Cybercrime@EAP III & CyberEast

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

1 September 2017
Updated 1 September 2022

Liabilities of Internet Service Providers in the Eastern Partnership Region (2022 update)

Prepared by Council of Europe experts
under the Cybercrime@EAP III Project
and the CyberEast 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)
E-mail cybercrime@coe.int

Disclaimer

This review has been prepared in 2017 by independent Council of Europe experts Hein Dries and Dave O'Reilly with the support of the Cybercrime Programme Office of the Council of Europe. It was updated in 2022 by independent Council of Europe experts Markko Kunnapu and Roeland van Zeijst within the CyberEast Project framework.

This document has been produced as part of projects 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. No liability is assumed for findings in this report.

Contents

Acronyms

2AP	Second Additional Protocol to the Convention on Cybercrime
AMK	Antimonopoly Committee of Ukraine
ANRCETI	National Regulatory Agency for Electronic Communications and Information Technology of the Republic of Moldova
CERT	Computer Emergency Response Team
CMS	Communications Monitoring System (Belarus)
CoE	Council of Europe
ComCom	Georgian National Communication Commission (also: GNCC)
CSAE	Child Sexual Abuse and Exploitation
CSAM	Child Sexual Abuse Material
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service (attack)
DDT	Ministry of Digital Development and Transport of the Republic of Azerbaijan
DNA	Deoxyribonucleic Acid
DPA	Data Protection Authority
EEA	European Economic Area
EAP	Eastern Partnership
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms
ECJ	European Court of Justice (supreme court of the EU in matters of EU law)
ECtHR	European Court of Human Rights (CoE court interpreting the ECHR)
ERDR	Uniform Register of Pre-Judicial Investigations of Ukraine
EU	European Union
FIRST	Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation (EU)
GNCC	Georgian National Communication Commission (also: ComCom)
GPO	General Prosecutor's Office
ICT	Information and Communications Technology
ICTA	ICT Agency of the Republic of Azerbaijan
IDDA	Innovation and Digital Development Agency of the Republic of Azerbaijan
IP	Internet Protocol
ISAC	Information Sharing and Analysis Centre
ISP	Internet Service Provider
KGB	State Security Committee of the Republic of Belarus
LEA	Law Enforcement Authority/Authorities
MLAT	Mutual Legal Assistance Treaty (also used for a request pursuant to it)
MOU	Memorandum of Understanding
NCCIR	National Commission for the State Regulation of Communications and Informatization of Ukraine
NCPDP	National Center for Personal Data Protection of the Republic of Moldova
NIS	Network and Information Systems (EU's NIS Directive applies to their security)
NSDC	National Security and Defence Council of Ukraine
OAC	Operations and Analysis Center under the President of the Republic of Belarus
OTA	Operational-Technical Agency of the Republic of Georgia
PSRC	Public Services Regulatory Commission of the Republic of Armenia
SIS	Security and Intelligence Service of the Republic of Moldova
SMS	Text message (from Short Message Service)
SNS	National Security Service of the Republic of Armenia
SORM	System for Operative Investigative Activities
SSU	Security Service of Ukraine
T-CY	Cybercrime Convention Committee
URL	Uniform Resource Locator (website address)

1 Introduction

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

During the recent years, cybercrime and other criminal offences generating electronic evidence have increased. As shown in the recent CyberEast *Cyber Barometers*,[1] [2] [3] [4] [5] the COVID-19 pandemic has exacerbated offences committed online. This has put more pressure on law enforcement authorities worldwide to access and obtain computer data for criminal investigation purposes, including by invoking the Budapest Convention on Cybercrime, the importance of which was underlined by the release of its Second Additional Protocol in 2022.

Meanwhile, the perceived importance of privacy, personal data protection and the safeguarding of fundamental rights has also changed. Partly due to the global ripple-effects of the EU's General Data Protection Regulation (GDPR) awareness is growing among individuals and within the private sector, while countries are increasingly introducing new legislation on these topics.

When it comes to accessing evidence for the purpose of criminal investigations, private sector entities – including Internet Service Providers (ISPs) – are expected to cooperate with 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. For example, ISPs are also under *other* legal obligations to protect the privacy of their users. Some sector-specific obligations, for example, require service providers to provide a certain level of consistent service. Such obligations may sometimes be at odds with cooperating with law enforcement in the framework of criminal investigations. Electronic communications regulators in the EAP region, while often being designated as key players locally, are not always actively able to resolve 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 it. Non-cooperative business entities, for whatever motive, will relatively easily find ways *not* to cooperate in practice, or to delay the process so 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 and regulations. In this light, there can be genuine business interests and common goals, enabling private entities to share with law enforcement and cooperate with state authorities on a voluntary basis as a matter of good business practice. While legislation has been and will be the basis for cooperation, there is also additional room for practical measures, cooperation agreements and MOUs that allow closer collaboration and coordination among public and private sector entities.

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

[1] *Cybercrime and Cybersecurity Barometer in Armenia*, CyberEast/CyberSecurity East, 2022.
[2] *Cybercrime and Cybersecurity Barometer in Azerbaijan*, CyberEast/CyberSecurity East, 2022.
[3] *Cybercrime and Cybersecurity Barometer in Georgia*, CyberEast/CyberSecurity East, 2022.
[4] *Cybercrime and Cybersecurity Barometer in Moldova*, CyberEast/CyberSecurity East, 2022.
[5] *Cybercrime and Cybersecurity Barometer in Ukraine*, CyberEast/CyberSecurity East, 2022.

2 Purpose and design of the study

The current document provides an update to a similar study from 2017.[6] As important changes have taken place in terms of policy and legislative frameworks, while the nature and scale of cybercrime have professionalized and increased, it was found necessary to provide updates on these developments at both the international and EAP countries' level, as observed mid-2022.

