECHR), a lack of such regime may even imply a contravention of art 10(1) of the Convention, which has been ratified by all Members of the Council of Europe. In relation to the Budapest Convention: article 15 of this Convention implies that due attention is given to human rights, including freedom of speech. In this regard, having a balanced regime in place is a positive obligation under this convention as well.

4.2.2 Roles

Service providers can benefit from the exemptions of "mere conduit" and of "caching" when they are not involved or responsible for the data transmitted. Among other issues, this requires that they do not modify the data that is transmitted or received - apart from manipulations of a technical nature which take place in the course of the transmission and that they do not alter the content or integrity of the data contained in the transmission.

For example: a service provider who deliberately collaborates with one of the users of the service in order to undertake illegal acts goes beyond the activities of "mere conduit" or "caching" and, as a result, cannot benefit from the liability exemptions established for these activities.

The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds. Such injunctions can in particular consist of orders by courts or other administrative authorities that require the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.

4.2.3 No obligation to monitor

Recital (47) of Directive 2000/31/EC states that *Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation*.

In other words: intermediaries cannot be asked to monitor any and all content that traverses their service. This does not mean that it is conceivable that when, in the course of their work, they become aware of an illegal act, they can be asked to report it. However: no general obligation to monitor can be mandated by member states according to article. 15.

The article prevents, also, that member states "privatise" surveillance activities by making them an obligatory part of a licensing regime, for example.

4.2.4 Regulating ISP Liability

This study will assess whether a balanced regime is in place safeguarding the freedom of speech online, in each of the EAP3 countries, based on the information received through questionnaires. It will assess whether the main elements of the European regime – that is used, here, as an example of a well-balanced regime, are in place.

4.3 Duty to protect subscriber's identity

European treaties, such as the ECHR in article 8, recognize the right to privacy (including correspondence) in many guises. In the EAP3 region only the Republic of Belarus is not a signatory to this Convention. At the international level the right to privacy has also gained recognition in the Universal Declaration of Human Rights of 1948 (in article 12) and the International Covenant on Civil and Political Rights (article 12).

4.3.1 Proportionality and Subsidiarity

Given the important nature of this right, any infringement on this right is subject to stringent tests on necessity in, for example, the case law of the European Court of Human Rights (ECtHR) that safeguards the ECHR. In general, the regime of this treaty requires that infringements by public authorities, whilst possible, if prescribed by law, must meet strict requirements of proportionality (they must not go further than is required to achieve the goal that they are aiming to achieve, for example) and subsidiarity (they must be necessary in a democratic society). Overall these infringements should therefore be based on a clear and balanced legal regime. Article 8 of the ECHR summarize these requirements as follows:

> **Article 8 – Right to respect for private and family life**
>
> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Private life includes the privacy of communications, which covers the security and privacy of mail, telephone, e-mail and other forms of communication; and informational privacy, including online information.[2]

A last requirement is that of legality: any breaches must be foreseen by law, meaning that there cannot be arbitrary application of state power in breach of communications privacy, but instead, any use of such power must be based on a prior law, that outlines the use of this power, and authorizes it, within reasonable limits, to be used in cases where this is necessary.

[2] Cf. ECtHR Copland v. the United Kingdom, no. 62617/00, 2007

4.3.2 ECtHR Case Law on Interception

In recent case law the court has, on the one hand, identified the risk that new technologies pose in the hands of state actors: if interception of electronic communications, electronic storage of DNA material or other technologies are used – this poses a threat to private life and may lead to arbitrary interference by public authorities. At the same time, the court recognizes the need for criminal justice and the protection of rights of others and emphasized that, if sufficient safeguards exist, these technologies can be used by member states to the ECHR under the conditions of subsidiarity, proportionality and legality as previously described. It specifically recognized the positive obligation to provide effective prosecution.[3]

In practise this means that recourse against arbitrary use of state powers should be given to both subjects of surveillance, as well as those executing or being ordered to make resources available, or any other interested party, in order to prevent arbitrary state intervention and abuse of power. In one case the court even mandated that state authorities (in this case: the Serbian Intelligence Services) provide transparency as to the number of times they use their surveillance power to an NGO.[4] In another case a set-up whereby it was factually possible to execute surveillance on mobile networks without prior order was performed by state authorities, and in which this could be achieved without transparency to the network operator, due to the pre-installation of equipment and the order to authorize the surveillance was issued retrospectively, was heard by the court, which found that such a practise was illegal. The mere (pre-)installation of such equipment was not.[5] Moreover the court held that a government may only intercept telephone communications where the body authorizing the surveillance has confirmed that there is a "reasonable suspicion" of wrongdoing on the part of "the person concerned."

Due to the Snowden revelations and the increased use of police and intelligence oriented interception, both the Committee of Ministers of the Council of Europe and the Council of Ministers of Justice and home Affairs of the EU have issued positions on this matter outlining, amongst others, the need for independent oversight of any measures that amount to interception and surveillance of electronic communications.[6]

4.3.3 Regulating interception and the right to communications privacy

The combination of these requirements, in turn, implies a clear and balanced legal regime in which use of police power in cybercrime cases is sufficiently transparent and in which safeguards exist against both state abuse and non-compliance by law enforcement authorities and intermediaries alike.

This regime is often regulated in various places. Obligations to provide access (which are the subject of the below paragraph) are frequently found in telecommunications legislation, or in individual licenses issued by public authorities.

The right to communications privacy is often also subject of national legislation and is usually safeguarded in countries by both local telecommunications legislation, the constitution and

[3] Cf. ECtHR Szabó and Vissy v. Hungary, no. 37138/14, 2016; and ECtHR Van der Velden vs. The Netherlands, no. 29514/05 ,2006

[4] Cf. ECtHR Youth Initiative for Human Rights vs. Serbia , no 48315/06, 2013

[5] Cf. Orange Slovensko, A. S. v. Slovakia, no. 43983/02, 2006 and Roman Zhakarov vs. Russia, 47143/06, 2015

[6] Council of Europe: Recommendation CM/Rec(2014)4 of the Committee of Ministers to member States on electronic monitoring.

case law. In certain cases there are also specific requirements in telecommunications licensing regimes. It is the purpose of this study to analyse the way this important right is safeguarded, and how law enforcement orders and other interferences are balanced with the need for proportionality and legality.

Article 15 of the Budapest Convention on Cybercrime summarizes the balance between human rights and the procedural requirements of the convention, which consist of a set of measures authorizing law enforcement to use certain power in cases of cybercrime. It applies to all infringements on human rights, including the rights to private life and the freedom of speech.

Article 15 – Conditions and safeguards

1. *Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.*
2. *Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.*
3. *To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.*

The following paragraph outlines the further powers that the convention mandates for its signatories, especially in relation to ISP data.

4.4 Rules on providing law enforcement access to ISP infrastructure and data

4.4.1 Data types, definitions

The Budapest Convention on Cybercrime has several rules that mandate signatories to implement access to data in communications infrastructure that is crucial to solving cybercrime. This data can involve several types:

- Subscriber information as registered by a company:
  - Name address
  - Details of the subscriber as registered by a company)
  - Means of payment and related identifiers (bank account, credit card etc.)

- Traffic data, practical examples of which include:
  - Calling and called parties of telephone calls
  - IP addresses allocated to a subscriber

- Content data such as:
  - Phone conversations

- Email content
- Data content of an internet connection

In many cases, especially in relation to Internet based communications, precise definitions of the nature of the data involved are absent or quickly lead to lack of clarity. The Budapest Convention on Cybercrime, for example only describes traffic data and subscriber information and uses a functional description in Article 1 sub d (traffic data) and a more detailed one in Article 18 paragraph 3 (subscriber information):

> ***Article 1 - Definitions***
> *(..)*
> *d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.*

And:

> ***Article 18 – Production Order***
> *(..)*
> *3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:*
>
> *a. the type of communication service used, the technical provisions taken thereto and the period of service;*
> *b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;*
> *c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.*

This raises the question of how this definition is implemented in the Eastern Partnership region. A further analysis is done in this study.

4.4.2 Data related powers

The following legal powers are to be implemented by signatories of the convention, in order to allow law enforcement access to data in communications networks for the purpose of prosecution of cybercrime:

- The expedited preservation and partial disclosure of traffic data (art. 17)
- The production order (related to the production of any data held in a computer system or by a service provider - Art. 18)
- The search and seizure of stored computer data (Art. 19)
- The real-time collection of traffic-data (Art. 20)
- The interception of content data (art.21)

Implementation of all powers is subject to Article 15, as described earlier and hence requires careful consideration of the impact of the use of these powers in each individual case. With the exception of interception, all powers listed should be applicable (after a proportionality test) in cases where any of offences described in the convention are concerned.

Article 14 defines the selection of activities to be considered as offences under the treaty. These include activities relating to computer systems, data itself, activities performed by using a computer system and activities relating to content on internet systems such as child pornography or commercial scale copyright infringement:

a. Illegal access
b. Illegal interception
c. Data interference
d. System interference
e. Misuse of devices
f. Computer related forgery
g. Computer related fraud
h. Child pornography
i. Commercial scale copyright infringements

Or cases of:

j. other criminal offences committed by means of a computer system; and
k. the collection of evidence in electronic form of a criminal offence.

Some of these offences might be committed intentionally by a corporate body and the convention requires corporate liability for cybercrime offences to be included in legislation.

4.4.3 Powers to access data

The following outline provides a further insight that guides the analysis of the answers provided in this study.

Expedited preservation of stored computer data - Article 16 of the Convention:

1. Parties enable competent authorities to order or obtain the expeditious preservation of specified computer data, including traffic data if it is vulnerable to loss or modification.
2. The order should be valid for a minimum of 90 days (and may be made renewable)
3. The order can be given confidentially.

Cybercrime activities often take place outside the national jurisdiction using Internet service providers established in different countries. Illegal activities that use these services can be identified using data stored on the servers and networks of these service providers but this data can be very volatile. Traffic records, subscriber data and even content data is rarely stored for long periods of time and often gets deleted or overwritten in short periods of time. If an investigation is undertaken it can be several months, or sometimes years, before the relevant data can be formally requested using international instruments such as MLAT (Mutual Legal Assistance Treaty) from these non-national service providers. Due to this delay this data is often no longer available or destroyed. The expedited preservation of stored computer is a method whereby investigations can request the support of the foreign authorities to preserve relevant computer records, which are not released to the requesting authority until appropriate legal instruments have been duly processed. It enables the protection of relevant data pending appropriate relevant follow up that authorizes the release of the stored records. This strikes a reasonable balance and protects important electronic evidence and data pertinent to the case, until the certified and justified international disclosure request is received and processed.

Expedited preservation and partial disclosure of traffic data - Article 17 of the Convention:

1. Parties enable competent authorities to order the expeditious preservation of specified traffic data at any service provider involved
2. Competent authorities have the right to request expedited disclosure of sufficient traffic data to enable the authorities to identify the providers involved and in order to quickly reveal the path of the communication.

Expedited preservation is defined to protect and secure data, which might be volatile or vulnerable to tampering. This data might provide valuable relevant clues or electronic evidence to assist in a law enforcement investigation. However, in some cases, this evidence will prove that a connection was only routed through a service provider and that further evidence might be obtained from further countries in the chain of communications. Partial disclosure refers to the activity whereby the first foreign jurisdiction (and further jurisdictions in the chain) disclose to the requesting party the possible location of other relevant and necessary evidence in the chain of communications. The requesting party would then issue expedited preservation and partial disclosure requests to these additional jurisdictions if required or felt necessary. For example, a user in Ireland might be the subject of a cyber-fraud incident and the email user is identified in the Netherlands. An Expedited Preservation and Partial Disclosure of Traffic Data to The Netherlands to get the traffic and user subscriber data would cause the contacts in the Netherlands to inform the requesting party that the network connection in the Netherlands was actually coming from Ukraine and would provide the relevant IP address information to send a preservations request to the Ukrainian authorities.

Production order - Article 18 of the Convention:

1. Parties allow their own competent authorities to order anyone in their territory to submit specified computer data under their control.
2. Parties allow their own competent authorities to order service providers to submit subscriber information in that providers control.

A production order requests the recipient to disclose data which they are known to have in their control. The ease-of-access and the level-of-detail provided in the order to identify the requested data are relevant when transposing this requirement into national law.

Search and seizure of stored computer data - Article 19 of the Convention:

1. Parties –within their territory - allow their own competent authorities to search or access a computer system or part of it and computer data stored therein.
2. Parties allow - within their territory - their own competent authorities to search a computer-data storage medium in which computer data may be stored.
3. Parties make possible for the authorities to extend the search to other systems accessible from the original system, and within the party's territory.
4. It should be possible for the competent authorities of each party to:
    a. Seize or secure computer-systems or computer-storage
    b. Make and retain a copy of those data
    c. Maintain the integrity of the stored data
    d. Render inaccessible or remove computer-data in the accessed systems
5. Any person with knowledge of the computer system, or measures to protect the data in it, can be ordered to comply by the parties competent authorities.

Search and seizure describes expected protocols for gaining forced access to computer systems and computer data by authorised authorities. The national authorities can request permission from a court to conduct a search and to make copies of any data stored and to ensure that such copies are made to acceptable international forensic evidentiary standards.

Real-time collection of traffic data - Article 20 of the Convention:

1. Parties allow competent authorities to collect or record real time traffic data through technical means on their territory. If it is not done by authorities, collection should be possible in any event (such as through central storage or access).
2. Competent Authorities are able to compel a service provider to collect or co-operate/assist authorities with collection/recording of traffic data.
3. That orders related to the collection of traffic data can be made confidentially.

Real-time collection of traffic data specifies the interception of network communications by authorised national authorities on the network of service providers. It is also possible that such requests are not publicly declared so that a covert investigation is not prejudiced. These requests include the traffic records only and do not include the content of the communications. It is important to clearly and unambiguously specify what is considered traffic data and what is considered as content data.

Interception of content data - Article 21 of the Convention:

1. Interception of content data is possible for the competent authorities in a limited set of cases (serious offences)
2. Competent Authorities are able to compel a service provider to collect or co-operate/assist authorities with collection/recording of content data in these cases.

Orders related to the collection of content data can be made confidentially.

Real-time collection of content data specifies the interception of network communications by authorised national authorities on the network of service providers. It is also possible that such requests are not publicly declared so that a covert investigation is not prejudiced. These requests include the records of traffic activities and the content of the communications and must have a much higher barrier since this directly impacts on human rights of the participants of that communications. The use of this power should only be possible in cases where this is deemed necessary in a democratic society, and both the use of the power and the required safeguards should be clearly specified in legislation.

4.4.4 Data retention and the ECJ

Although the Budapest Convention is silent on this issue, there is a widespread practice in European countries to require ISPs and other electronic communications providers to retain traffic data that they log for a specified period. This is primarily done to enable law enforcement to request access once this is needed for an investigation, and prevents that potential evidence is destroyed before it can be analysed. Directive 2006/24/EU harmonized this practice and was to be implemented by al EU member states.

At the same time the directive's approach lead to significant privacy concerns as it also concerned data of non-suspect citizens that is retained for longer periods of time without proper safeguards being guaranteed by the directive text. For this reason a careful balance needs to be struck between the retention period and the right to privacy in national legislation.

As to the directive: in a recent case brought by Digital Rights Ireland, The European Court of Justice (not to be confused with the ECtHR) found that this European directive, that harmonized the data retention regime, was not proportional. It was held that the period of retention should be based on objective criteria, that restrictions on categories of data and access to data should be provided and that access should be for clearly defined purposes. This is especially so since it concerns unspecified blanket retention of all data, regardless of the purposes served or the persons concerned. Since insufficient safeguards are presented by the directive, it was struck down as incompatible with the EU's Human Rights Charter.

In this study, a further examination of the data retention regimes of the EAPIII countries shall be carried out in relation both with a view to the efficacy of implementation as well as to review whether these potential safeguards are in place.

4.5 Retention of data for business purposes

Data retention is only one solution for the problem of the volatility of digital evidence. In practise, it is often the case that businesses retain data voluntarily, and for entirely legitimate reasons. Such data may be kept for any number of business reasons such as:

- Fraud prevention
- Tax records
- Service delivery
-

It is important to note that, where personal data is concerned, data may potentially be subjected to limitations on any regime where unbridled retention and processing of records takes place. If data is kept for a valid reason that outweigh the interest of the data subject, or is held with the subjects permission, then this may well be of assistance to law enforcement.

In such cases the Production order that is mandated by the Convention may provide the tools to request the data and either prevent or solve crimes.

There are no international standards for the retention of data for business purposes in the telecommunications sector.

4.6 Obligations to report crime or cybersecurity incidents

Since the adoption of the Directive on Security of Network and Information Systems (NIS Directive) in the EU there is a duty, for each EU member state, to identify critical infrastructure, and, amongst others, appoint an authority (or possibly: multiple authorities) where providers of such infrastructure are supervised in relation to their network security. A part of this regime is the obligation to actively report security breaches and incidents.

Next to these national NIS authorities, each member state will also need to be equipped with a CSIRT (or CERT) team in order to promote swift operational cooperation and information sharing. A key duty for operators of critical (or essential – as the NIS directive calls it) infrastructure is that operators of this infrastructure have a duty to secure their networks and information systems. Lastly they have a duty to ensure continuity and a duty to report any incidents that, despite such measures, still occur.

When an incident occurs operators are required to report at least:

(a) the number of users affected by the disruption of the essential service;

(b) the duration of the incident;
(c) the geographical spread with regard to the area affected by the incident.

This information can be used for international cooperation, either between member states (which each have a duty to set up a single point of contact for such incidents) or between CSIRTs in order to better prevent further damage and take appropriate preventive measures.

From a criminal law perspective it is also not uncommon for serious crimes to attract a duty to report them to the police or prosecution. These duties usually encompass all witnesses of such crimes, and/or every person with knowledge about them, apart for the suspect or those who are exempted due to the prohibition on self-incrimination (Article 6 ECHR). Such regimes may or may not apply to cybercrime.

There is no international standard in relation to cybercrime reporting. Best practise, however, dictates that a low reporting threshold preferably through online reporting, are the most meaningful ways for governments to address the issue and prosecute cybercrime in an intelligence-lead manner.

5 Regulatory authorities

5.1 Role of regulators: EU as example

Regulatory authorities that are active in, or related to the telecommunications sector in the EU are supervise and oversee several legal regimes at the EU level. They supervise legislation related to electronic communications services and, especially when they are designated as competent security under the network and information systems security directive[7], are also responsible for the security of networks.

As such they are pivotal in securing networks and safeguarding society against the adverse effects of cybercrime and the related criminality – whilst balancing these needs with adequate safeguards for privacy. At the same time, regulators are usually responsible for overseeing the obligations of providers in relation to law enforcement and access to relevant data for the prosecution of crime. To oversee availability of systems that retain subscriber information, traffic data, and in many cases, the ability to intercept content data traversing their networks, is usually part of their tasks.

For the purposes of this study a broad analysis of the EU framework for regulation of the communications market was performed, and is presented here as a best practise and reference.

5.2 Tasks of regulators

Regulators may have many tasks, not all relevant for the context of this report. It is important to note that relevant obligations, for the purposes of this report, can be sub divided in several areas:

- Obligations to provide access to various types of data relevant for law enforcement
- Obligations related to the availability of facilities and their availability, safety, user privacy and security.
-

In the European Union different regimes exist that differ per member state and in which these authorities (which are sometimes several agencies in a country) play differing and complementary roles in relation to other supervisors. For the purposes of this report the main tasks they perform in relation to law enforcement and cybercrime, are:

- Implementation, supervision and enforcement of the regime of data retention
- Implementation, enforcement and supervision of legal interception facilities at providers
- Enforcement and supervision of privacy aspects in relation to traffic and content data
- Enforcement and supervision of network security and technical standards in this area to protect the communications secret/communications privacy.

Rules related to these tasks may, in some cases, be laid down in individual licenses of telecommunications carriers, but can also be subject of a general licensing or notification regime, in which equal provisions apply for certain categories of providers. In the latter cases there is usually a central registry of providers, kept by one or several authorities, that lists the providers that are active in certain markets. In a final category of cases, there may be

[7] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

obligations laid down in special or criminal legislation, which are overseen, implemented or executed by these authorities.

The European regimes are by no means equal, and are used here as a reference and, to some extent, best practise of implementation. The questions asked in the questionnaire that is part of this study, are based on these practises,

It should be noted that the precise modality of making available facilities, such as access to subscriber data, or the interception of content data, can be executed in any number of ways, so it is up to individual member states to implement these obligations, and provide a regime for oversight and supervision that matched the local implementation.

5.3 Implementation

For each of these tasks the following modalities of implementation can be observed:

- Data retention/subscriber data
    - This concerns, for example
        - Phone number/Name address combinations
        - Ip address/Name address combinations
        - Further subscriber details
    - Implementation of this obligation can be done in several ways – where different safeguards and technical facilities can be used or mandated:
        - Relevant data can be uploaded to a central database, accessible to law enforcement, operated uy a regulator or government agency.
        - These data can be obtained through direct access to provider databases and operational systems, in which case an interface and retrieval system will usually be mandated.
        - Data can be obtained on a case by case basis, through more or less automated systems, requiring an individual response from carries.
    - Independent oversight of such systems is often provided in the first two cases, since, where Law Enforcement has direct access to personal data, the risk of abuse is significant.
- Legal interception of content data
    - This concerns the interception of voice or data traffic
    - Different regimes may apply to voice and data streams
    - Equipment can be located:
        - At the provider
        - At the provider and data can be relayed to a central facility
        - At a central government agency or operational centre where providers are asked to deliver the relevant traffic
    - Costs for these facilities can be significant and can be:
        - Split between provider and public funds
            - Differences can exist in relation to capital expenses (initial investments into equipment etc.) and operational expenses (staff and legal advice etc.)
            - Regimes may differentiate between small and large providers.
        - Carried by the public budget
        - Be carried by the provider
            - Exception often exists in these first and last cases for small providers or non-public networks.
    - Oversight on any obligations of providers in this area is usually placed at an independent (non-law enforcement) agency to prevent a conflict of interest.

- Privacy aspects concern duties to safeguard the communications secret and data of network subscribers, obligations to prevent illegal interception and requirements related to the processing of personal data, location data and traffic data.
    - Obligations can be implemented through common standards
    - Several types of data may be subject to different legal regimes (traffic data and location data are treated differently for example, in the European telecommunications privacy regime)[8].
    - There may be notification obligations to regulators if and when breaches occur and personal data, or communications traffic is inadvertently disclosed.
- Security related tasks are often carried out by regulators and other bodies. In many cases regulators are part of a community of several institutions involved in securing national critical infrastructure. Specific Security related tasks may involve:
    - Regulating security measures and network operations with a view to safeguarding privacy and confidentiality of communications providers and their organisations and networks.
    - Auditing security management systems in place in relevant sector players.
    - Many regulators work with, or host a Computer Emergency (/Incident) Response Team (CERT or CIRT/CSIRT) that may have (amongst others) any of the following tasks:
        - Monitoring defined internet networks or infrastructures
        - Respond to incidents related to security
        - Sharing intelligence on threats and security risks.
    - In many cases regulators require network operators to report at least severe incidents to them, in order for a CERT or other body to be able to assess the risks for other networks and issue warnings to prevent attacks or incidents from occurring elsewhere.

The precise allocation of these tasks to any of a state's institution may vary widely. In many cases similar tasks are shared by various bodies and, although related, are performed in relative isolation form other stakeholders and agencies. This creates the need for closer and more comprehensive cooperation at the national level.

5.4 Obligations and enforcement

For the purposes of this study it is important to realize the layered nature of the European regime that applies to ISP liability and to access to data for law enforcement:

- Liabilities for user content are largely excluded for ISPs – only courts or competent authorities may enforce the deletion, blocking or making inaccessible of data generated by users of internet services. This is only different for hosting providers who are expected to act on actual knowledge of illegal content.
- In relation to access to data, the requirements to be imposed on providers are imposed by a generic or individual license or by way of direct regulation. They may include subscriber traffic, and/or content data.
- In cases where technical measures need to be taken in order to achieve this access, a regime exists to enforce the presence of the relevant facilities, and to ensure compliance.
- The oversight on these regimes is generally done by an agency without law enforcement status as to avoid conflict-of interest in case of disputes.

[8] Cf . Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

- Enforcement measures against providers should be proportional and the use of criminal law against industry players is customarily avoided. Fines and injunctions are generally used as measures against non-compliant businesses.

5.5 Types of agencies and cooperation required

Agencies that typically oversee or execute these tasks are:

- Post and telecommunications administrations
- Specialized technical agencies or inspections
- Ministerial departments responsible for telecommunications
- Data protection agencies
- Security related services or agencies
- Specialized law enforcement bodies

The choice of agencies usually also depends on the required administrative powers, legal safeguards required and the logical clustering of tasks. In practise, the outcomes vary significantly per member state, even if these tasks are all related and similar laws apply throughout the EU.

As can be seen from both the common tasks of regulators as well as the typical governmental agencies involved, various interests are at stake when it comes to regulating the domains of security, privacy and access to data for enforcement purposes. In practise, therefore, many questions will need to be addressed in order to achieve good cooperation. These may include:

- Issues related to accuracy and availability of information
- Exchange of relevant data and intelligence
- Agreeing on information exchange protocols and technologies
-

In practise the area of concern for this study involves many different stakeholders, and the access to data for law enforcement, as well as the security of networks requires close cooperation between various actors in order to achieve the desired results and to balance the interests involved. For this reason, public-private cooperation between stakeholders in this area is essential.

In order to achieve this cooperation at least the following conditions can be seen as essential:

- Regular meetings between relevant stakeholders
- Adequate instruments to communicate, also between industry and public sector actors
- Adequate instruments (such as memoranda of understanding or standing committees) to agree common positions on practical issues, especially where these cover several of the domains mentioned
- Efficient exchange of information relevant for each of the stakeholders
-

The next section will detail various ways to operationalize public-private cooperation – in so far as it falls outside the scope of the mandatory obligations (liabilities) of the actors involved.

5.6 Voluntary/non-regulatory cooperation

Although issues such as ensuring safety of users on the Internet, obligations to report cyber-incidents or handling of identified illegal content can be dealt with through regulation, these are also in some cases dealt with through less formal non-regulatory/voluntary cooperation initiatives. Even where a regulatory obligation is in place, it may be the case that the obligation is implemented in practice through the form of a cooperation initiative, such as a binding voluntary code of practice. Non-regulatory/voluntary initiatives have the added advantage of typically being quicker to put in place when there is a recognised immediate-term requirement.

There are a wide range of non-regulatory/voluntary cooperation initiatives that can be put in place between ISPs, regulators and law enforcement agencies. The purpose of this section is to briefly describe some of the different types of cooperation initiatives that can be put in place.

- **Blocking access or fast takedowns of illegal content:**

The absence of a legal obligation to monitor or report illegal content can present a challenge to ISP cooperation due to concerns that ISPs may have about liability under other obligations (such as privacy of communication legislation) in cases where content is incorrectly identified as being illegal in the absence of a law enforcement or court order to remove content. Another area to be considered is how, in practice, when a member of the public becomes aware of illegal content, that content can be reported to the appropriate agency or ISP. The same problem may arise within law enforcement agencies wherein it may be difficult for an investigating officer to determine, having received a report or otherwise identified illegal content, the appropriate ISP to communicate with. Having a single point of contact, such as a reporting hotline, that is able to report the matter to the relevant agency or ISP is one form of cooperation initiative that can be helpful in these cases. The problem of correctly identifying the correct ISP/hosting company is further exacerbated if the content is held outside of the jurisdiction. Involvement in international cooperation initiatives such as INHOPE can be helpful in such cases[9]. Cooperation agreements can also be helpful in cases where ISPs identify illegal content on each other's networks, so that complaints can be forwarded as appropriate.

- **Addressing common cyber-security threats:**

In some countries ISPs have a regulatory obligation to protect their customers and themselves against fraud or financial damage. This obligation can take a variety of forms, ranging to general obligations arising as an implication of ISPs being categorised as critical national infrastructure to specific solutions to protect customers against, for example, various types of telecommunications fraud (e.g. premium number dialling). However, the practical implications of this may require cooperation between the ISPs in the form of either information exchange or shared infrastructure to make a meaningful impact on the threat for the ISP subscribers.

- **Information sharing initiatives:**

Where an ISP finds itself the target of a particular attack, or identifies a vulnerability that exposes its operations to attack, there are advantages to sharing this information with other ISPs so that they can assess their exposure to the same type of attack. This type of information sharing can might for containment of such incidents to within a single

[9] http://www.inhope.org/gns/who-we-are/at-a-glance.aspx

organisation and prevent escalation into a major national cyber-security incident. National CERTs (Computer Emergency Response Teams) can have an important role to play here, but alternatives such as informal ISP fraud and security forums or bilateral communication can also be a feasible where a national CERT is not operational or the incident falls out of scope of the responsibilities of the national CERT. It can also be helpful in such informal fraud and security forums to involve law enforcement agencies (if law enforcement agencies have a crime prevention role) in a collaborative fashion.

- **Awareness training initiatives:**

Information awareness programmes are an important way for ISPs and state agencies to share information about their perspectives on the matter of law enforcement access to information. ISPs can provide information to state agencies on, for example, what information they have, how to request it, common problems experienced with requests received and so on. State agencies can provide information to ISPs on changes to regulatory regimes, requirements for information retention and so on. The format of the awareness initiatives can be wide-ranging, from ISP involvement in police or judicial training events to law enforcement involvement in private security conferences.

6 Situation report summaries

To understand the situation regarding liability framework, regulatory and voluntary cooperation within the EAP countries, a survey was circulated to relevant agencies within those countries. The responses have been analysed and in the sections below, a summary of the situations as reported can be found.

6.1 Armenia

The principle legal instruments regulating the obligations of Internet Service Providers are the Law on Electronic Communication[10] and the decisions and regulations of the Public Services Regulatory Commission of the Republic of Armenia (PSRC)[11], such as the Regulation on Licensing, Regulation on Radio Frequency Usage Authorization, Regulation on Numbering Resource Usage Authorisation as well as individual licenses for network operation of the Internet Service Providers. The framework of the PSRC's regulatory competencies includes the areas of licensing and authorisation, spectrum management, numbering, tariff-setting, consumer protection, market analysis and enforcement, interconnection and infrastructure access, universal service, dispute resolution as well as cooperation with other responsible authorities and international organisations.