Initially having been carried out under Result/Immediate Outcome 1 of the project Cybercrime@EAP III (*Analysis of current initiatives, challenges and opportunities regarding public/private cooperation in the Eastern Partnership region*), this updated report offers further insight into current challenges and future opportunities for effective cooperation between law enforcement in the EAP states and the Internet Service Providers, thereby contributing directly to Output 3.4 of the CyberEast Project *(Implementation of existing agreements on public/private cooperation and the conclusion of such agreements in the remaining countries).*

During the preceding study, desk research was conducted into the legislative and regulatory backgrounds of the participant countries. This was then followed by the circulation of a questionnaire, obtaining clarifications and further information about legislative basis and practical matters. Those responses were then processed and assembled into the 2017 report.

The current study incorporates updates to the findings and contents of that report, having been expanded in order to cover relevant five-year developments, by combining further desk research with processing of the *Cybercrime and Cybersecurity Barometers* for the EAP region, as well as several other pertinent CoE studies.[7] [8] [9]

[6] *Liabilities of Internet Service Providers in the Eastern Partnership Region*, Cybercrime@EAP III, 2017. https://rm.coe.int/study-on-liabilities-of-internet-service-providers-in-the-eastern-part/16808f1e1a

[7] *Cooperation between law enforcement and internet service providers against cybercrime: towards common guidelines*, CoE, 2020.

[8] *Data retention in the States Parties to the Budapest Convention on Cybercrime*, CoE, 2020.

[9] *Regional Study on Personal Data Protection aspects of law enforcement action on cybercrime in the Eastern Partnership region*, CoE, 2020.

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. Where practical shortcomings are identified, it may be advantageous for countries to consider also less formal cooperation methodologies to address these. For example, if there are difficulties identifying which ISP to request data from and what data is available, 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: Countries may have rules in place concerning the cost of requests and how costs to the ISPs would be reimbursed or compensated. If such a compensation or reimbursement mechanism is available, then 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 lawful 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. **See Recommendation 14.**

Recommendation 4: Although in general ISPs are not monitoring the content and are not liable for it, rules for ISP obligations and related 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 and procedures for ISPs for blocking and takedown should be clearly defined and should therefore be based on a clear legal basis for all types of illegal content to be considered.

Recommendation 6: Such obligations should be differentiated 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, as monitoring should be specific in relation to the goals and legal basis where they are imposed nonetheless. However, this doesn't preclude possible obligations related to prevention and detection, including through automatic means, of illegal content.

Recommendation 8: Independent oversight or judicial control should be provided for, in order to safeguard freedom of speech and freedom of expression, 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, a court or an independent agency for oversight of ISPs' obligations to protect the confidentiality of their subscribers' communications.

Recommendation 10: It was noted that all EAP countries have legislation in place to protect secrecy of communication and confidentiality of subscriber identity. Conflicts may arise between the lawful requirements of law enforcement for access to data and ISPs' obligations

to protect personal data, as well as the privacy 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: In case a country has introduced a data retention scheme for metadata, traffic and location data should be retained on a clear legal basis, both in relation to traditional (voice) services as well as in relation to internet data 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 assess the obligations related to data retention and to balance the needs of law enforcement, communications privacy and freedom of speech and expression. **See Recommendation 3.**

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 LEA bodies. Where they are part of the executive branch of government, full focus should be placed on their true independence within the rule of law.

Recommendation 17: Oversight of the law enforcement-related obligations (access to data and interception) should not be enforced by law enforcement bodies themselves. Both ex ante and ex post oversight should be conducted by a court or other independent authority.

Recommendation 18: Given the large overlaps with the area of security, the development of a clear security policy and legislative acts, which outline inter alia 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 and encourage 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 removal of, or blocking access to, illegal content, pending receipt of appropriate legal process (i.e., court order). In case of takedown or removal of illegal content, a copy should be kept for possible administrative, civil or criminal proceeding purposes.

Recommendation 21: 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 appropriate mechanisms to share information between ISPs

about ongoing threats or incidents. In some countries, in parallel with the EU's NIS Directive, there may be obligations to report such incidents to national CERTs/CSIRTs, but even in cases where there is no obligation 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 ISPs on their reports can help them to provide better reports in future. It is therefore recommended that countries consider adopting a practice of providing feedback to reporting entities with whom ongoing 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 ongoing cyber incidents or threats. Countries should consider the use of such a platform by, for example, their national CERT/CSIRT if 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 ISPs and competent authorities working together 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 relevant international law that serves a purpose in safeguarding freedom of speech and the right to private life of individuals in relation to the rights and obligations that exist for Internet Service Providers vis-à-vis their subscribers as well as public authorities. 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) law enforcement, including when it comes to fighting cybercrime, whilst protecting the rights of all citizens against any type of abuse.

A balanced implementation of these various rights and obligations is often conducive to a fair and open debate in relation to public-private cooperation, especially if all relevant interests are weighed. This requires a thorough analysis of those interests involved, and was, hence, the goal of a questionnaire that was sent to EAP project countries. This section focuses on sources of (international and European) law that exist in order to facilitate an analysis of the answers received, with minor updates as distilled from the 2022 Barometers as well as related debates.

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's e-Commerce Directive[10] and the associated liability regime for Internet Service Providers. In order for them to offer internet services, the European Union (EU) in 2000 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 the 2000 directive.

In December 2020, the European Commission presented a proposal for a new regulation[11] (Digital Services Act) that would replace several provisions of the directive. As of mid-2022, the negotiations for the new regulation were not yet finalized in the European Union, therefore the e-Commerce Directive still remains as a valid legislative standard and point of reference.