Any person who is seeking market entry and wishing to own and operate a public electronic communications network must apply for an operator (network) license. Operator licenses are granted within 23 working days after the receipt of the application, pursuant to the licensing procedures set forth in the relevant legislation. However, a person may enter the market and provide public electronic communication services as a service provider, by making use of the network infrastructures of the existing operators. In this case, simple notification of the service provider to the PSRC prior to deployment of its services is sufficient (simple notification procedure).

Generally speaking ISPs do not have any ability or right to influence user-generated content without a court order. As a result, they are not held liable for content generated by users. Network Neutrality was declared in the Principle of Internet Governance[12]. Except for emergency circumstances a court order is required for blocking, deletion or prevention of certain types of information being hosted or made accessible online.

ISPs do not have any obligation to monitor user-generated content or initiate any other action if a user (a) creates, publishes or hosts illegal content on their network or (b) accesses illegal content on their network. If an ISP becomes aware of illegal content accessed, created, published or hosted on their network, the ISP has the right, but not the obligation, to inform the police.

In accordance with Article 49 (Privacy of the Customer Information) of the Law on Electronic Communication[13], every operator and service provider shall regard and treat as confidential all information regarding the type, location, use, destination, quantity and technical configuration of services used by their customers. This duty is enforced by the Public Services Regulatory Commission (PSRC) in cooperation with the law enforcement and data protection agencies. The PSRC may impose fines and penalties if it determines after an administrative notice and a public hearing that a licensee has failed to comply with the

[10] http://www.arlis.am/

[11] http://www.psrc.am/en

[12] http://igf.am/wp-content/uploads/2015/03/IG_Principles_EN.pdf

[13] http://www.arlis.am/

relevant provisions of the Law on Electronic Communication on confidentiality of subscriber identity and communication. In certain cases, the PSRC may change, suspend, or request for judicial termination of a license or an authorisation for violation of provisions of the law. An ISP may respond to requests for access to subscriber data only within the legal scope of Article 49 of the Law on Electronic Communication. In particular, an ISP may disclose subscriber data as authorised by law in connection with the surveillance, investigation or prosecution of a criminal offence or threat to national security, or with the written consent of the subscriber, or where the disclosure is necessary in defence of the ISP. Beyond these circumstances, the PSRC has no legal powers to compel an ISP to respond to request for access to subscriber data.

The PSRC regulations specify that call data records (time, duration, caller phone number and correspondent phone number) must be retained for two years. Enforcement measures and penalties are available to the PSRC in cases where an ISP does not conform with the requirements to retain phone call records. The minimum size of such a penalty is USD10,000 (approx.) but higher penalties can be defined. For IP connections there is no obligation on the ISPs, but the main operators have signed a Memorandum of Understanding with the police and undertook an obligation to keep information about source IP address, destination IP address, time and duration. The duration of retention is defined in the Memorandum of Understanding, which is not available online.

In accordance with Article 50 (Interception, Wiretapping or Disclosure of Messages) of the Law of Electronic Communication, no party other than a party to a message transmitted by any electronic communications means may intercept, tap or disclose the content of this message unless authorised to do so in writing by the parties to the message or by a court decision pursuant to the Law. In such cases, and in accordance with the procedures prescribed by the law, all operators and service providers must grand law enforcement or security personnel access to any equipment, facilities, switches, routers or other similar equipment. The PSRC regulations and license pre-conditions specify that an ISP must provide the technical ability to perform lawful interception. The PSRC may impose penalties for non-conformance with these requirements. As mentioned above, the minimum size of such a penalty is USD 10,000 (approx.) but higher penalties can be defined.

There are no regulations applicable to the security of data held by ISPs for business purposes. There are also no regulations that impose obligations on ISPs for retention of data for business purposes and for maintaining the security of that data. If an ISP becomes aware of a data breach the ISP has the right to inform the police, but is not obliged to do so. If an ISP becomes aware of a crime conducted on or via its infrastructure, the ISP has the right to inform the police but is not obliged to do so except for a general obligation to report any type of crime.

Armenia has an information security strategy, adopted in 2007[14]. There is a non-governmental CERT, which provides information about incidents.

6.2 Azerbaijan

No Information was provided by the authorities of Azerbaijan.

6.3 Belarus

The principle legal instruments regulating the obligations of Internet Service providers are:

[14] http://www.mfa.am/u_files/file/doctrine/Doctrineeng.pdf

- The Law of the Republic of Belarus of July 19, 2005 "On Telecommunications"[15]
- Decree of the President of the Republic of Belarus of 1 September 2010, No. 450 "On licensing of certain types of activities"[16]
- Resolution of the Council of Ministers of the Republic of Belarus of August 17, 2006, No. 1055 "On Approval of the Rules for the Provision of Telecommunication Services"[17]
- Decree of the President of the Republic of Belarus of 1 February 2010, No. 60 "On measures to improve the use of the national segment of the Internet"[18]
- Order of the Operational and Analytical Centre under the President of the Republic of Belarus dated August 2, 2010, No. 60 "On approval of the Regulation on the procedure for determining Internet Service Providers authorised to provide Internet services to state bodies and organisations using information that constitute state secrets in their activities"[19]

Additionally, the following rules and regulations are relevant to the deletion, blocking or prevention of certain types of information being hosted or made accessible online:

- The Decision of the Operational-Analytic Centre Under the President of the Republic of Belarus, the Ministry of Communications and Information of the Republic of Belarus of February 19, 2015, No. 6/8 "On approval of the Regulation on the procedure for limiting access to information resources (their constituent parts) located in the global computer network Internet"[20]
- The Law of the Republic of Belarus of July 17, 2008 "On the Mass Media" (Articles 38, 51-1)[21]

The role of the Ministry of Communications and Informatization in the oversight of ISPs is as follows:

- Development and implementation of telecommunication development programs.
- Coordination of activities in the field of creation and development of telecommunication networks.
- Long-term planning of the use of the radio-frequency spectrum by radio electronic means for civil purposes.
- Establishment of a unified procedure for interaction of telecommunication networks through the public telecommunication network, as well as monitoring and centralised management of the public telecommunication network.
- Determination of the requirements for the construction, numbering, organisational and technical support for the operation of telecommunication networks, their management, to ensure the protection of telecommunication networks from unauthorised access to them and messages transmitted thereon, the use of the radio frequency spectrum, the order of traffic transmission, the provision of telecommunication services.
- Regulation of the activities of telecommunication operators.
- Allocation and withdrawal of numbering resources.
- International cooperation in the field of telecommunications, including interaction with international organisations and telecommunications administrations of other

[15] http://www.pravo.by/document/?guid=3871&p0=H10500045
[16] http://pravo.by/document/?guid=3871&p0=P31000450
[17] http://www.pravo.by/
[18] http://oac.gov.by/files/files/pravo/ukazi/Ukaz_60.htm
[19] http://oac.gov.by/files/files/pravo/prikazi_oac/Prikaz_OAC_60.htm
[20] http://oac.gov.by/files/files/pravo/post_oac/Post_OAC_6.8.htm
[21] http://www.pravo.by/document/?guid=3871&p0=H10800427

states, ensuring the fulfilment of obligations under international treaties of the Republic of Belarus.
- Development and adoption of regulatory legal acts.

The role of the Operational and Analytical Centre Under the President of the Republic of Belarus in the oversight of ISPs is as follows:

- Coordinates the activities of government agencies, Internet service providers on information security when using information networks, systems and resources of the national segment of the Internet.
- Representing the Republic of Belarus in international organisations on security issues using the national segment of the Internet.
- Determining, upon agreement with the President of the Republic of Belarus, a list of telecommunication operators authorised to pass international traffic and join foreign communication networks.
- Making decisions, mandatory for execution by telecommunications operators and other participants of the telecommunication services market on the provision of data services and telephony by the IP protocol.
- Considering the applications of legal entities and individual entrepreneurs on licensing of activities in the field of communications in the provision of data services and telephony by the IP protocol, on the results of this review, make to the Ministry of Communications and Informatization of the Republic of Belarus, binding decisions.
- Taking measures to counter unfair competition, to protect rights and legitimate interest of telecommunication operators and other participants of the telecommunication services market in the provision of data services and telephony by the IP protocol.
- Regulating tariffs for telecommunication services on connection of data transmission networks.
- Defining jointly with the Ministry of Communications and Informatization of the Republic of Belarus terms of connection to telecommunication networks, to the public telecommunication network, as well as the order of their interaction.
- Taking measures to resolve disputes arising between telecommunication operators on the connection of data transmission networks, the transmission of data traffic, the inclusion of data transmission networks, granting access to public telecommunication networks and infrastructure.
- Defining jointly with the Ministry of Communications and Informatization of the Republic of Belarus telecommunication operators authorised to pass inter-network traffic.
- Exercise other powers in accordance with the law.

ISPs cannot be held liable for user activity irrespective of whether the ISP provides connectivity or content hosting/caching services. ISPs are not legally obliged to report illegal content however, according to Paragraph 8 of the Decree of the President of the Republic of Belarus of December 28, 2014, No 6 "On Urgent Measures to Counter Illicit Drug Trafficking", the owners of Internet resources are required to "Analyse the content of their information resources and prevent the use of their information resources for the dissemination of messages and/or materials aimed at illicit drug trafficking; inform the internal affairs bodies of attempts to use their information resources to disseminate messages and/or materials aimed at illicit drug trafficking." They are also obliged to act on illegal content reported to them by competent authorities within a specified period of time. Repeat violations of any act may lead to suspension of internet services. This is also decided upon by competent authorities. Liability for content is limited, since ISPs are to act on authorities' orders only.

Article 54 of the Law of the Republic of Belarus of July 19, 2005 "On Telecommunications"[22] guarantees in the territory of the Republic of Belarus the secrecy of telephone and other messages transmitted over telecommunication networks. Telecommunication operators and telecommunication service providers are obliged to ensure the secrecy of telephone and other messages. Restriction of the right to privacy of telephone and other messages transmitted through telecommunication networks is allowed only in cases provided for by legislative acts. Telecommunications operators and telecommunication service providers can provide information on the facts of providing telecommunication services only to subscribers or their representatives, as well as in other cases provided for by legislative acts. In accordance with Articles 17 and 18 of the Law of the Republic of Belarus of 10 November 2008 "On Information, Informatization and Protection of Information", "Information on the provide life of an individual and personal data refers to information whose dissemination and/or provision is limited. No one has the right to demand from an individual the provision of information about is private life and personal data, including information constitution personal and family secrets, the privacy of telephone conversations, postal and other communications concerning his state of health, or to receive such information in a manner other than the will of the physical person, except for cases established by legislative acts of the Republic of Belarus. The collection, processing, storage of information on the private life of an individual and personal data, as well as the use of them, are carried out with the written consent of this individual, unless otherwise provided by legislative acts of the Republic of Belarus." The requirement to protect the secrecy of subscriber information is also reflected in the Decree of the President of the Republic of Belarus of April 16, 2013, No. 196 "On some measures to improve the protection of information".[23] The procedure for the receipt, transfer, collection, processing, accumulation, storage and provision of information on the private life of a physical person and personal data, as well as their use, is established of legislative acts of the Republic of Belarus.

According to Paragraphs 18 and 37 of the List of Supervisory Bodies and Area of their Control (Supervisory) Activity, approved by the Decree of the President of the Republic of Belarus, No. 510 of October 16, 2009, "On Improving Control (Supervisory) Activity in the Republic of Belarus":

- State supervision of telecommunications is performed by the State Inspectorate of the Republic of Belarus for Telecommunications of the Ministry of Communications and Informatization
- Control (supervision) over the fulfilment by licensees of licensing legislation, licensing requirements and conditions for the licensed type of activity is performed by the Ministry of Communications and Informatization of the Republic of Belarus and the Operational and Analytical Centre under the President of the Republic of Belarus.

The rules and regulations applicable to the retention of connection or call data (including Internet connection data) are as follows:

- Decree of the President of the Republic of Belarus No. 129 of 03.03.2010 "On approval of the Regulation on the procedure for interaction of telecommunication operators with bodies that carry out operational search activity".[24]
- Decree of the President of the Republic of Belarus No. 6 of December 28, 2014 "On Urgent Measures to Counter Illicit Drug Trafficking".
- Resolution of the Ministry of Communication and Informatization of the Republic of Belarus No.6 dated February 18, 2015 "On approval of the Instruction on the

[22] http://www.pravo.by/document/?guid=3871&p0=H10500045

[23] http://oac.gov.by/files/files/pravo/ukazi/Ukaz_196.htm

[24] http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm

procedure for the formation and storage of information about information resources visited by users of Internet services."[25]

- Decree of the President of the Republic of Belarus of 1 February 2010 No. 60 "On measures on improving the use of the national segment of the Internet."[26]
- STB 2271-2016 "Telecommunication networks. System of technical means for ensuring operational-search activities. Technical requirements."

Providers of Internet services perform identification of subscriber devices when providing Internet services, accounting and storage of information about subscriber devices, as well as information about the provided Internet services. The owners of points of collective use of Internet services (such as internet cafe's) or their authorised persons carry out identification of users of Internet services at points of collective use, accounting and storage of personal data of users of Internet services, as well as information about Internet services provided by points of collective use. The specified information is retained for one year from the date of rendering of the Internet services, as per Paragraph 6 of the Decree of the President of the Republic of Belarus No. 60 of 1 February 2010 "On measures to improve the use of the national segment of the Internet"[27]. Access to stored data is made in accordance with Articles 209, 210 and 212 of the Code of Criminal Procedure of the Republic of Belarus[28]. Penalties for non-compliance are specified in Article 23.4 of the Code of the Republic of Belarus on Administrative Offences[29].

In accordance with clauses 75-77 of the Regulation on licensing certain types of activities approved by the Decree of the President of the Republic of Belarus of 1 September 2010, No. 450, "On licensing of certain types of activities", a state body, within the limits of their competence, upon identifying a violation by a licensee, of their licensing requirements and conditions, and in accordance with established procedure can instruct the licensee to eliminate the violations identified and determine the term for their elimination (Paragraph 75). If in the established period the licensee does not eliminate the violations indicated in the instruction, or a written notification was not provided to the licensing or other supervisory body, the licensing authority on its own initiate or on the proposal of another supervisory authority can decide to suspect the license for up to six months (Paragraph 76). If in the established period the licensee does not eliminate the violations that entailed suspension of the license, the licensing authority that issued the license can take a decision to terminate it (Paragraph 77). Article 12.7 of the Code of the Republic of Belarus on Administrative Offences provides for administrative liability in the form of a fine for violation of the rules and conditions for the implementation of activities specified in licenses, if there is no crime in these acts.