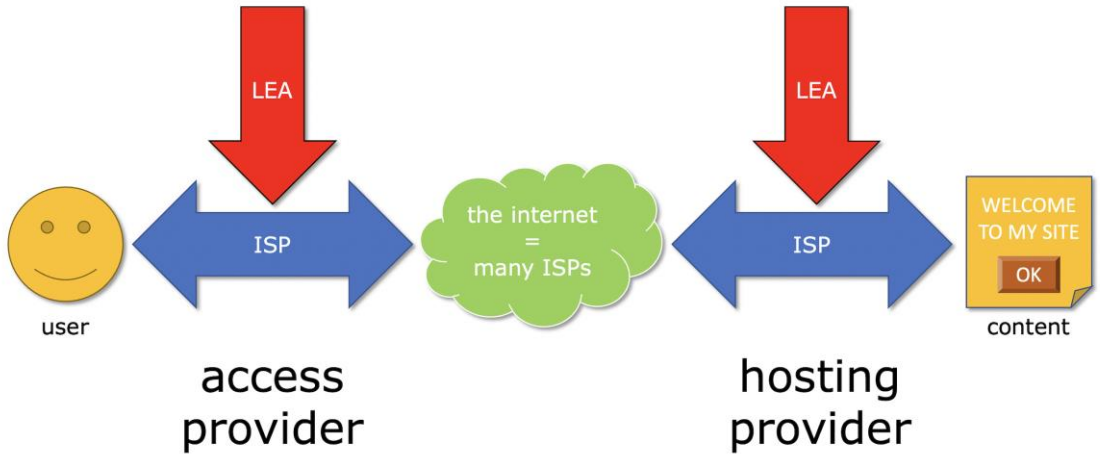
The technical and business role that an intermediary entity plays in providing internet communications services is critical in the way they are legally treated. For the purposes of the e-Commerce Directive, European law distinguishes between three distinct roles:

- 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:

[10] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031

[11] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN



Note that, in practice, large internet providers are responsible for carrying traffic across the globe ('the internet'). 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 nor user details. Except for very specific circumstances, the use of LEA powers against intermediary caching services is also virtually unheard of and does not play a large role in practice.

Mere conduit (art. 12)

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 the data they transport, as long as they strictly keep to their role as a conduit. A party that *exclusively* transports internet traffic and does not select nor 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 an authority, in specific circumstances, can dictate that certain content should be blocked or made inaccessible, this decision is applicable to all providers, including mere conduit providers.

Caching providers (art. 13) and hosting providers (art. 14)

With ***caching and hosting providers***, a new legal issue is introduced, which is the level of knowledge the provider has concerning the illegality of specified content. This, in turn, is a further factor in determining whether liability protections can be invoked. In such 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, this protection from liability fails if the service provider does not act expeditiously to remove disputed content, once they have obtained actual acknowledge of its existence and proof that it is located on their services.

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 case, have the necessary information to decide whether that specified content is indeed likely to be illegal in the specific situation. For example, following an allegation of a copyright breach, 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 put intermediaries in a position to judge such disputes. In similar cases, it is intended to provide 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 also has actual knowledge of its illegality.

Exclusion of liability by this directive is *horizontal*: it concerns any type of liability for any content traversing 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.

One of the most important aspects of this regime is that it safeguards ***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 to the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), a lack of such a regime may imply a contravention of article 10(1) of the Convention, which has been ratified by all Members of the Council of Europe, including all EU member states. In relation to the Budapest Convention on Cybercrime: its article 15 implies that due attention be 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 Limited liability only for limited roles

Service providers can benefit from the exemptions of being a 'mere conduit' and of 'caching' when they are not involved in 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 need to take place in the course of a transmission – and that they do not alter the content nor the integrity of data contained in the transmission.

For example: a service provider which deliberately collaborates with one of its users to undertake illegal acts, clearly goes beyond the limited activities of 'mere conduit' and 'caching' so, as a result, it cannot benefit from the liability exemptions established for these activities.

The limitations of the liability of intermediary service providers established in the e-Commerce Directive do not affect the possibility of injunctions of different kinds. Such injunctions can in particular consist of an order of a court or an administrative authority to terminate or prevent any infringement, including the removal of illegal information or disabling public access to it.

4.2.3 No obligation to monitor

Recital 47 of the e-Commerce Directive 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 made to monitor any and all content that traverses their services. It is certainly conceivable that when, in the course of their work, they become aware of an illegal act, they can be asked to report it. However, article 15 ensures that no general obligation to monitor can be mandated by member states. It also prevents 'outsourcing' of surveillance activities, for example by making them part of a licensing regime.

4.2.4 Regulating ISP liability

This study assesses whether a balanced regime is in place, safeguarding freedom of speech online, in the Eastern Partnership countries, based on data collected through questionnaires, desk research and the 2022 Cyber Barometers. It will assess whether the main elements of the European regime – used, here, as an example of a well-balanced regime – are in place.

4.3 Duty to protect subscriber's identity

At the international level, the right to privacy has 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). Fundamental European treaties, such as the ECHR in article 8, similarly recognize the right to privacy (including correspondence) in many guises. In the Eastern Partnership region, only the Republic of Belarus is not a signatory to this Convention.

4.3.1 Proportionality and subsidiarity; private life and legality

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) which 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) and ***subsidiarity*** (they must be the lowest level of infringement, necessary in a democratic society). Overall, these infringements should therefore be based on a clear and balanced legal regime. Article 8 of the ECHR summarizes 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 privacy of communications – covering security and privacy of mail, telephone, e-mail and other forms of communication – as well as informational privacy, including online information.[12]

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

4.3.2 ECtHR case law on interception; reasonable suspicion

In 21st-century case law the Court has identified the risk that new technologies pose in the hands of state actors: if interception of electronic communications, electronic storage of DNA-based information 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 has recognized the need for criminal justice and the protection of the rights of others. Therefore, it has 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 described in the previous section. Furthermore, the Court has specifically, repeatedly recognized a positive obligation which members states have to provide effective prosecution.[13]

[12] Cf. ECtHR Copland v. the United Kingdom, № 62617/00, 2007.

[13] Cf. ECtHR Szabó and Vissy v. Hungary, № 37138/14, 2016 and ECtHR Van der Velden vs. the Netherlands, № 29514/05, 2006.

In practice, this means that recourse against arbitrary use of state powers should be given to subjects of surveillance as well as to 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 mandated that state authorities provide transparency to an NGO as to the number of times they use their surveillance power.[14]

In another case, the Court condemned a practice whereby state authorities could execute surveillance on mobile networks without prior order and without transparency to the network operator, due to the pre-installation of equipment and the authorization order being issued retroactively. The mere (pre-)installation of such equipment, however, was deemed legal.[15]

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.