The rules that apply in relation to interception of Internet data and/or call content are:

- The law of the Republic of Belarus No. 307-3 of July 15, 2015 "On the operational search activity"
- Decree of the President of the Republic of Belarus of 03.03.2010 No. 129 "On approval of the Regulation on the procedure for interaction of telecommunications operators with bodies that carry out operational search activities"[30]

[25] http://kodeksy-by.com/norm_akt/source-Minions%20RB/type-%20Resolution%20/%206-18.02.2015.htm

[26] http://oac.gov.by/files/files/pravo/ukazi/Ukaz_60.htm

[27] http://oac.gov.by/files/files/pravo/ukazi/Ukaz_60.htm

[28] http://etalonline.by/?type=text&regnum=HK9900295#load_text_none_1_3

[29] http://www.pravo.by/document/?guid=3871&p0=hk0300194

[30] http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm

The cost of the required equipment is paid by the ISPs and the law enforcement agency, in accordance with Articles 10-11 of the Decree of the President of the Republic of Belarus of 03.03.2010 No. 129 "On approval of the Regulation on the procedure for interaction of telecommunications operators with bodies that carry out operational search activities"[31]. The control of telecommunication networks is carried out in accordance with the resolution on conducting an operational search activity with the sanction of the prosecutor or his deputy. Decisions on the conduct of the operational search measures, on its suspension, resumption or termination shall be made by an official of the body that carries out the operational search activity. The decision to conduct operational search measures must be motivated in accordance with Article 19 of the Law of the Republic of Belarus of July 15, 2015, No. 307-3 "On operative investigative activities". The control of telecommunication networks conducted with the connection to telecommunication networks of citizens or organisations providing telecommunication services is carried out using the forces and means of the internal affairs bodies of the Republic of Belarus, the state security bodies of the Republic of Belarus and the Operational and Analytical Centre under the President of the Republic of Belarus in accordance with acts of legislation on operational search activities (in particular Article 31 of the Law of the Republic of Belarus of July 15, 2015, No. 307-3 "On operative investigative activities").

The requirement for the protection of commercial information that are applicable to the security of data held by ISPs for business purposes are general and are provided for in Chapter 7 of the Law of the Republic of Belarus of November 10 2008, No. 455-3 "On information, informatisation and protection of information"[32]. The obligation to report crime when an ISP becomes aware of a crime conducted on or via its infrastructure is specified in Articles 166 and 170 of the Code of Criminal Procedure of the Republic of Belarus[33].

There is no cybersecurity strategy however aspects of providing computer security are included in the concept of national security of the Republic of Belarus, approved by the Decree of the President of the Republic of Belarus of November 9, 2010 No. 575 "On the Approval of the National Security Concept of the Republic of Belarus"[34].

It is possible for an ISP to take down illegal content upon a request to do so in accordance with the Decision of the Operational Analytical Centre under the President of the Republic of Belarus, the Ministry of Communications and Informatization of the Republic of Belarus of February 19, 2015 No. 6/8 "On approval of the Regulation on the procedure for limiting access to information resources (their constituent parts) located in the global computer network Internet"[35]. The same mechanism can be used for fast takedown of illegal content.
ISPs share with each other information about on-going threats or incidents. State authorities and ISPs are given the opportunity to use an automated system for exchanging information in computer incidents. The National Centre for Responding to Computer Incidents of the Republic of Belarus has a website[36] where an individual or legal entity can leave its report.

6.4 Georgia

The principle legal instruments regulating the obligations of Internet Service Providers are:

[31] http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm
[32] http://oac.gov.by/files/files/pravo/zakoni%20/zakon_455-3.htm
[33] http://etalonline.by/?type=text&regnum=HK9900295#load_text_none_1_3
[34] http://kgb.by/ru/ukaz575/
[35] http://oac.gov.by/files/files/pravo/post_oac/Post_OAC_6.8.htm
[36] https://cert.by/?lang=en

- The Law of Georgia "On Electronic Communication"[37]
- The National Commission for Communications of Georgia ("the Commission") Resolution No. 3 "on provision of services and protection of consumer's rights in electronic communications", 17th March 2006, Tbilisi.

A person wishing to obtain authorisation for the provision of electronic communications networks and means or the delivery of services by electronic communications networks and facilities shall submit to the Commission a declaration, the form of which is approved by the Commission. The Law of Georgia "On Electronic Communications" describes the role of the Commission at Article 11:

> "1. In the field of electronic communications, the Commission independently regulates the activities of authorised persons and the use of the radio-frequency spectrum and numbering resource by license holders and permission, including the adoption, monitoring and control of the implementation of normative and individual legal acts, limits of powers defined by this Law, established by the same Law and the Code of Georgia on Administrative Offenses of Sanctions for the revealed violations. (20.12.2011 N5546).
> 2. The main tasks of the Commission:
> A) Formation, preservation and development of a competitive environment in the field of providing electronic communications networks and facilities and electronic communications services;
> B) Ensuring the delivery by authorized e-communication service providers to end-users (including persons with disabilities) of quality services, a wide range of services and affordable tariffs for them;
> C) Assistance to the implementation by authorized persons, owners of electronic communication networks and means of effective investment in the introduction of innovative technologies.
> 3. The main functions of the Commission:
> A) Authorization of activities in the field of electronic communications;
> B) Management of exhaustible resources and ensuring their effective use, optimal allocation and effective redistribution of the radio-frequency spectrum in order to ensure the introduction of innovative electronic communication technologies and the development of a competitive environment, the establishment of transparent and non-discriminatory conditions and rules for acquiring the right to use the radio-frequency spectrum or numbering resource, issuance and cancellation of relevant licenses and permits for the use of exhaustible resources; (20.12.2011 N5546)
> C) Conducting research and analysis of the relevant segments of the services market, identifying authorized persons with significant market power, in order to ensure competition, the assignment of specific obligations specified in this Law and supervision and control over their implementation;
> D) Ensuring certification, standardization and metrological maintenance of electronic communication means in accordance with the regulations for the certification of radio installations and telecommunications terminal equipment;
> E) Regulation of technical, economic and legal relations related to admission to the elements of electronic communications network or interconnection;
> F) The resolution within the limits of their authority of disputes arising between the authorized persons performing activities in the sphere of electronic communications, and also by these persons and the consumer;
> G) Overseeing compliance with the conditions for authorization of activities in the field of electronic communications, licensing and licensing conditions, and carrying

[37] https://matsne.gov.ge/en/document/view/29620

> out, in case of violation of their activities, provided for by law; (20 December 2011 No. 5546)
> H) Open, public and transparent relations with the society;
> I) Coordination of electromagnetic compatibility of radio-electronic facilities and arrangements for its international legal protection;
> J) Representation of Georgia in the international organizations operating in the field of electronic communications and the protection of its interests within its authority and competence delegated by the Government of Georgia;
> K) Determining the rules for establishing amateur radio communications and using amateur radio stations;
> M) The resolution of disputes between the owners of the license and the permission concerning the use of the right granted by the license and the permission, within the limits of authority in accordance with the rules established by Chapter VI of this Law; (20.12.2011 N5546)
> O) Approval of the provision on portability of subscriber numbers, identification of a system of a central database on the portability of subscriber numbers in order to open tender, registration of a contract with him and monitoring of the performance of contractual terms. (8/04/2011 N4526)
> P) In case of establishing on the international and regional market of electronic communications a provision that has a significant and not a continuing negative impact on the activities of authorized persons operating in the electronic communications market in Georgia until the removal of this significant and not overcoming negative impact, the establishment of a reasoned decision, adopted in the course of public administrative proceedings, appropriate effective regulations for all relevant authorized persons operating in the field of e- ics- communications. (20.12.2011 N5546)
> P) Control of the degree of protection of classified information in the field of electronic communications."

The Commission does not have the authority to compel and ISP to respond to requests for access to subscriber data.

The document "on provision of services and protection of consumer's rights in electronic communications"[38] contains rules and regulations regarding blocking, deletion or prevention of certain types of information being hosted or made accessible online (Articles 10(1), 10(2), 10(3) and 25). If an ISP is informed of illegal content being hosted or cached on their network, they must remove it. ISPs are not legally obliged to report illegal content, but if such content is identified it must be removed nonetheless. Art 25 of this regulation stipulates the following obligations for Service Providers:

> "Article 25. Protection of Rights and Legitimate Interests of Consumers (9.11.2007 No 7)
> (..)
> 3. Service provider shall be obliged to ensure the secrecy and safety of the information transmitted by consumers. The tapping of telephone conversation (…)
> 4.Service provider shall be obliged to:
> (a) ensure the conformity of service with the Legislation in force;
> (..)
> (e) ensure the operation of a transparent and effective mechanism for the consideration of consumers complaints in order timely and legally to solve the complaints in question;

[38] https://www.gncc.ge/uploads/other/1/1033.pdf

(f) ensure the presence of a mechanisms of restricted access to the services intended for adults;
(g) to respond to the received information concerning the allocation of inadmissible production and adopt appropriate measures in order to eliminate it;
(h)protect the integrity and impenetrability of the network and prevent any unauthorized use of networks and facilities;
(i) take measures to protect consumers from any possible risks posed by service; on request, to provide consumer with filtering software;
(j) if, for technical reasons, a service provider cannot ensure the protection of the network in his possession, he must inform the consumers about the existing risk of unauthorized access to the network on the part of third persons; in case of availability of relevant technical possibility, the service provider must offer to the consumers concerned the service designed to protect consumers from such unauthorized access;
5. Based on the notification from a consumer, service provider shall address the issue and adopt all available measures in order to prevent the use of his network for:
(a) unauthorized access;
(b) transmission of a message containing inadmissible production; and
(c) the intimidation, insult and other humiliating acts in respect to a consumer.
6. With due consideration of legal interests of consumer, service provider shall be entitled at his discretion to determine the rules for the provision of certain services to consumers, which rules must not contradict the Legislation in force and may involve additional rights or obligations"

The obligations of ISPs to protect the secrecy of the communications of their subscribers are reflected in:

- The Law of Georgia "on Protection of Personal Data"[39]
- The Law of Georgia "On Electronic Communications", Article 8(1) states that "Information on consumers of electronic communications networks, as well as information transmitted by the consumer through these networks, is secret and its protection is guaranteed by the legislation of Georgia."
- Decree No. 3 "on provision of services and protection of consumer's rights in the field of electronic communications", Articles 8 and 25, Paragraph 3 states "The provider of services shall ensure the confidentiality of transmitted information about the client and his protection. Receiving, including disclosure of information is permitted in accordance with applicable law."

This duty to protect the secrecy of communication is overseen by the inspector for the protection of personal data, as well as by the National Commission for Communications of Georgia.

In cases of violation of the legislation of Georgia in the field of electronic communications including requirements and obligations determined by decisions of the Commission, or violation by the license holder of licensing conditions, the Commission has the right to warn the offender in writing. The Commission also has the power, should a violation be repeated within a one year period, to impose a fine in the amount of 0.5% of the licensee's income for the previous 12 calendar months (as determined by the Tax Code of Georgia) but not less than 3,000GEL and not more than 30,000GEL (Article 45) and the suspension and cancellation of the authorisation to operate (Article 19).

[39] https://matsne.gov.ge/en/document/view/1561437

Article 5 of Resolution No. 3 "on provision of services and protection of consumer's rights in electronic communications" states that "The Service Provider must store at least the following data (a) first and last name; (b) provision of services and types of services; (c) the number and cost of the service, the date and the total amount of VAT (d) the period for payment or the date". It is further stated that "The provisions of clauses (a) and (b) the information is protected from the termination of the service contract within 1 year, and (c) and (d) the information is protected from rendering services for 3 years." Failure to retain the required data by the ISP can be sanctioned in the first instance by a written warning and then by a fine, as described above.

On the request of an authorized state body, and taking into account submitted documents, an ISP can limit the access to IP addresses where illegal content is located. ISPs apply the takedown procedure upon submission of a court order.

Information about on-going threats or incidents is shared between ISPs informally. At the moment, there is no uniform mechanism for exchange of data related to incidents between ISPs. There is an obligation in ISPs in respect to international call terminations for the purposes of financial fraud prevention imposed by a Commission decision.

Georgia has a National Cybersecurity Strategy 2017-2018 and an Action Plan that were adopted by the Georgia Government by Resolution No. 14 of 13 January 2017.

6.5 Moldova

The principle legislation regulating the obligations of Internet Service providers is Law no. 20-XVI dated 03.02.2009 on preventing and fighting cybercrime[40]. Other relevant legislation is published on the website of the National Regulatory Agency for Electronic Communications and Information Technology of the Republic of Moldova[41].

According to Article 6 of Law no. 20-XVI dated 03.02.2009, ISPs must make users aware of the conditions of access as follows: "Computer system owners whose access is prohibit or restricted for certain categories of users are required to alert users about the legal conditions of access and use and the legal consequences of unanswered access to such computer systems. The warning must be accessible to any user." According to Article 11 of the same law, "Violation of this law entails disciplinary, civil, administrative or criminal liability under law."

ISPs are required to report certain violations to competent authorities according to Article 7 of Law no. 20-XVI, paragraph 1 (b) "(1) Service providers are required to: (..) b) To communicate to the competent authorities the information on computer traffic, including data on illegal access to information in the information system, attempts to introduce illegal programs, violation by responsible persons of the rules on the collection, processing, storage, dissemination, distribution of information, or the rules of protection of the information system according to the status of the information or its degree of protection, if they have contributed to the acquisition, distortion or destruction of the information or caused other serious consequences, disruption of the functioning of the information systems, other computer crimes;"

Furthermore, ISPs are required to facilitate the monitoring of the services they offer as described in Article 7 of Law no. 20-XVI, as follows "f) To ensure the monitoring, surveillance

[40] http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=333508

[41] http://en.anrceti.md/fileupload/1?page=1

and storage of traffic data over a period of 180 days to identify service providers, service users and channel through which communication has been transmitted; g) To ensure the decipherment of the computer data contained in the network protocols with the preservation of these data for a period of 90 days." If an ISP detects illegal content, Article 5 of the same law requires them to report this content; "In the framework of cybercrime prevention and fighting activities, the competent authorities, service providers, non-governmental organizations, other civil society representatives cooperate through information exchange, experts, through joint investigation of cases and identification of offenders, training personnel, through initiatives to promote programs, practices, measures, procedures and minimum standards for the security of information systems, through cybercrime information campaigns and the risks to user of computer systems, through other activities in the field." There appears to be no obligation to monitor for illegal content for ISPs themselves.

ISPs are obliged to protect the privacy of personal data in accordance with the Law on Personal Data Protection, No. 17-XVI, 15.02.2007[42].

There are no rules for interception of Internet data and/or call content ("legal interception"). In practice interception is performed on the basis of the Criminal Procedure Code, No. 122-XV, dated 14.03.2003:

> "Article 132. Interception and Communication Recording
> (1) Interception and communication recording involves the technical means through which the content of conversations between two or more persons can be found and their recording involves the storage of information obtained from interception on a technical support.
> (2) The provisions of paragraph (1) shall apply exclusively to criminal cases having as their object the prosecution or the trial of persons against whom there is data or evidence regarding the commission stipulated in the following articles of the Criminal Code: art.135–145, 150, 151, 158, 164–1651, art.166 paragraph (2) and (3), art.1661, 167, art.171 paragraph 2) and (3), art.172 paragraph 2) and (3), art.175, 1751, art.186 paragraph (3)–(5), art.187 paragraph (3)–(5), art.188, 189, art.190 paragraph (3)–(5), art.191 paragraph (2) letter d) and paragraph (3)–(5), art.1921 paragraph (3), art.2011 paragraph (3), art.206, 207, 2081, 2082, art.216 paragraph (3), art.217 paragraph (3), art.2171 paragraph (3) and (4), art.2173 paragraph (3), art.2174 paragraph (2) and (3), art.219 paragraph (2), art.220 paragraph (2) and (3), art.224 paragraph (3) and (4), art.236, 237, art.2411 paragraph (2), art.2421–243, art.244 paragraph (2), art.248 paragraph (2)–(5), art.259–2611, 275, 278–2791, art.2792 paragraph (3) letter b), art.280, 282–286, 289–2893, art.290 paragraph (2), art.292, 295–2952, art.303 paragraph (3), art.306–309, 318, 324–328, 333–335, art.3351 paragraph (2), art.337–340, 342–344, art.352 paragraph (3), art.362, 3621, art.368 paragraph (2), art.370 paragraph (2) and (3). The list of crime components is exhaustive and can only be changed by law.
> (3) The communication of the suspect, the accused, or others, including those whose identity has not been established, may be subject to interception and registration, of which there are data that may reasonably lead to the conclusion that they contribute in a way to the preparation, commission, favouring or concealing the offences referred to in paragraph (2), either receive or transmit relevant and important information for the criminal case.
> (4) The communication of the victim, the injured party, his relatives and his family members as well as the witness may be intercepted and recorded if there is imminent danger to his/her life, health or other fundamental rights if the crime is to

42 http://en.anrceti.md/files/filefield/3.1.7%20%20Law%20on%20Personal%20Data%20Protection_0.doc

be prevented or if there is the obvious risk of irremediable loss or distortion of evidence. The interception and recording of communications within the meaning of this paragraph shall be ordered in accordance with the procedure provided for in Article 132a and only with the written prior agreement or prior written request of the persons referred to in this paragraph.
The measure ordered pursuant to this paragraph shall be terminated immediately upon the disappearance of the basis on which its authorization was based or at the express request of the person in respect of whom the measure was ordered."