After the so-called Snowden revelations[16] as well as the confirmed 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 European Union have issued positions on this matter, outlining, amongst others, the need for independent oversight of any measures that amount to interception or surveillance of electronic communications.[17]

During recent years, there has been an increasing trend to use national security powers to prevent, detect and deter serious crime, including crimes posing a threat to national security.

Often, authorities can have tasks related to both national security and criminal justice, leading them to operate on the basis of divergent legislative frameworks. Therefore, in order to assess and understand the spectrum of rights and obligations, conditions and safeguards related to national security need to be taken account, as they also affect tasks and obligations of ISPs.

There have also been several judgments of the EctHR that are of relevance while assessing the domestic legislation and obligations provided for ISPs. National security, mass surveillance and bulk collection of data were addressed in two recent EctHR judgments.[18] [19]

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 the use of police powers 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 next paragraph) are frequently found in telecommunications legislation, or in individual licenses issued by public authorities.

---

[14] Cf. ECtHR Youth Initiative for Human Rights v. Serbia, № 48315/06, 2013.

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

[16] See, for example: Lawfare – Snowden Relevations. https://www.lawfareblog.com/snowden-revelations

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

[18] Cf. ECtHR Big Brother Watch and others v. the United Kingdom, nos. 58170/13, 62322/14 and 24960/15, 2021.

[19] Cf. ECtHR Centrum för rättvisa v. Sweden, № 35252/08, 2021.

The right to communications privacy is often a subject of national legislation and is usually safeguarded in countries through local telecommunications legislation, case law and even the constitution, although the latter does not necessarily provide direct guarantees. In certain cases, specific applicable requirements exist in telecommunications licensing regimes.

This document describes how this important right is safeguarded by balancing law enforcement orders and other interferences with the need for proportionality, subsidiarity 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 powers related to online digital evidence, often (but not necessarily) related to cybercrimes in progress. These conditions and safeguards apply to all infringements on human rights, including the right to a private life and to 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 section 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; traffic data and subscriber information

The Budapest Convention on Cybercrime has several rules that mandate its signatories to implement access to data, available in online communications infrastructure, that is crucial to investigating crimes, often those of a cybercrime nature. This data may involve several types:

- ***Subscriber information*** as registered by a service provider, e.g.:
  - Customer's full name;
  - Address;
  - Date of birth;
  - Payment identifiers used (bank account number, credit card number, etc.).

- ***Traffic data***, practical examples of which include:
  - A listing of called parties by telephone;

- IP address allocated to a subscriber;
- Website URLs requested;
- Connections set up between sets of IP addresses and port numbers.

- ***Content data*** such as:
  - Audible phone conversations;
  - Text and multimedia messages content (e.g., a displayed SMS message);
  - The content of an e-mail;
  - Humanly readable information exchanged through 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 may lead to lack of clarity. The Budapest Convention on Cybercrime only distinguishes between traffic data and subscriber information and, for these, uses a functional description in Article 1 sub d (for traffic data) and one more detailed one in Article 18 paragraph 3 (for 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.*

Article 18 – Production Order

(..)

5. *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.*

Although the Budapest Convention itself does not define 'content data', the meaning has been explained in Point 209 of the accompanying Explanatory Report:

*209. "**Content data**" is not defined in the Convention but refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data).*

This raises the question of how this definition is implemented in the Eastern Partnership region, which is further explored in this document.

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 investigating crimes which may be linked to electronic evidence, including cybercrimes:

- The expedited preservation of stored computer data (art. 16);
- 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).

These powers will be elaborated on further below in 4.4.3.

Implementation of all the listed powers is subject to Article 15, as described in 4.3, and hence requires careful consideration of the impact of the use of these powers in each individual case. With some possible exceptions – especially regarding interception of content data – all powers listed should be applicable (after a proportionality test) at least in those cases where any of the offences described in the convention are concerned.

Article 14 references a list of defined illegal activities to be classified as offences under the treaty (Articles 2 through 10), namely criminal activities relating to computer systems, data itself, activities performed by (mis)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 (DDoS);
e. Misuse of devices;
f. Computer-related forgery;
g. Computer-related fraud;
h. Child pornography (CSAM);
i. Commercial-scale copyright infringement;

additionally, pursuant to Article 14, the data-related powers may *also* be used in cases of:

j. other criminal offences committed by means of a computer system;

or simply for:

k. the collection of evidence in electronic form of a criminal offence.

Some of the offences listed above might be committed by a corporate body and the convention therefore also requires corporate liability for cybercrime offences to be included in legislation.

Although the procedural powers at domestic level are all provided by the Budapest Convention, certain aspects related to the 2022 Second Additional Protocol[20] (2AP) need to be taken into account as well. In addition to measures regulated by the Convention, the Second Additional Protocol provides for the following cross-border measures:

- Request for domain name registration information (2AP art. 6);
- Disclosure of subscriber information (2AP art. 7);
- Giving effect to orders from another Party for expedited production of subscriber information and traffic data (2AP art. 8).

Although the measures referred above are not domestic procedural measures, but instead offer additional possibilities for international cooperation (the Parties are states) and direct

[20] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. https://rm.coe.int/1680a49dab

cooperation between law enforcement authorities and ISPs, they (will) also have implications for domestic legislation, such as on electronic communications or telecommunications.
In order to implement the provisions of the protocol, signatories need to take legislative and other measures enabling ISPs located in their territory to receive and to respond to lawful requests sent from another party to the protocol. Through such new legislation, ISPs will obtain additional tasks and obligations related to these novel cross-border cooperation measures.

4.4.3 Powers for accessing data

The following outline explores the powers listed in 4.4.2 as defined in the Budapest Convention on Cybercrime, further providing context to the information collected in this study. Kindly note that the Convention is an international treaty, to which the so-called parties are countries.

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 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.

Most activities making up a cybercrime take place, either intentionally or unintentionally, outside the national jurisdiction, as they use services provided by ISPs established in different countries. Illegal activities that depend on these services can be identified using data stored on the servers and networks of these providers, but even though it is stored at some point, this data still tends to be volatile. Subscriber information, traffic data and even content data is rarely stored for long periods of time. Even if it is, it often gets deleted or overwritten rapidly.