The cost of equipment required to facilitate legal interception is borne by the ISP. The prosecutor serves warrants for interception, as described in the Criminal Procedure Code, No. 122-XV, dated 14.03.2003:

"(1) The interception and recording of communications shall be carried out by the criminal investigative body or by the investigative officer. The technical assurance of the interception of communications shall be carried out by the authority empowered by law with such attributions, using special technical means. The representatives of the subdivision within the institution authorized by law, who technically provide for the interception and registration of communications, as well as the persons who directly perform listening to recordings, the criminal investigation officers and the prosecutor are bound to keep the secret of the communications and bear responsibility for the breach of this obligation.
(2) In order to ensure interception and registration of communications, the criminal investigation body or the prosecutor shall submit to the body authorized by law the extract from the investigative judge decision, certified by him, regarding the ordering of intercepting the communications. The letter enclosed to the extract from the investigative judge decision shall contain a statement with respect to criminal liability of the person who will technically perform the special investigative measure. The extract from the decision must contain the name of the court and the name of the examining investigative judge, the date and time of the issue of the order, details of the examination of the prosecutor's request to authorize the measure, the identification of the subscriber or of the technical unit through which the communications to be intercepted are kept, the duration of the interception, the person or the criminal investigation body responsible for the execution of the decision, the signature of the examining investigative judge and the stamp of the court.
(3) If other information such as identification data of subscribers or persons who have received communications on the subject of interception and their location as well as other data can be obtained in the process of intercepting and recording communications, the investigating judge may order to intercept communications and obtain this information.
(4) The technical subdivision of the body empowered by law to perform the interception and recording of communications shall send to the criminal prosecution body the signal of the intercepted communications and other information indicated in the extract from the decision of the investigative judge in real time, without registering them.
(5) Information obtained in the process of intercepting and recording communications can be listened and viewed in real-time by the criminal investigation body and the prosecutor.
(6) The information obtained in the process of intercepting and recording communications shall be transmitted by the technical subdivision that carried out the interception of communications to the criminal investigating officer or the prosecutor on the packed information carrier, sealed with the stamp of the technical subdivision and indicating the serial number of the carrier.

(7) Within 24 hours after expiring the intercept authorization period, the criminal investigative body or the prosecutor draws up, at the end of each authorization period, a report on the interception and recording of communications.

(8) The minutes of interception and recording of communications must contain: date, place and time of the filing, the position of the person who carried out the special investigative measure, the number of the criminal case within which the special measure was taken, the mention of the prosecutor's order and the decision of the investigative judge on the authorization of the special measure, identity and technical identification data of the subject whose communications have been intercepted and recorded, the period of interception, the use of technical means, other relevant information obtained by intercepting and recording communications with respect to identifying and / or locating subjects, the quantity and identification number of the material carriers on which the information was recorded, the number of shorthand communications. The shorthand communications, which is relevant for the criminal case, is attached to the minutes.

(9) The shorthand of communications is the full reproduction, in written form, on paper, of intercepted and recorded communications that are important for the criminal case. The shorthand of the communications shall indicate the date, time and duration of the communication, the names of the persons, if known, whose communications are stenographied, and other data. It is forbidden to stenograph the communications between a lawyer and the person he / she defends. Each page of the intercept report and the shorthand shall be signed by the person who made it. The original support on which the intercepted communications were recorded is enclosed to the minutes, mentioning the packaging and sealing.

(10) Intercepted and recorded communications are played back in the language of the communication. If communication has taken place in a language other than that of the State, the communication shall be translated into the language in which the criminal proceedings are conducted by an authorized translator.

(11) At the end of the authorized period for interception and recording of the communication, the criminal investigation body shall submit to the prosecutor the minutes of the interception and the original support on which the information was recorded.

(12) The prosecutor, after verifying the content of the minutes and the transcript with the contents of the records by ordinance, decides on their relevance for the criminal case and disposes which communications are to be transcribed on a special support.

(13) The intercepted and recorded communications will be kept entirely on the original support submitted to the criminal investigation body by the technical subdivision. This support shall be retained by the investigating judge who authorized the special investigative measure.

(14) The intercepted and recorded communications that have been stenographed by the criminal investigating body and which were considered by the prosecutor to be relevant for the criminal case are transcribed by the technical subdivision of the criminal investigating authority on a separate support which is attached to the case materials and shall be kept at the prosecutor in charge of the prosecution.

(15) Within 48 hours from the end of the period of authorization of interception and registration, the prosecutor shall provide the judge with the minutes and the original support on which the communications were recorded. The Investigation Judge shall make a statement on compliance with the legal requirements for the interception and recording of communications by the criminal investigation body and shall decide which of the recorded communications are to be destroyed, designating the persons responsible for the destruction. Dismissal of information based on the decision of the investigative judge is recorded by the person responsible in the minutes, which is attached to the criminal case."

The Law on Electronic Commerce No. 284-XV, dated 22.07.2004 specifies the rules applying to the retention of data by ISPs for business purposes, as well as specifying the security of that data. The Law on Preventing and Fighting Cybercrime, No. 20-XVI, dated 03.02.2009 specifies the rules that apply when an ISP becomes aware of a data breach other criminality conducted on or via its infrastructure. The main obligation is to report these incidents in accordance with Article 7 of that law.

The enforcement measures and penalties that can be used to sanction ISPs for non-conformance with required legal obligations are specified in the Civil Code of the Republic of Moldova, No. 1107-XV, 06.06.2002.

6.6 Ukraine

The principal legal instruments regulating the obligations of Internet Service Providers are:

- The Law of Ukraine "On Telecommunications"[43]
- Rules for the provision and receipt of telecommunications services, Decree of the Cabinet of Ministers of Ukraine 11.04.2012, No. 295, with changes.[44]
- Decision of NCCR (the National Regulator in the Telecommunications Field) 01.11.2012, No. 560 "On approval of the procedure for maintaining the register of operators, telecommunications providers and the recognition of the decision of the NCCR as of 11.11.2010, No. 514", register in the Ministry of Justice of Ukraine on 22.11.2012, No. 1958/22270[45].
- Decision of the NCCR 11.11.2010, No. 513 "On approval of licensing conditions for carrying out activities in the field of telecommunications for the provision of services for the maintenance and operation of telecommunication networks, terrestrial television and broadcasting networks, wire broadcasting and television networks" registered in the Ministry of Justice of Ukraine on November 30.2010, No. 1200/18495[46].
- Rules for the implementation of activities in the field of telecommunications (activities to provide Internet access services), approved by the decision of the National Commission, which carries out state regulation in the field of communication and information, on December 10, 2013, No. 803, registered with the Ministry of Justice of Ukraine on February 03, 2014 under No. 207/24984[47].

The ISP activities are carried out subject to the inclusion in the register of operators, telecommunications providers, which is maintained by the NCCR (the National Regulator in the Telecommunications Field), and in cases specified by law, also with appropriate licenses and/or permits. The telecommunications operator is required to obtain a license to provide services for the maintenance and operation of telecommunications networks, broadcasting networks, wire broadcasting and television networks. Part 7 of Article 42 of the Law of Ukraine "On Telecommunications" provides for an exceptional list of activities that are subject to licensing.

Clear rules and mechanisms for blocking, removing or preventing hosting of certain categories of information are not defined by law, except for blocking information that violates copyrights and related rights, as well as restrictions on the access of subscribers of

[43] http://zakon3.rada.gov.ua/laws/show/1280-15

[44] http://zakon2.rada.gov.ua/laws/show/295-2012-%D0%BF

[45] http://zakon3.rada.gov.ua/laws/show/z1958-12

[46] Http://zakon3.rada.gov.ua/laws/show/z1200-10

[47] http://zakon2.rada.gov.ua/laws/show/z0207-14

subscribers to resources through which child pornography is distributed. According to Clause 18 of the first part of Article 39 of the Law of Ukraine "On Telecommunications" operators, telecommunications provides are obliged to restrict access of their subscribers to resources through which the distribution of child pornography is carried out on the basis of a court decision. A number of other legislative and regulatory acts establish the ability and duty of the ISP to block, delete information from the Internet segment, restrict access to certain resources:

- Article 34 of the Constitution of Ukraine[48].
- Item 4.5 of the Cybersecurity Strategy of Ukraine, approved Decree of the President of Ukraine of March 15, 2016, No. 96/2016[49].
- Decree of the President of Ukraine of 15.05.2017, No. 133/2017 "On the decision of the National Security and Defence Council of Ukraine of April 28,2017" on the application of personal special economic and other restrictive measures (sanctions) "establishes a prohibition to Internet providers providing access services Users of the Internet to resources according to the list established in the decision of the National Security and Defence Council[50].
- The Law of Ukraine "On Copyright and Related Rights"[51].

Part four of Article 40 of the Law of Ukraine "On Telecommunications" clearly states that operators, telecommunications providers are not responsible for the content of information transmitted by their networks. The responsibility of the provider of hosting services and the owner of the website comes in the event of failure to comply with the requirement for termination of copyright infringement and related rights using the Internet according to the procedure established in Article 52-1, 52-2 of the Law of Ukraine "On Copyright and Related Rights". Legislation does not directly provide for accountability, but, in connection with the adoption of a number of regulations, the possibility exists in which case, a court takes the final decision. In case of the distribution of Child Pornography, there is also an obligation to terminate the offending account, upon the order of competent authorities. In relation to copyright infringements there is an obligation to monitor hosted information for infringements, according to Articles 52-1, 52-2 of the Law of Ukraine "On Copyright and Neighbouring Rights".

Article 34 of the Law of Ukraine "On Telecommunications" defines the general framework for protection of information about the consumer. Additionally, the following Acts specify additional duties to protect personal data:

- The Law of Ukraine "On access to public information"[52] (Articles 7 and 10)
- The Law of Ukraine "On Information"[53]
- The Law of Ukraine "On Protection of Personal Data"[54]
- The Code of Criminal Procedure of Ukraine (Article 162)[55] states that "The secret protected by law contained in things and documents includes: (7) Information held by telecom operators and providers, about communication, subscriber, provision of telecommunications services, including services, their duration, content, transmission routes, and the like; (8) personal data of a person who has in her personal

[48] http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
[49] http://www.president.gov.ua/documents/962016-19836
[50] http://www.president.gov.ua/documents/1332017-21850
[51] http://zakon3.rada.gov.ua/laws/show/3792-12
[52] http://zakon5.rada.gov.ua/laws/show/2939-17
[53] http://zakon3.rada.gov.ua/laws/show/2657-12
[54] http://zakon5.rada.gov.ua/laws/show/2297-17
[55] http://zakon3.rada.gov.ua/laws/show/4651-17/paran1602#n1602

possession or in the personal data base that is located at the owner of personal data."

Operators, telecommunications providers should ensure and bear responsibility for the safety of information regarding the consumer received at the conclusion of the contract, rendered telecommunication services, including the receipt of services, their duration, content, transmission routes and the like. The telephone directories intended for promulgation, including electronic versions and databases of information and reference services, may contain information on the name, patronymic, address and telephone number of the subscriber in the event that the agreement on provision of telecommunication services contains the consumer's consent to publication of such information. During the automated processing of information about subscribers, the telecommunications operator ensures its protection in accordance with the law. The consumer has the right to freely exclude information about themselves completely or partially from electronic versions of databases.
ISPs are required to keep records of the telecommunications services provided during the statute of limitation period defined by law and provide information on the telecommunication services provided in accordance with the procedure established by law. The general limitation period is three years.

The rules applying in relation to the interception of Internet data and/or call content are defined in Articles 263-265 of the Code of Criminal Procedure of Ukraine[56]. The obligation of the ISP to provide the technical ability to perform lawful interception is specified in part 4 of Article 39 of the Law of Ukraine "On Telecommunications" as follows: "Telecommunications operators are obliged to establish for their own means, on their telecommunications networks, the technical means necessary for the implementation of operational search activities by the authorized bodies, and to ensure the operation of these technical means, as well as within their powers to facilitate the conduct of operational search activities and prevent the disclosure of organizational and tactical methods for their conduct. Telecommunications operators are obliged to ensure the protection of specified technical means from unauthorized access."

In practice, based on the definition of the investigating judge within the framework of a criminal case, information is removed by authorised bodies of the National Police and security agencies. The order of the investigating judge is made on the proposal of the prosecutor. The cost of required equipment and transmission is borne by the ISP.
When sending a request for access to data held by an ISP, law enforcement and control authorities should maintain the following principles:

1. Request to the National Police
    a. The presence in the production of the operational search case;
    b. Entering information about criminal proceedings in the ERDR;
2. Request of the Security Service of Ukraine
    a. Receive data and information necessary to ensure the national security of Ukraine;
    b. When carrying out measures to combat terrorism and finance terrorist activities;
    c. Presence of counterintelligence;
    d. The presence in the production of the operational search case;
    e. Entering information about criminal proceedings in the ERDR;
3. Request of the Anti-Monopoly Committee of Ukraine
    a. When conducting research;
    b. The existence of a case of violation of the anti-monopoly legislation

[56] http://zakon3.rada.gov.ua/laws/show/4651-17/paran2413#n2413

The procedure for processing the request by the competent authorities is not provided for by law, except for the rules of office-work that are established by regulatory and legal acts and internal documents by the competent body (i.e. the signature of the authorized person, the details of the document, etc.). Legislation establishes cases according to which the ISP provides information to law enforcement and supervisory bodies for the performance of their tasks and powers:

- Clauses 5 and 7 part 3 of Article 19 of the Law of Ukraine "On Telecommunications"
- Clause 1 of the clause on the NCCR, Decree of the President of Ukraine of 23.11.2011, No. 1067/2011[57].
- Articles 2 and 23 of the Law of Ukraine "On the National Police"[58].
- Paragraphs 2 and 6 of the Regulation of the National Police, Decree of the Cabinet of Ministers No. 877 of October 28, 2015.
- Part 1 of Article 8 of the Law of Ukraine "On Operative-Search Activity"[59].
- Part 2 of Article 93 of the Code of Criminal Procedure of Ukraine[60].
- Paragraph 3 of Part 1, Paragraph 1 of Part 2 of Article 25 of the Law of Ukraine "On the Security Service of Ukraine"[61].
- Paragraph 5 of Part 2 of Article 7 of the Law of Ukraine "On Counterintelligence Activities"[62].
- Articles 22, 22-1 of the Law of Ukraine "On the Antimonopoly Committee of Ukraine"[63].