When a criminal investigation is undertaken, it can be several months, or sometimes even years, before the relevant data can be formally requested. This would be especially the case when an international instrument such as an MLAT (Mutual Legal Assistance Treaty) were used. Due to this delay, the requested data is often no longer available or destroyed.

The expedited preservation of stored computer data is a method whereby authorities can order the preservation of relevant computer records in their jurisdiction. This preservation power can be used for local and national investigations and will also be invoked when law enforcement abroad invokes the Budapest Convention to request the support of a national authority to preserve relevant computer records in their jurisdiction. Such records are not released to the requesting authority abroad until appropriate legal instruments have been duly processed.

This elegant mechanism enables the protection of relevant data, pending appropriate relevant follow-up that actually authorizes the release of the records, thus striking a reasonable balance with human rights. Important electronic evidence and data pertinent to the case are protected and remain available until a certified and justified disclosure request is received and processed.

Expedited preservation and partial disclosure of traffic data – Article 17:

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.

As discussed in the preceding paragraphs, expedited preservation is meant 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. In

some cases, the acquired evidence will show that a connection was only routed through the service provider and that further evidence might be obtained from other providers in the chain of communications, which then typically would be contacted next by law enforcement.

The delay involved provides an obvious obstacle when the data is only released to law enforcement after such intermediary connections might no longer exist. This problem is further exacerbated when different jurisdictions would be involved.

Partial disclosure refers to the activity whereby the first foreign jurisdiction discloses 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 as required.

For example, an internet user in Ukraine might have fallen victim to a cyber-fraud incident and the e-mails used in the scam originate from an e-mail provider in the Netherlands. What if the e-mail provider was actually being accessed through an access provider based in Spain?

In this case, a request for Expedited Preservation and Partial Disclosure of Traffic Data from Ukraine to the Netherlands, to get the suspect's traffic data and subscriber data, would cause the contact point in the Netherlands to inform the requesting party that the network connection into the Netherlands was actually coming from Spain. The responding officer in the Netherlands would therefore provide the relevant IP address information to their counterpart in Ukraine, for them to send a subsequent preservation request to the Spanish 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 provider's control.

A production order instructs the recipient of it to disclose data which they are known to have in their control. Both 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 allow – within their territory – 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 on 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 of measures to protect the data in it, can be ordered to comply by the parties' competent authorities. (Note that this, again, is subject to human rights conditions, in particular when it relates to crime suspects.)

Search-and-seizure describes the 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, as well as 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 traffic data or to assist/co-operate with the authorities in collecting and recording traffic data.
3.	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, or ordered by, authorised national authorities on the network of a service provider. It is common practice that the service provider is forbidden from alerting any related clients to such requests, so that a covert investigation is not prejudiced.

Requests under article 20 include the real-time interception traffic data only and do not include the content of the communications. It is, therefore, important to clearly and unambiguously specify what is considered traffic data and what is considered 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 content data or to assist/co-operate with the authorities in collecting and recording content data.
3. 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, or ordered by, authorised national authorities on the network of a service provider. Again, it is quite common that such requests are forcibly kept confidential so that a covert investigation is not prejudiced.
As this type of request pertains to the content of the communications itself, it must have a much higher barrier since this directly impacts on the human rights of any participants to those communications. The use of this power should therefore only be possible in cases where this is deemed absolutely necessary in a democratic society, and both the use of the power and the required safeguards should be clearly specified in legislation.

4.5 On data retention

Data retention defines the policies of persistent data and records management for meeting legal and business data archival requirements. Although the Budapest Convention on Cybercrime is silent on this issue and does not regulate data retention, the principle has been referred to by the Cybercrime Convention Committee (T-CY) as useful in the fight against cybercrime. Preservation of data and obligatory data retention cannot be considered as mutual alternatives, but they can effectively complement each other.

4.5.1 Obligatory data retention and the ECJ

There has existed 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, typically one year. This was primarily done to enable law enforcement to request access once it was needed for an investigation and to prevent potential evidence from being destroyed before it could be legally obtained and analysed. The main legislative instrument on this matter used to be the Data Retention Directive 2006/24/EU[21] that harmonized this practice throughout the European Union and was, historically, to be implemented by all EU member states.

However, as elaborated upon in section 4.3, a careful balance needs to be struck between data retention and the right to privacy. The directive's approach led to significant privacy concerns as it included the data of non-suspect citizens to be retained for longer periods of time without proper safeguards being provided through the directive text. In April 2014, the EU's European Court of Justice (ECJ, not to be confused with the EctHR) declared the directive invalid.[22]

The Court ruled that the EU directive which harmonized the data retention regimes was not proportional. It was held that the period of retention should be based on objective criteria,

[21] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0024

[22] Digital Rights Ireland v. Minister for Communications (C-293/12); Kärntner Landesregierung (C-594/12). https://curia.europa.eu/juris/document/document.jsf;jsessionid=CDC9872EDB6D78911AFB57C0B7C703E6?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=11149242

that restrictions on categories of data and data access should be included and that access should be for clearly defined purposes only. This was considered especially relevant as the directive created unspecified blanket data retention, regardless of the purposes served or the persons concerned. Since insufficient safeguards were included, the directive was struck down as ultimately incompatible with the Charter of Fundamental Rights of the European Union.

In December 2016, the Court ruled[23] that, similarly, for EU member states, national legislation requiring general and indiscriminate retention of telecommunications data was not in line with the EU's e-Privacy Directive,[24] nor with the Charter of Fundamental Rights of the EU.
Although data retention legislation has since been subject to change in several EU member states, while in some of them national legislation has been declared invalid, discussions at the EU level continue.[8] There have been additional judgments[25] by the Court, addressing different aspects related to data retention, use of retained data as well as conditions and safeguards.