Administrative liability is available as an enforcement measure to sanction an ISP for non-conformance with requirements to provide access to data in response to requests from a competent authority.

There are no legislatively established rules relating to the retention of data for business purposes. General legislative provisions provide an obligation for an ISP, in cases where a crime is detected being conducted on or via its infrastructure, to report to the relevant competent authority. The national regulator has no legislative right to require the ISP to fulfil a request for access to information about a subscriber, which is sent by a law enforcement or regulatory authority. Only for the fulfilment of its own tasks and powers can the national regulator receive such information from the ISP on its own written request.

The Cybersecurity Strategy of Ukraine was approved by the Decree of the President of Ukraine No. 96 of March 15, 2016[64]. Point 4.5 of the Cybersecurity Strategy provides for the introduction of a blocking by operators and telecommunications providers of certain (identified) information resources (information service) by a court decision. The blocking mechanism is not defined. Article 52(1) and 52(2) of the Law of Ukraine "On Copyright and Related Rights" specifies "the duty of the provider of hosting services and the owner of the website to prevent and stop infringements of copyright and related rights using the Internet on behalf of a person who considers his rights violated, with further appeal to the court." Paragraph 18 of Article 39 of the Law of Ukraine "On Telecommunications" provides for the

[57] http://zakon3.rada.gov.ua/laws/show/1067/2011
[58] http://search.ligazakon.ua/l_doc2.nsf/link1/T150580.html
[59] http://zakon3.rada.gov.ua/laws/show/2135-12
[60] http://zakon2.rada.gov.ua/laws/show/4651-17
[61] http://zakon5.rada.gov.ua/laws/show/2229-12
[62] http://zakon5.rada.gov.ua/laws/show/374-15
[63] http://zakon2.rada.gov.ua/laws/show/3659-12
[64] http://zakon2.rada.gov.ua/laws/show/96/2016

obligation to limit, on the basis of a court decision, the access of its subscribers to the resources through which child pornography is distributed.

7 Analysis and recommendations

7.1 Law enforcement access to data

From a criminal justice point of view, law enforcement agencies need to be able to gain access to data that is held by ISPs as part of investigations of various types. Such access needs to be balanced with safeguards (depending on the type of access required), and these safeguards are the topic of Section 0. The purpose of this section is to examine the obligations on ISPs to provide law enforcement access to data, the circumstances under which such access is granted and how access is made available in practice.

The analysis has been broken into several sub-sections, considering different types of access that may be required, ranging from subscriber identification to interception of content data. Preservation of data and blocking of illegal content are also considered.

7.1.1 Subscriber identification

The category of request most frequently made to ISPs by law enforcement agencies is a request for the subscriber identity data related to the use of a specific IP address at a particular time. There is often an obligation on ISPs to retain this information for a specified period of time and provide it, on request, to competent authorities. In some cases where there is no legal or regulatory obligation, a less formal Memorandum of Understanding can be put in place between the law enforcement authorities and ISPs.
The questionnaire requested information on the retention of Internet connection records, and the responses are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Retention Obligation	MoU[65]	No information provided	Legal Obligation [66]	No information provided	Legal Obligation [67]	Legal Obligation [68]

It was noted that where information was available there is either a legal obligation or an MoU in place already.
Related issues such as periods of data retention and safeguards to protect customer privacy are discussed elsewhere in this report.

[65] For IP connections there is no obligation for ISPs but the main operators have signed a Memorandum of Understanding with the police and undertook to keep information about source, destination IP address, time and duration in their database. The duration of retention is defined in the MoU, which is not available online.

[66] Internet service providers are required to identify subscriber devices when providing Internet services, accounting and storage of information about subscriber devices as well as information about the provided Internet services.

[67] Article 7(1)(a) of Law no. 20-XVI dated 03.02.2009 states that "(1)Service providers are required to: (a) to keep records of service users, …. (f)To ensure the monitoring, surveillance and storage of traffic data over a period of 180 days to identify service providers, service users and channels through which communication has been transmitted."

[68] In accordance with Paragraph 7 of the first part of Article 39 of the Law of Ukraine "On Telecommunications", operators, telecommunications providers are required to keep records of telecommunications services rendered within the limitation period determined by law and provide information on telecommunications services provided in accordance with the procedure established by Law."

Recommendation 1: ***Information is not available about how well the arrangements for law enforcement access to ISP data are working in practice, but where practical shortcomings are identified, it may be advantageous for countries to consider less formal cooperation methodologies to address these. For example, if there are difficulties identifying which ISP to request data from, a single point of contact could be established for all ISPs to accept law enforcement access requests. The single point of contact can then work with the ISPs to route the request to the appropriate ISP for handling.***

7.1.2 Preservation of data

Considering the rapid pace at which evidence in cybercrime cases can be permanently lost, it is recognised that there is a need for mechanisms to facilitate expedited preservation of data[69]. A procedure that enables preservation of data allows an instruction to hold data to be served on, for example, an ISP in anticipation of completion of due legal process. The preserved data does not necessarily need to be disclosed until the due legal process has been completed, depending on the circumstances and on national legislation.

Problems can arise with preservation of data because the volumes of data covered by the preservation request may be substantial and therefore the costs of storing and processing the data may also be substantial. Questions could arise as to who will bear these costs. Additionally, there have been cases in the past where preservation requests have been made but the preservation request has not been followed through with the completion of the due legal process, perhaps due to other unrelated aspects of the investigation failing to produce adequate results. In these cases, the ISP has undertaken a potentially lengthy preservation activity, which has ultimately been called off.

The questionnaire requested information on what rules apply in relation to a request from a competent authority for preservation of data by an ISP. The questionnaire also requested information on whether legislation imposes an obligation on ISPs to preserve data on request from a competent authority and who enforces this obligation. Finally, the questionnaire also requested information about what procedure must be followed for a competent authority to gain access to data that has been preserved by an ISP:

The results are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Rules in Place	Yes	No information provided	Yes	No information provided	No[70]	No
Legislative	Yes[71]	No	Yes[72]	No	Yes[73]	No[74]

[69] See for example Article 16 and 17 of the Council of Europe Budapest Convention on Cybercrime (http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561).

[70] The response to this question in the questionnaire indicates that there are no rules, however the subsequent questions about legislative basis and enforcement authority were populated as described in this summary table.

[71] RA Law on Electronic Communication, Article 50

[72] Presidential Decree No. 129 of 3 March 2010 on "Adoption of Statute Regulating the Procedures of Interaction between Telecommunications Operators and Agencies Carrying out Crime Detection Activities" and also Law of the Republic of Belarus No. 45-3 of 19 July 2005 "On Telecommunications"

Basis		information provided		information provided		
Enforcement Authority	National Security Agency	No information provided	State Security Committee, Operative and Analytical Centre[75]	No information provided	Prosecutor's Office, Police	Prosecutor's Office[76]
Access to Preserved Data	Court Order	No information Provided	Prosecutor's Order[77]	No information provided	Court Order	Police, Security Service or Antimonopoly Committee Order

Recommendation 2: ***Upon receipt of a request from a competent authority, the scope and cost implications of the request may not be immediately apparent to either the ISP or the competent authority concerned. To prevent unnecessary discussion at the time of the request, it is recommended that countries consider putting in place, in advance, rules to govern the cost of handling law enforcement requests at an ISP.***

7.1.3 Interception of Internet data/call content data

The purpose of this section is to consider the legal/regulatory basis and practical measures by which interception of Internet and call content data is achieved. Considering the intrusive nature of this measure, the requirement for content interception must be balanced with appropriate safeguards. The topic of safeguards is considered separately in Section 0.

Several categories of legal/regulatory rules were considered in the context of this study; firstly the rules that apply in relation to interception of Internet data and/or call content ("legal interception") and secondly the rules that create an obligation on ISPs to provide the technical ability to perform legal interception. The questionnaire requested that the participant countries provide information on these categories of rules, and the responses are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Basis for	Law[78]	No	Law[79]	No	Law[80]	Law[81]

[73] Law no. 20-XVI dated 03.02.2009 on preventing and fighting cybercrime

[74] Special laws obliging the ISP to ensure the storage of data at the request of the competent authority, as well as compensation for costs, are not available. The duty to preserve the data obtained during the investigative measures is established by part four of Article 263 of the Code of Criminal Procedure of Ukraine.

[75] These two agencies enforce the obligations within their respective competencies.

[76] The above mentioned legislation establishes the right to demand information and the obligation of the ISP to provide such information. In case of non-fulfillment, responsibility, penalties are provided for by the Criminal Procedure Code of Ukraine.

[77] Delivery of an order according to an adopted form signed by head of a competent authority and sanctioned by a competent public prosecutor.

Legal Interception		information provided		information provided		
Requirement to Provide Ability	License Condition[82]	No information provided	Law[83]	No Information Provided	Law[84]	Law[85]

The participant countries were asked to provide information about how legal interception is performed in practice and which agencies bear the cost of the required equipment (ISP, law enforcement authority, etc.).

The responses to these questions from the questionnaire are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine

[78] Article 50 (Interception, Wiretapping or Disclosure of Messages) of the Law on Electronic Communication states "no person other than a party to a message transmitted by any electronic communications means may intercept, tap or disclose the content of this message unless authorized to do so in writing by the parties to the message or by a court decision pursuant to the Law. In the cases and in accordance with the procedures prescribed by law all operators and service providers must grant law enforcement or security personnel access to any equipment, facilities, switches, routers or other similar equipment, including wave dropping devices."

[79] Article 31 of the Law of the Republic of Belarus No. 307-3 of 15 July 2015 "On Operational Search Activities", Article 214 of the Code of Criminal Procedure of the Republic of Belarus (Monitoring and Recording Communications), Presidential Decree No. 129 of 3 March 2010 "On Adoption of Statute Regulating the Procedure of Interaction between Telecommunications Operators and Agencies Carrying out Crime Detection Activities", Law of the Republic of Belarus No. 45-3 of 19 July 2005 "On Telecommunications"

[80] Although the response to the specific question in the questionnaire states "there are no rules for interception of Internet data and/or call content ('legal interception') the response to the next question cites Article 132(8) of the Criminal Procedure Code No. 122-XV dated 14.03.2003, that provides a legal basis for interception and communication recording.

[81] Articles 263, 264, 265 of the Code of Criminal Procedure of Ukraine (http://zakon3.rada.gov.ua/laws/show/4651-17/paran2413#n2413)

[82] PSRC regulation, license pre-conditions – "operator (ISP) has to cooperate with National Security Agency".

[83] Presidential Decree No. 129 of 3 March 2010 on "On Adoption of Statute Regulating the Procedure of Interaction between Telecommunications Operators and Agencies Carrying out Crime Detection Activities", Law of the Republic of Belarus No. 45-3 of 19 July 2005 "On Telecommunications".

[84] Criminal Procedure Code no. 122-XV dated 14.03.2003, Law no 20-XVI dated 03.02.2009 on preventing and fighting cybercrime and Law no. 59 dated 29.03.2012 on Special Investigative Activity.

[85] Part 4 of Article 39 of the Law of Ukraine "On Telecommunications" specifically states that telecommunications operators are obliged to establish for their own means, on their telecommunications networks, the technical means necessary for the implementation of operational search activities by the authorized bodies, and to ensure the operation of these technical means, as well as within their powers facilitate the conduct of operational search activities and prevent the disclosure of organizational and tactical methods for their conduct. Telecommunications operators are obliged to ensure the protection of specified technical means from unauthorized access." Additionally, the Decree of the President of Ukraine No. 8/2017 "On the Decision of the National Security and Defense Council of Ukraine of December 29, 2016" on the improvement of measures to ensure the protection of critical infrastructure facilities.

Legal Interception Practical Approach	Black Box[86]	No information provided	Black Box[87]	No information provided	No information provided[88]	No information provided[89]
Cost Borne By	ISP	No information provided	ISP and Law Enforcement [90]	No Information Provided	ISP	ISP[91]

NOTE: Recommendation 2 is also applicable to lawful interception.
Recommendation 3: *The practice and use of legal interception should be subject to a transparent regime and to independent oversight in order for society to have*

[86] Although the response in the questionnaire to the specific question on how legal interception is performed contains the answer "N/A", a response later in the questionnaire indicates as follows "Competent authority has direct access to the 'black box', which is installed on ISP connection with the upstream. But in order to have legal base, competent authority must have appropriate court decision."

[87] The response in the questionnaire was "The authority that is conducting crime detection activities delivers an order that is sanctioned by a prosecutor's office and sent to a competent authority or the ISP." This provides no information about how legal interception is performed in practice from a technical point of view. However it is possible to infer from the response to the question on who bears the cost that a Communication Monitoring System (a.k.a. "black box") is used.

[88] The response to the questionnaire cites the relevant provisions of the criminal procedure code, but does not provide any information about how interception is performed in practice.

[89] The response to the questionnaire states "Based on the definition of the investigating judge within the framework of the criminal case, information is removed by authorized bodies of the national police and security agencies, however no information is provided about how information is performed in practice.

[90] The operator carries out its own expense and other sources not prohibited by law" acquisition, installation maintenance and repair of Communications Monitoring System (CMS), except the remote CMS control points; protection of information on the tactics of conducting investigative activities, limiting the number of persons involved in the installation, maintenance and repair of CMS (in agreement with authorized units); work on the implementation of technical requirements for CMS in the telecommunications network; acquisition and operation of the channel-forming equipment located at telecommunication facilities for the establishment of communication channels with the remote CMS control points in accordance with the procedure agreed with the KGB and the Operations and Analysis Centre (p.10 of the Regulation on the Interaction of Telecommunication Operators with the Authorities Performing Investigative Activity, approved by the Decree of the President of the Republic of Belarus of March 3, 2010, No. 129). The KGB and the Operations and Analysis Centre, using funds allocated from the republican budget for their maintenance, and other sources not prohibited by law, acquire the remote CMS control points that are not part of the telecommunications facilities, channel-forming equipment for organizing communication channels between telecommunication facilities and remote points CMS management, with the exception of the channel-forming equipment located at the telecommunication facilities, and the authorized units perform work on the organization of communication channels between telecommunications objects and the remote CMS control points (with the participation of the operator and in accordance with the procedure agreed with him) operation of CMS and remote CMS control centers. Other authorized bodies, at the expense of funds allocated from the republican budget, and other sources not prohibited by law, acquire the equipment necessary to conduct operational search operations through remote points of command of the KGB SORM and the Operations and Analysis Centre (p.11 of the Regulation on the Interaction of Telecommunication Operators with the Authorities Performing Investigative Activity, approved by the Decree of the President of the Republic of Belarus of March 3, 2010, No. 129).

[91] The procedure for covering expenses has not been legislatively determined, in practice it is at the expense of the ISP.

insight into the balance struck between user privacy and protection and, on the other hand, the needs of the criminal justice authorities.

7.2 Liability Framework

The questionnaire asked about the liability regime that is applicable to Internet Services, with a view to establishing to what extent providers of these services are held liable for content or actions of their subscribers, and to what extent they are obliged to monitor these. Since, in the EU (and the US, to some extent), it is common to distinguish between several types of Internet providers (hosting, access and caching), and adopt specific, graded and proportional obligations in relation to their response to the detection or a report of illegal content, it was also asked if there were different obligations in place in relation to the type of ISPs involved.

The responses were varied, but in many cases no specific responsibilities exist for ISPs in relation to third party content. Rather: it is left entirely up to state actors to determine the legality of content, and, similarly, responses to such cases of illegal content (such as the takedown, making inaccessible or deletion of material or blocking of access) are mandated by competent authorities exclusively. The responses can be summarized as follows:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
ISP Liability for user content	None – based on Telecoms law and Net Neutrality requirements.	No information provided	Only upon notice by competent authority	No specific regulation.	No specific regulation.[95] Unclear.[96]	None – based on Telecommunications law
Basis for blocking or takedown	Court order.	No information provided	Request from defined authorities	Complaint of users, authorities.	None	Disconnection in cases of child pornography. Otherwise none.
Obligation to monitor	None	No information provided	None (But can be agreed contractually)	"For safety of information transmitted by consumers "[93]	For limited types of content, such as malware.[97]	None
Obligation to report illegal content	None, right to inform police.	No information provided	Only for "owners of internet resources" [92]	Obligation to respond to reports.[94]	No	None.

[92] According to paragraph 8 of the Decree of the President of the Republic of Belarus of December 28, 2014 No. 6 "On Urgent Measures to Counter Illicit Drug Trafficking" owners of Internet resources are required:
- to analyse the content of their information resources and prevent the use of their information resources for the dissemination of messages and / or materials aimed at illicit drug trafficking;
- to inform the internal affairs bodies of attempts to use their information resources to disseminate messages and / or materials aimed at illicit drug trafficking.

[93] Art 25 par 3.

[94] Art 25 par. 4 sub e, f and g: Service provider shall be obliged to: (e) ensure the operation of a transparent and effective mechanism for the consideration of consumers complaints in order timely and legally to solve the complaints in question; (f) ensure the presence of a mechanisms of restricted access to the services intended for adults; (g) to respond to the received information concerning the allocation of inadmissible production and adopt appropriate measures in order to eliminate it;

[95] Art. 20 of Law no. 20-XVI dated 03.02.2009 on preventing and fighting cybercrime, provides that Violation of this law attracts disciplinary, civil, administrative or criminal liability under the law. There is no mention of a regime governing third party content, however.

[96] Art. 20 of Law no. 20-XVI dated 03.02.2009 on preventing and fighting cybercrime, provides that Violation of this law attracts disciplinary, civil, administrative or criminal liability under the law. There is

ISP roles defined	No	No information provided	Partly (Reporting regime)	No	No	No

Recommendation 4: ***Rules for ISP liability for ISP content should be established that are horizontal and cover all types of content. In case such liability is made possible, it should be clearly addressed in criminal, civil (including copyright) and administrative law.***

Recommendation 5: ***If liability for user content is provided for, the responsibilities for ISPs for blocking and takedown should be clearly defined and be based on a clear legal basis for all types of illegal content available.***

Recommendation 6: ***Such obligations should be different depending on the type of service provided, and special care should be given to the legal basis for blocking of access to internet resources.***

Recommendation 7: ***General obligations to monitor for certain types of illegal content should be avoided where possible, and be specific in relation to their goals and legal basis where they are imposed nonetheless.***

Recommendation 8: ***Independent oversight or judicial control should be provided for, in order to safeguard freedom of speech, where blocking or monitoring obligations are imposed.***

7.3 Safeguards

The needs of law enforcement authorities to conduct their investigations must be balanced with appropriate safeguards. The need for appropriate safeguards, and the adoption of the principle of proportionality, has been repeatedly recognised[98]. The requirements of national legislation, including legislation protecting the privacy of personal data, also need to be considered.

no mention of a regime to takedown illegal content upon request of national authorities however. It is only provided as a measure of international cooperation in article 8 of the same law.

[97] Art 7. of Law no. 20-XVI dated 03.02.2009 on preventing and fighting cybercrime, provides that providers are to report computer crimes: " (1) Service providers are obliged: (..) b) to communicate to the competent authorities the data on the information traffic, including data on illegal access to information in the information system, on the attempts to introduce illegal programs, the violation by the responsible persons of the rules for collecting, processing, keeping, distributing, distributing information or rules of protection of the information system provided according to the status of the information or its degree of protection, if they have contributed to the acquisition, distortion or destruction of the information or caused other serious consequences, disruption of the functioning of the information systems, ;"

[98] For example at Article 15 of the Council of Europe Convention on Cybercrime, referencing others such as the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international instruments.

7.3.1 Confidentiality of subscriber identity and secrecy of communication

The questionnaire requested information from the participant countries regarding whether there is an obligation on ISPs to protect the secrecy of the communication of subscribers and if so, where that obligation is reflected in the law. Similarly, the questionnaire also requested information from the participant countries regarding the obligation on ISPs to protect their subscriber's identity.

The responses are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Protect Secrecy of Communication	Yes[99]	No information provided	Yes[100]	Yes[101]	Yes[102]	Yes[103]
Protect Subscriber Identity	Yes[104]	No information provided	Yes[105]	Yes[106]	Yes[107]	Yes[108]

Information was also requested on which agency is responsible for overseeing the ISPs obligation to protect the secrecy of communication and what enforcement measures are available to sanction ISPs for non-conformance.

The responses are summarised in the following table:

[99] Article 49 (Privacy of Customer Information) states that every operator and service provider shall regard and treat as confidential all information regarding the type, location, use, destination, quantity and technical configuration of services used by their customers.

[100] Article 42 (Rights and Duties of the Telecommunications Operation) of the Law of the Republic of Belarus No. 45-3 of 19 July 2005 "On Telecommunications", Presidential Decree No. 450 of 1 September 2010 on Licensing of Certain Activities (in regard to licensing of activities on technical protection of information, including use of cryptographic methods and use of electronic digital signature), Presidential Decree No. 196 of 16 April 2013 on Some Measures How to Improve Information Protection.

[101] Law of Georgia "ON Protection of Personal Data", Law of Georgia "On Electronic Communications", Article 8(1) states "Information on consumers of electronic communications networks, as well as information transmitted by the consumer through these networks, is secret and its protection is guaranteed by the legislation of Georgia"

[102] Law no. 20-XVI dated 03.02.2009 on preventing and fighting cybercrime. Article 6.

[103] Article 7, 10 of the Law of Ukraine "On Access to Public Information", Law of Ukraine "On Information".

[104] Law on Electronic Communications, Article 49 (Privacy of the Customer Information)

[105] Articles 17, 18 of the Law of the Republic of Belarus of November 10, 2008 "ON Information, Informatisation and Information Protection", Article 54 of the Law of the Republic of Belarus No. 45-3 of 19 July 2005 "On Telecommunications", Paragraph 149(1) of Regulations on licensing certain types of activities, approved by the Decree of the President of the Republic of Belarus of September 1, 2010 No. 450 "On licensing of certain types of activities", The Decree of the President of the Republic of Belarus of April 16, 2013, No. 196 "On some measures to improve the protection of information"

[106] Law of Georgia "On Electronic Communications", Resolution No. 3 "on provision of services and protection of consumer's rights in electronic communications", The Law of Georgia "On Protection of Personal Data".

[107] Law on the protection of personal data, No. 133 dated 08.07.2011.

[108] Law of Ukraine "On the Protection of Personal Data" (http://zakon2.rada.gov.ua/laws/show/2297-17).

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Authority Responsible for Oversight	Regulator, Law Enforcement, Data Protection [109]	No information provided	Inspectorate for Telecommunications, Operative and Analytical Centre[110]	Data Protection Authority, National Commission on Communications[111]	Communications Regulator [112]	Not Defined[113]
Enforcement Measures	Administrative Sanctions [114]	No information provided	Administrative Sanctions[115]	Administrative Sanctions[116]	Civil Sanctions [117]	Administrative and Criminal Sanctions [118]

7.3.2 Legal Interception

The legal basis and practical aspects of legal interception were discussed earlier in this report. This section examines the safeguards that are in place to protect customer confidentiality. As mentioned in Section 4.3.3, and as further reported above, obligations on

[109] The duty is enforced by the PSRC in cooperation with the law enforcement and personal data protection agencies.

[110] According to Paragraph 18 and 37 of the List of Supervisory Bodies and their Control (Supervisory) Activity, approved by the Decree of the President of the Republic of Belarus of October 16 2009 No. 510 "On Improving Control (Supervisory) Activity in the Republic of Belarus", state supervision of telecommunications, including supervision over the fulfillment of licensing legislation, requirements and conditions, is to be carried out by The State Inspectorate of the Republic of Belarus for Telecommunications of the Ministry of Communications and Informatisation. If users are state organizations the user databases that ISPs develop are cryptographically protected and licensed by the Operative and Analytical Centre of Belarus. Data Integrity is controlled by the Analytical Centre as well.

[111] Inspector for the protection of personal data (an official responsible for overseeing the implementation of legislation governing data protection) and the Commission (the National Commission for Telecommunications Regulation).

[112] The questionnaire provides a link to the website of the National Regulatory Agency for Electronic Communications and Information Technology of the Republic of Moldova. (http://en.anrceti.md/fileupload/1)

[113] The body that is responsible for monitoring compliance with the ISPs obligation to protect the confidentiality of personal data and other user information is not defined by law.

[114] The PSRC may impose fines and penalties if it determines after an administrative notice and a public hearing that a licensee has failed to comply with the relevant provisions of the RA Law on Electronic Communication on confidentiality of subscriber identity and communication. In certain cases, the PSRC may change, suspend, or request for judicial termination of a license or an authorization for violation of provisions of the law.

[115] From delivery of an order, demand, fines up to suspension and withdrawal of license.

[116] Written warnings, followed by fines, followed by suspension or cancellation of authorization to operate.

[117] A reference is made to the Civil Code of the Republic of Moldova, No. 1107-XV dated 06.06.2002.

[118] Administrative liability (penalties) are defined in parts 4, 5 of Article 188-39 (violation of legislation in the field of personal data protection) of the Code of Ukraine on Administrative Offenses. Criminal liability – Article 182 (violation of privacy) of the Criminal Code of Ukraine.

ISPs to provide the ability to law enforcement agencies are frequently found in telecommunications legislation, or in individual licenses issued by public authorities. The right to communications privacy is often also subject of national legislation and is usually safeguarded in countries by both local telecommunications legislation, the constitution and case law. In certain cases there are also specific requirements in telecommunications licensing regimes.

The questionnaire requested information from the participant countries about what type of order is required to compel an ISP to facilitate legal interception of a subscriber's communication. The results are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Order Required for Interception	Court Order	No information provided	Prosecutor Order[119]	No information provided	Prosecutor Order[120]	Court Order[121]

Recommendation 9: ***Where there is not an authority responsible for oversight, countries should consider establishing, or assigning responsibility to, an agency for oversight of ISP's obligations to protect the confidentiality of their subscriber's communications.***

Recommendation 10: ***It was noted that all participant countries for which information is available have legislation in place to protect secrecy of communication and confidentiality of subscriber identity. Conflicts will inevitably arise between the requirements of law enforcement for access to data and the ISPs obligation to protect the secrecy of subscriber communication. Countries should consider assigning authority to the agencies responsible for oversight to take an active role in such cases.***

Recommendation 11: ***Countries should further consider assigning authority to the agencies responsible for oversight of ISPs to provide concrete guidance to all relevant parties on the interpretation, scope and application of proportionality measures.***

7.4 Data retention

Data retention is an important tool for law enforcement to be able to have sufficient digital evidence, especially when a crime is committed using networks. In such cases data retention provides for the retention of relevant logs and records in order to establish a trail of evidence, clarifying which user, subscriber or account was implicated in certain communications, which may, in turn, provide law enforcement authorities with important indications of the responsible parties for certain acts committed online, or through communications networks.

Data retention concerns so called traffic data, meaning information pertaining to origin and destination of communications, not being content. In practise the level of detail of such information that is recorded depends on the cooperation and parameterization of networks.

[119] Delivery of an order according to an adopted form signed by head of a competent authority and sanctioned by a competent public prosecutor. Code of Criminal Procedure of the Republic of Belarus, Articles 103, 209, 210.

[120] The prosecutor serves warrants for interception. Criminal Procedure Code No. 122-XV, dated 14.03.2003 (Article 132 – Performing and certifying interception and recording of communications).

[121] Determination of the investigating judge, made on the proposal of the investigator, the prosecutor.

For this reason it is important that definitions of such data are precisely defined, especially in relation to internet traffic, which is prone to various issues hampering the traceability of users through the network. In European countries there is a widespread practise to differentiate retention times of such data in relation to data networks as opposed to voice networks or services. This differentiation is usually motivated by both volume and costs involved, as well as privacy considerations.

The relevant data retention regimes in the EAP3 region can analysed according to the responses of the questionnaire, as follows:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Data retention obligation (basis)	Regulator (PSRC) – policy and MoU (Voluntary)	No information provided	Presidential decrees and ministerial decrees	No information provided	Law	Law
Retention period voice/phone	2 Years	No information provided	5 years	No information provided	180/90 days (traffic/decryption keys)	3 years
Retention Period data	Voluntary (MoU)	No information provided	5 years	No information provided	180/90 days	3 years
Definition of traffic data (internet)	Yes	No information provided	Not available [122]	No information provided	Yes[123]	Not available

Recommendation 12: ***Traffic data should be retained on a clear legal basis, both in relation to traditional (voice) services as well as in relation to data (internet) based services.***

[122] Only subscriber data to be retained is defined: subscriber's number, last name, first name, patronymic, address of the subscriber or the address of the installation of the terminal subscriber unit (terminal), subscriber numbers, data allowing to identify (identify) the subscriber or his terminal device (terminal), and for subscribers of the cellular mobile network Telecommunications - also the details of the identity document (its name, series, number, date of issue and name of the state body that issued the document);.

[123] According to the Council of Europe International Cooperation Wiki/Website – there is a definition: http://www.coe.int/sr_ME/web/octopus/international-cooperation-wiki/-/asset_publisher/ToV4OWWBJueW/content/moldova/pop_up?_101_INSTANCE_ToV4OWWBJueW_viewMode=print&_101_INSTANCE_ToV4OWWBJueW_languageId=sr_ME

Recommendation 13: A clear definition of traffic data to be retained in case of Internet connection data should be provided.

7.5 Regulatory Authorities

It is common for states to have a separate telecommunications authority or agency that functions at arm's length of the (more politicized) executive and administration. This allows telecommunications regulators a certain independence in assessing the needs of society and in safeguarding the various interests at stake, where the critical telecommunications infrastructure is concerned.

Regulatory authorities in the region all have different tasks, and their responsibility in relation to access to data for law enforcement, as well as their role in relation to legal interception and privacy protection is varied. In practise, the telecommunications regulators (or related agencies), have different mandates.

In the questionnaire related to this study, questions were asked about the tasks fulfilled by these authorities. In short their roles can be summarized as follows:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Seperate regulator	Yes (PSRC)	No information	No[124]	Yes (GNCC)	Yes (Ancreti)	Yes (NCCIR)
Access to data	Yes	No information	LEA & Operational Centre	No Information	Yes	No
Interception of content data	Yes (License condition)	No information	KGB& Operational Centre	No Information	Yes (Also GPO & Police)	No
Privacy and consumer rights	Yes (consumer protection)	No information	Ministry of Communications, Operational Centre	Yes	Yes	Yes
Cyber security strategy	Yes	No information	Yes	Yes	No information	No

Recommendation 14: ***An independent regulator should be considered in order to balance the needs of law enforcement, communications privacy and freedom of speech.***

[124] Licensing is done by the Operative and Analytical Center under the President, and various other tasks are performed by the Ministry of Informatization and Communications, rather than by independent bodies.