As several member states have expressed, also including during the proceedings at the Court, the conditions imposed by the Court are difficult or perhaps even impossible to implement in practice. Both legal and technical problems have been raised and member states together with EU institutions have been discussing possible solutions. One of the solutions could be a whole new legislative act on data retention. Currently, discussions are taking place on whether and how data retention facilities could be addressed in the newly planned e-Privacy Regulation[26] that is to replace the previous e-Privacy Directive. During these negotiations, the topic of data retention has been addressed, including creating possibilities for the EU and its member states to adopt further legislation. However, as of mid-2022, negotiations haven't been finalised.

For this document, data retention regimes of the EAP countries have been examined, both with a view to the efficacy of implementation as well as to the verification of appropriate safeguards.

---

[23] Tele2/Watson judgment in joined cases C-203/15 (Tele2) and C-698/15 (Watson).
https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=11152172

[24] 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).
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

[25] See also the following judgments:

- C-207/16 Ministerio Fiscal (2 October 2018);
  https://curia.europa.eu/juris/document/document.jsf?docid=206332&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=11156600
- C-623/17 Privacy International (6 October 2020);
  https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=11158309
- C-511/18, C-512/18, C-520/18 La Quadrature du Net (6 October 2020 & 16 November 2020);
  https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=11157776
- C-746/18 Prokuratuur (2 March 2021);
  https://curia.europa.eu/juris/document/document.jsf?text=&docid=238381&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=11158547
- C-140/20 Commissioner of An Garda Síochána (5 April 2020).
  https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=11156600

[26] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

4.5.2 Retention of data for business purposes

Data retention is only one solution to the problem of the volatility of digital evidence. In practice, it is often the case that businesses retain data voluntarily (or possibly being compelled by other laws), and for entirely legitimate reasons.
Such data may be kept for any number of business reasons such as:

- Fraud prevention;
- Billing and tax records;
- Service delivery;
- Quality of service.

It is important to note that, where personal data is concerned, data may potentially be subjected to limitations on unbridled retention or processing of records. However, as long as data is kept for a valid reason that outweighs the interest of the data subject, or is simply held with the subject's permission, then this may well be of assistance to law enforcement.

In such cases, the production order that is mandated by Article 18 of the Budapest Convention on Cybercrime 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. This would, to a large extent, depend upon the national legislation on billing and tax matters, statutory limitation periods for civil claims, etc. It would, however, also depend on the service provider and its business policies, including corporate policies and whether there is a need for certain categories of data. For example, in case of a subscription including unlimited phone calls, text messages and mobile data, there might be no need for retention of any user-side traffic data. Similarly, location data might not be needed for business purposes. Therefore, it often depends on the individual provider whether certain categories or data are retained. Additionally, barring legal obligations, a provide can decide on its own when such data would be deleted from the system or overwritten with other data.

Therefore, when a provider is retaining data for their own business purposes, there is no clear predictability from the law enforcement authorities' side and LEA cannot be certain whether the data in question exists and is still there by the time of the preservation or production order.

4.6 Obligations to report crimes and cyber security incidents

The first Directive on the security of Network and Information Systems (NIS Directive)[27] in the EU established, for each EU member state, a duty to identify critical infrastructure and operators of essential services, and to appoint one or more authorities to supervise providers of such services in relation to their network and information security. A part of this regime is the obligation to actively report security breaches and incidents to the national competent cyber security authority. In case such a security breach involves personal data, the national Data Protection Authority (DPA) needs to be notified as well.

Next to their national NIS authorities, each member state will also need to be equipped with at least one CSIRT (or CERT) team facilitating swift operational cooperation and information sharing. A key duty for operators of critical 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.

[27] 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. https://eur-lex.europa.eu/eli/dir/2016/1148/oj

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 EU member states (which each have a duty to set up a single point of contact for such incidents) or between CSIRTs directly in order to 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 public prosecutor. This obligation usually applies to all witnesses of such crimes, and/or every person with knowledge about them, apart for those who are exempted due to the prohibition on self-incrimination, such as the suspect (Article 6 ECHR).

Such obligations may or may not apply to cybercrime. It is also important to bear in mind that, as ISPs do not have an obligation to monitor the content processed, they usually do not have information whether their services are being used for criminal purposes. However, in case they are notified about illegal activities, including about illegal content being hosted on their systems, they would normally have an obligation to report this to law enforcement authorities.

There is no international standard in relation to cybercrime reporting. Best practices include a low reporting threshold, preferably through easy online reporting, as the most meaningful way for governments to address the issue and investigate cybercrime in an intelligence-led manner.

In December 2020, the European Commission presented its proposal for the NIS 2.0 Directive[28] which would increase the requirements, oversight and number of sectors covered when compared to the 2016 version. As of mid-2022, these negotiations haven't been finalised yet.

4.7 ISP obligations in the fight against illegal content

As discussed before, ISPs have an obligation to take necessary measures if they are notified about illegal activities on their infrastructure, while also being forbidden from generally monitoring content directly.

The existing framework is based on the e-Commerce Directive[29] and is to be replaced by new instruments such as the proposed Digital Services Act[30] and Digital Markets Act.[31] These will be similar to the current system, while addressing several issues in a more detailed manner.

There have also been other initiatives addressing particular categories of content that is to be considered illegal. While there have been plenty of discussions on how to define illegal content, what should be considered illegal, etc., there is a common understanding and agreement that content related to *terrorism* or *child sexual abuse and exploitation* (CSAE) should be illegal.

[28] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

[29] Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031

[30] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

[31] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act).
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

4.7.1 Terrorist content

In April 2021, the European Union adopted a new instrument, the so-called Terrorist Content Online Regulation,[32] addressing terrorist content and providing obligations for both public and private sector in EU (and EEA) member states. For definitions of 'terrorist offences' and 'terrorist content' the Regulation refers to the EU Directive on combating terrorism[33].

The Terrorist Content Online Regulation provides member states' competent authorities with the power to issue orders to remove or disable access to terrorist content, accompanied by procedures at the national level as well as a basis for cross-border cooperation. Service providers have an obligation to fulfil removal orders and, when necessary, to preserve the data for administrative or judicial review, complaint handling or criminal investigation purposes.

As this regulation entered into force in June 2022, no studies have yet been conducted on its implementation. Pursuant to the regulation, the European Commission is to report on its implementation by June 2023, whereas by June 2024 a full evaluation would be carried out.

4.7.2 Child sexual abuse and exploitation

Similar to terrorist content, there have been discussions on how to better fight child sexual abuse and exploitation, including the online dissemination of such material. In May 2022, the European Commission published a proposal[34] on preventing and combating child sexual abuse.

This regulation is to be based on the principles and frameworks provided by both the European Electronic Communications Code[35] as well as the Digital Services Act.[30] For the purposes of defining child sexual abuse material, references are made to existing Directive 2011/93/EU.[36]

The main objective of the proposed regulation against child sexual abuse is to provide additional obligations to service providers to minimize the risk of misuse of their services, detecting and reporting, as well as removing and disabling access to such illegal content.

As of mid-2022, discussions on this new proposal have started at the EU level, but it is too early to predict when the text will be adopted. Still, the evolving text of the proposal as well as other publicly available documents can be used as guidance, enabling a preliminary assessment of possible implications for service providers, including their future obligations.

---

[32] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0784

[33] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017L0541

[34] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse.
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0209&from=EN

[35] Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20181217

[36] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093

5 Regulatory authorities

5.1 Role of regulators: EU as example

Regulatory authorities related to the telecommunications sector in the European Union oversee several legal regimes that are connected at the EU level. They supervise legislation regarding electronic communications services and, especially when they are designated as the *competent authority* under the NIS Directive,[28] hold specific responsibilities towards network security.

As such, regulators 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 the required access to relevant data for the investigation and prosecution of crimes. To oversee the 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 such regulators' tasks.

For this document, a broad analysis of the EU framework for regulation of the communications market was performed, which is presented here as a continuing best practice and reference.

5.2 Tasks of regulators

It is important to note that relevant obligations for service providers, for the purposes of this report, can be sub-divided in two main areas:

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

Within the European Union, different regimes exist that differ per member state and in which the regulatory authorities (which are sometimes spread over 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 (if any);
- Implementation, enforcement and supervision of 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 privacy/secrecy and integrity of communications.

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 categories of providers. In such cases, there is usually a central registry of providers, maintained by one or several authorities, listing the providers that are active in certain markets. Additional obligations may be laid down in special or criminal legislation, which are overseen, implemented or executed by these authorities.

The European regimes are by no means identical, and are used here by way of reference and, to some extent, as a best practice of potential implementation. The questions asked in the questionnaire, which was foundational to the following chapters, are based on these practices.

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 EU member states to implement these obligations, and provide a regime for oversight and supervision that matches the local implementation.

5.3 Common implementation modalities

For each of the following obligations, implementation modalities can be observed and evaluated: data retention/subscriber data, legal interception of content data, privacy protection and security duties.

5.3.1 Data retention/subscriber data

As discussed in paragraph 4.4.1, this obligation concerns, for example:

- Phone number related to name and address;
- IP address related to name and address;
- Payment identifiers (bank account number, credit card number, etc.);
- Further subscriber details.

Implementation of this obligation can be done in several ways – where different safeguards and technical facilities may be used or mandated. Modalities include:

1) Relevant data is uploaded by all service providers to a central database, accessible to law enforcement, operated by a regulator or government agency;
2) Data can be directly accessed in provider databases and operational systems, in which case an interface and retrieval system will usually be mandated;
3) Data may be obtained on a case-by-case basis, through more or less automated systems, requiring individual responses from the service provider.

In the first two cases, independent oversight of such systems is often provided in order to account for the risk of abuse or overreach which might exist in situations where law enforcement agencies are able to gain direct access to personal data.

5.3.2 Legal interception of content data

This obligation concerns the interception, by or on behalf of authorities, of voice or data traffic, as clarified in paragraphs 4.4.1 and 4.4.3. Different regimes may apply to either content type.

For the location of legal interception equipment, generally speaking there are three modalities:

1) Equipment is located exclusively at the provider;
2) Equipment is located at the provider, from where data is relayed to a central facility;
3) Equipment is located in a central government agency or operational centre where providers are required to deliver the relevant traffic.

Costs for these facilities may be significant and, regardless of the equipment modality, can be:

a) Split between provider and public funds;
b) Carried by the public budget;
c) Paid for exclusively by the provider.

Regimes may differentiate between small and large providers – notably regarding a) and c) – as well as between public and non-public networks. Differences may also exist in relation to capital expenses (initial investments into equipment) and operational costs (staff/legal advice).

Oversight on any obligations of providers in this area is usually placed at an independent, (non-law enforcement) agency as to prevent a conflict of interest.

5.3.3 Privacy protection

Privacy aspects concern duties to safeguard the secrecy of communications and data of network subscribers, obligations on the providers to prevent illegal interception and further requirements related to the processing of personal data, location data and traffic data.

The relevant obligations can be implemented through common standards, whereby different types of data may be subject to different legal regimes (for example, traffic data and location data are treated differently under the European telecommunications privacy regime[25] [26]).

There may exist an additional obligation to notify the designated regulator should a data breach occur, especially when personal data and/or communications traffic is inadvertently disclosed.

5.3.4 Security duties

Security-related tasks are often carried out by regulators and other bodies. In many cases, regulators are part of a community or network of several institutions involved in securing the 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 within relevant sector players;
- Working with, or even hosting, a Computer Emergency (/Security Incident) Response Team (CERT or CSIRT) that may have (amongst others) any of the following tasks:
    1) Monitoring defined internet (sub)networks or infrastructures;
    2) Responding to (cyber) security incidents;
    3) 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/CSIRT or other body to be able to assess the risks to other networks, as well as to issue warnings as to prevent such attacks or incidents from occurring elsewhere.