Recommendation 15: ***Notwithstanding their mandate, regulators should endeavour to co-operate with industry on a voluntary basis, preferably on the basis of clear and agreed terms (Memorandum of understanding).***

Recommendation 16: ***Roles of the regulatory agencies in relation to both privacy and access to (content) data should be clearly defined, and provide clear powers to supervise these important areas. Regulators with this mandate should be relatively independent and not related, directly, or indirectly to law enforcement bodies or the executive branches of government.***

Recommendation 17: ***Oversight on the law enforcement related obligations (access to data and interception) should not be enforced by law enforcement bodies themselves.***

Recommendation 18: ***Given the large overlaps with the area of security, the development of a clear security policy, which outlines the role of the regulator and other inspections and government stakeholders in this area, is desirable.***

7.6 Voluntary/non-regulatory cooperation

7.6.1 Agreements in Relation to Fighting Illegal Content

The term illegal content is often used to refer to illegal images of children, but depending on national legislation may also include other areas such as:

- Content related to the grooming of children
- Advertisement of child sex tourism
- Content related to child trafficking and sexual exploitation of children
- Racist of xenophobic content
- Content inciting hatred
- Financial scams
- Content related to the sale or distribution of drugs
- Content related to the sale or distribution of arms

The first aspect to consider in relation to fighting illegal content is whether there is an obligation for ISPs to either monitor or report illegal content. The absence of a legal obligation to monitor or report illegal content can present a challenge to ISP cooperation in this area due to concerns that ISPs may have about liability under other obligations (such as privacy of communication legislation) in cases where content is incorrectly identified as being illegal in the absence of a law enforcement or court order to remove content.

According to the survey responses received, the following table summarises the obligation on ISPs to (a) monitor their connectivity, hosting or caching of content for illegal content, and (b) report illegal content that they detect on their networks.

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Obligation	No	No	Yes[125]	Partial[126]	Yes[127]	Partial[128]

[125] Provided for in a number of cases in paragraph 4 of Article 22.16 of the Administrative Code of the Republic of Belarus. Also, according to paragraph 12 of Presidential Decree No. 60 of 1 February 2010 "On Measures on Improving Use of the National Segment of the Internet": "Liability for the content in the national Internet segment is borne by persons who placed the information. Liability for violation of

to Monitor		information provided				
Obligation to Report	No[129]	No information provided	Yes[130]	No[131]	Yes[132]	No

Another area to be considered is how, in practice, when a member of the public becomes aware of illegal content, that content can be reported to the appropriate agency or ISP. The same problem may arise within law enforcement agencies wherein it may be difficult for an investigating officer to determine, having received a report or otherwise identified illegal content, the appropriate ISP to communicate with. Having a single point of contact, such as a reporting hotline, that is able to report the matter to the relevant agency or ISP is one

---

the decree as well as nonfulfillment of a regulation of requirement made by a competent authority according to paragraph 11 of the Decree is borne by internet providers, hosts (authorized representatives) or points of collective access to Internet services." Paragraph 11 of the Decree states: "Upon detection of Decree violations as well as other legislative acts in the national Internet segment by crime detection authorities, public prosecution and preliminary investigation authorities, Committee of State Control, tax authorities according to their competencies, these agencies deliver and order in accordance with the established procedure for legal entities and entrepreneurs to remove detected violations within a fixed period of time."

[126] If an ISP is informed of illegal content, it must be removed.

[127] Provided for in Article 7(1)(b) of Law N. 20-XVI dated 03.02.2009 on preventing and fighting cybercrime: "(1)Service providers are required to…(b)To communicate to the competent authorities the information on computer traffic, including data on illegal access to information in the information system, attempts to introduce illegal programs, violation by responsible persons of the rules on the collection, processing, storage, dissemination, distribution of information, or the rules of protection of the information system according to the status of the information or its degree of protection, if they have contributed to the acquisition, distortion or destruction of the information or caused other serious consequences, disruption of the functioning of the information systems, other computer crimes."

[128] Article 52-1, 52-2 of the Law of Ukraine "on copyright and neighboring rights" specifies the duty of the provider of hosting services and the owner of the website to prevent and stop violations of copyright and related rights using the Internet.

[129] If a person is informed about illegal content the ISP has a right (but not an obligation) to inform the police.

[130] According to Paragraph 8 of the Decree of the President of the Republic of Belarus of December 28, 2014 No. 6 "On Urgent Measures to Counter Illicit Drug Trafficking" owners of Internet resources are required "(a) to analyze the content of their information resources and prevent the use of their information resources for the dissemination of messages and/or materials aimed at illicit drug trafficking and (b) to inform the internal affairs bodies of attempts to use their information resources to disseminate messages and/or materials aimed at illicit drug trafficking."

[131] The law of Georgia "On Electronic Communications" and Resolution No. 3 "on the provision of services and protection of consumer's rights in the field of electronic communications" does not oblige the ISP to notify the commission of detected illegal content. If such a fact is revealed, the ISP must remove the illegal content.

[132] Article 5 of Law no. 20-XVI dated 03.02.2009 on preventing and fighting cybercrime: "In the framework of cybercrime prevention and fighting activities, the competent authorities, service providers, non-governmental organizations, other civil society representatives cooperate through information exchange, experts, through joint investigation of cases and identification of offenders, training personnel, through initiatives to promote programs, practices, measures, procedures and minimum standards for the security of information systems, through cybercrime information campaigns and the risks to users of computer systems, through other activities in the field."

form of cooperation initiative that can be helpful in these cases. The problem of correctly identifying the correct ISP/hosting company is further exacerbated if the content is held outside of the jurisdiction. Involvement in international cooperation initiatives such as INHOPE can be helpful in such cases[133].

Cooperation agreements can also be helpful in cases where ISPs identify illegal content on each other's networks, so that complaints can be forwarded as appropriate. The questionnaire requested information about any agreements that are in place in relation to fighting illegal content such as child pornography, viruses, hate speech, botnets and removal of illegal content from ISP services. The results are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Cooperation Agreements	No	No information provided	Yes[134]	No information provided	No information provided	No

Finally, the questionnaire requested information on the mechanisms available to the participant countries to facilitate takedown of illegal content. The responses are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Illegal Content Takedown Requirement	Court Order	No information provided	No information provided[135]	Court Order	Court Order	Court Order
Fast	Yes[136]	No	Yes[137]	No	No	Partial

[133] http://www.inhope.org/gns/who-we-are/at-a-glance.aspx

[134] Paragraph 8 of Presidential Decree No. 60 of 1 February 2010 "On Measures on Improving Use of the National Segment of the Internet". Resolution of the Operative and Analytical Centre under the President of Belarus No. 4/11 of 29.06.2010. Presidential Decree No. 6 of 28.12.2014.

[135] The response to the questionnaire describes a mechanism by which an ISP subscriber (or state agency) can request that their own access to the Internet is restricted to preclude certain categories of illegal content but does not describe whether a request to take down illegal content will be considered by an ISP or whether a court order is required.

[136] This is possible, if the source is located in Armenia, for foreign sources there is no any regulation.

[137] In compliance with Paragraph 12 of Resolution of the Operative and Analytical Centre under the President of Belarus and Ministry of Communication and Informatisation of Belarus No. 4/11 of 29.06.2010 on Adoption of Statute Regulating the Procedure and Restricted Access of Internet Users to Information Prohibited from Distribution by Legislative Acts: "The list of restricted access is made up by Republican Unitary Enterprise 'BelGIE' (hereinafter referred to as RUE 'BelGIE') according to decisions of management of the Committee for State Control, Prosecutor General's Office, Operative and Analytical Centre, other state agencies (hereinafter referred to as authorized state agencies) on putting internet resource identifiers onto the list of restricted access. Such decisions are made by management of the authorized state agencies according to their competencies. RUE 'BelGIE' and the owner of the Internet resource that is to be restricted (if it is located in the national Internet segment) are notified according to the procedure during 3 days about the decision that has been made by the authorized state agency. The notification contains the following: Internet resource identifiers, access to which is to be restricted; reason for restriction with reference to the legislative act that prohibits data from distribution. Those

Takedown Possible	information provided	Informatio n Provided	Informatio n Provided	[138]	

Recommendation 19: ***Countries should consider development of coordination actions between ISPs, law enforcement and other competent authorities to enable simple reporting of illegal content and routing of complaints to the relevant authority or ISP.***

Recommendation 20: ***Countries should consider putting in place fast/provisional takedown measures to enable blocking of illegal content pending receipt of appropriate legal process (e.g. court order).***

7.6.2 Requirements to put in place countermeasures to prevent fraud or financial damage

In some countries ISPs have a regulatory obligation to protect their customers and themselves against fraud or financial damage. This obligation can take a variety of forms, ranging to general obligations arising as an implication of iSPs being categorised as critical national infrastructure to specific solutions to protect customers against, for example, various types of telecommunications fraud (e.g. premium number dialling). The questionnaire requested information from the participant countries on whether ISPs are required to put in place countermeasures to counteract financial damage to ISP infrastructure and financial fraud prevention. The responses are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Obligation to Prevent Fraud or Financial Damage	No obligation	No information provided	In some cases[139]	In some cases[140]	No information provided	No information provided

Recommendation 21: ***When information has been provided it is noted that there are some cases where obligations have been put in place to prevent fraud or financial damage. Countries should continue to consider the use of obligations to prevent fraud in cases where ISP action is required to protect customers against certain types of fraud or financial damage, particularly in cases where coordinated action of multiple ISPs is required to achieve the desired effect.***

---

notifications that are not made up in compliance with requirements provided for by part 3 of the current article are to be returned without completion but with specifications of reasons for return."

[138] Articles 52-1, 52-2 of the Law of Ukraine "On Copyright and Related Rights"

[139] For those ISPs that provide services to state agencies a range of normative and legal acts developed by the Operative and Analytical Centre of the Republic of Belarus are applicable, among which are (a) Presidential Decree No. 196 of 16 April 2013 on "Some Measures How to Improve Information Protection"; (b) Order of the Operative and Analytical Centre under the President No. 82 of 16 November 2010 on "Adoption of a Statute Regulating the Procedure of Endorsement of Work Performance and Provision of Services to State agencies (organizations) while Carrying out Activities on Technical Information Protection, Including Cryptographic Methods and Application of Electronic Digital Signatures".

[140] In respect to international call terminations, ISPs have particular obligations re financial fraud prevention imposed by GNCC relevant decision.

7.6.3 Information Sharing About On-going Threats or Incidents

Where an ISP finds itself the target of a particular attack, or identifies a vulnerability that exposes its operations to attack, there are advantages to sharing this information with other ISPs so that they can assess their exposure to the same type of attack. This type of information sharing can might for containment of such incidents to within a single organisation and prevent escalation into a major national cyber-security incident. National CERTs (Computer Emergency Response Teams) can have an important role to play here, but alternatives such as informal ISP fraud and security forums or bilateral communication can also be a feasible where a national CERT is not operational or the incident falls out of scope of the responsibilities of the national CERT.

It can also be helpful in such informal fraud and security forums to involve law enforcement agencies (if law enforcement agencies have a crime prevention role) in a collaborative fashion.

The questionnaire requested information about whether ISPs share information with each other about on-going threats of incidents. The questionnaire also requested information about whether there is a platform or other established way to exchange information between state agencies and ISPs regarding malware/viruses, financial frauds or the presence of illegal information. Finally, information was requests on whether ISPs making reports of various types (e.g. data breaches, security incidents or crimes) are provided with feedback on their report (e.g. status of the report, action taken or how similar reports could be improved in future). The responses are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Information Sharing	Informal [141]	No information provided	No information provided [142]	Informal[143]	No information provided	No information provided
Information sharing platform	Informal CERT[144]	No information provided	National CERT[145]	No information provided	No information provided [146]	No information provided

[141] Informally each ISP has an address for reporting (abuse@isp.am)

[142] The response to this question in the questionnaire indicates that ISPs can, like any other natural or legal person, report crimes in compliance with the criminal procedure code. However, no information was provided in response to the question about whether ISPs share information with each other about ongoing threats or incidents.

[143] In particular cases information is shared through unofficial communication. At the moment there is no uniform mechanism for exchange of data related to incidents between ISPs.

[144] Informally there is a non-governmental CERT, which provides actual information about incidents.

[145] Public authorities and ISPs are given the opportunity to use an automated system for exchanging information about computer incidents. The National Computer Emergency Response Team of the Republic of Belarus has a website where an individual or legal entity can make a report.

[146] In response to this question in the questionnaire a list of reporting points was provided, which does not provide any information about whether there is an information sharing platform available.

Feedback provided	No	No information provided	Yes[147]	No information provided	No information provided [148]	No information provided

Recommendation 22: ***There are significant advantages to information sharing between ISPs to prevent threats and incidents spreading from one ISP to others. It is therefore recommended that countries consider adopting an appropriate mechanism to share information between ISPs about on-going threats or incidents. In some countries there may be obligations to report such incidents to national CERTs but even in cases where there is no obligation to report there are advantages to informal information sharing of this type.***

Recommendation 23: ***It is reasonable to expect that agencies receiving incident reports from ISPs are likely to be receiving these reports over an extended period of time. Providing feedback to reporting entities on their reports can help those entities to provide better reports in future. It is therefore recommended that countries consider adopting a practice of providing feedback to reporting entities with whom on-going relationships are expected so that those entities can provide better reports in future if necessary.***

Recommendation 24: ***Technological platforms are available to assist with confidential or anonymized information sharing about on-going incidents or threats. Countries should consider the use of such a platform by, for example, their national CERT if such exists and is operational.***

7.6.4 Involvement in Awareness Training Programmes

Information awareness programmes are an important way for ISPs and state agencies to share information about their perspectives on the matter of law enforcement access to information. ISPs can provide information to state agencies on, for example, what information they have, how to request it, common problems experienced with requests received and so on. State agencies can provide information to ISPs on changes to regulatory regimes, requirements for information retention and so on.

The format of the awareness initiatives can be wide-ranging, from ISP involvement in police or judicial training events to law enforcement involvement in private security conferences.
The questionnaire requested information about whether either (a) ISPs provide awareness information to state agencies or (b) state agencies provide awareness information to ISPs. The responses are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine

[147] In compliance with Law of the Republic of Belarus No. 300-3 of 18 July 2011 on "Applications of Citizens and Legal Entities" if the full range of requirements applied to the application is fulfilled, the ISP will receive a well-grounded response within a legally set period of time. In case of requests from competent authorities to provide information, ISPs only provide the requested information without receiving any subsequent response from the competent authority.

[148] In response to this question in the questionnaire a list of reporting points was provided, which does not provide any information about whether feedback is provided.

Involvement in Awareness Training Programmes	No such practice	No information provided	Yes[149]	No information provided	Yes[150]	No information provided

Recommendation 25: ***ISPs and competent authorities have important information to share with each other regarding their perspectives on the matter of law enforcement access to data held by ISPs. Countries should consider ISP and competent authorities working to raise each other's awareness of the other's perspective in an appropriate forum.***

[149] Participation in joint conferences, including IT Security Conference that is positioned as a negotiations platform for private companies, state companies and the law enforcement agencies on discussion of issues of cybercrime.

[150] The National Institute of Justice, the Police Academy.