Note
The precise allocation of the listed tasks listed above to any of a state's institutions may vary widely. In many cases, similar tasks are shared by various bodies and, although these might be related, the tasks are performed in relative isolation from 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 report 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 (see also 4.2.1).
- In relation to access to data, requirements of service providers are imposed by a generic or individual license or by way of direct regulation (see also 5.3.2). They may include subscriber data, traffic data and/or content data (as elaborated upon in 4.4.1).
- In cases where technical measures need to be taken in order to achieve data access, a regime will exist to enforce the presence of such facilities and to ensure compliance.

As mentioned in 5.3.2, oversight on such a regime is generally provided by an agency without law enforcement status to avoid conflicts of interest in a potential dispute.
- Enforcement measures against providers should be proportional and the use of criminal law against industry players is customarily avoided (as explained in 4.2.1). Fines and injunctions are generally used as measures against grossly non-compliant businesses.

5.5 Types of agencies and cooperation required

Agencies that typically oversee, authorize or execute the tasks listed in section 5.4 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;
- Courts.

The choice of agencies usually depends on the required administrative powers, needed legal safeguards and the logical clustering of tasks. In practice, 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 (5.2) as well as the typical governmental agencies involved as listed above, various interests are at stake when it comes to regulating the domains of security, privacy and access to data for law enforcement purposes.

In practice, therefore, many questions will need to be addressed in order to achieve good cooperation. These will typically include:
- Issues related to accuracy and availability of information;
- Exchange of relevant data and intelligence;
- Agreeing on information exchange protocols and technologies.

As the area of concern for this report involves many different stakeholders, the access to data for law enforcement, as well as the security of networks, both require 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 is essential.

In order to achieve such cooperation, at least the following conditions can be seen as essential:
- Regular meetings between relevant stakeholders;
- Communications instruments, including between industry and public-sector actors;
- Collaboration instruments (MOUs 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;
- Cooperation related to ICT-related matters, platforms, hardware and software.

The next section will detail various ways to operationalize public-private cooperation – insofar as it falls outside the scope of the mandatory obligations and liabilities of the actors involved.

5.6 Voluntary and non-regulatory cooperation

Although issues such as ensuring the safety of internet users, encouraging the reporting of cyber incidents and the handling of identified illegal content can be dealt with through legislative acts, these are also often dealt with through less formal cooperation initiatives. And

even where a regulatory obligation is in place, it the obligation might have been implemented through the form of a cooperation initiative, such as a binding voluntary code of practice.

Voluntary and non-regulatory initiatives have the added advantage of typically being quicker to put in place when there is a recognised immediate-term requirement. Such initiatives and practical measures facilitate the protection of users and victims, as well as the fight against (cyber)crime and illegal content.

In addition to domestic cooperation, platforms have also been established at the international level. For instance, in 2015 the EU launched its EU Internet Forum,[37] involving governments, Europol as well as industry and technology companies, with as its main objective countering terrorist content and hate speech online. As back then, EU and member states' legislation didn't fully address all the relevant aspects, having a voluntary cooperation framework and commitment by the industry was the best quick and feasible solution to tackle these issues.

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

5.6.1 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 their 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 it.

Another concern here is how, in practice, when a member of the public becomes aware of illegal content, that content can be flagged and/or 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 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[38] can be helpful in such cases.

Other cooperation agreements can also be helpful in situations where ISPs identify illegal content on each other's networks, allowing complaints to be forwarded as appropriate.

5.6.2 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 arise as an implication of ISPs being categorised as critical infrastructure, but also as a specific way to protect customers against, for example, various types of telecommunications fraud (e.g., premium number dialling). The

[37] EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online.
https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243

[38] INHOPE: Fighting CSAM since 1999. https://www.inhope.org/EN/articles/who-we-are

implementation may require cooperation between ISPs in the form of information exchange or even a shared infrastructure to make a meaningful impact on the threat for their subscribers.

Another example is Europol's multi-lingual, multi-jurisdictional NoMoreRansom.org platform, which brings together law enforcement agencies and IT security companies to identify and provide ransomware decryption tools for free to the general public, including the option to file a police report to the victim's country. As of 2022, the platform generates over 1 million decryption tool downloads each year and has saved ransomware victims around € 1 billion.[39]

5.6.3 Information sharing initiatives

Where an ISP finds itself the target of a particular attack, or identifies a vulnerability that exposes its operations to attack or failure, there are advantages to sharing this information with other ISPs so that they can assess their exposure to a similar attack or vulnerability. This important type of information sharing can expedite the 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) have an important role to play here, but alternatives such as informal ISP Fraud and Security Forums, Information Sharing and Analysis Centres (ISACs) or bilateral communication can also be helpful where a national CERT is not fully operational, or the incident falls out of scope of the responsibilities of that CERT.

It can also be helpful in such informal Fraud and Security Forums or ISACs to involve law enforcement agencies, if they have a (cyber)crime prevention role, in a collaborative fashion.

By setting up regular meetings, properly configured communications channels and procedures, and perhaps joint exercises, trust and rapport can be built between key players pre-emptively. This will enhance the expedience and efficacy of this voluntary network should the need arise.

5.6.4 Mutual awareness 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 the relevant state agencies on, for example, what data they have, how to request it, common challenges experienced with requests received and so on. State agencies can in turn provide information to ISPs on any relevant or upcoming changes to regulatory regimes, requirements for information retention and so on.

The format of mutual awareness initiatives can be wide-ranging, from ISP involvement in police or judicial training events to law enforcement involvement in private security conferences.

The Council of Europe regularly provides multi-stakeholder conferences and training initiatives to Eastern Partnership countries. It has proven particularly productive when representatives from various stakeholder groups are able to join, exchanging views as well as contact details.

[39] NoMoreRansom.org. https://www.nomoreransom.org/en/index.html

6 Situation reports

To assess the situation regarding liability framework, regulatory obligations and voluntary cooperation within each of the EAP countries, a survey was circulated in 2017 to relevant agencies within those countries. In the sections below, a summary of the situations as reported were contained. Following the surveys, the Council of Europe has implemented its Cybercrime and Cybersecurity Barometer in the EAP region in 2021-2022, followed by several conferences where the situations were further elaborated upon. Finally, complementary desk research was performed mid-2022 and some text was restructured to improve comprehensive legibility.

Where the situation has changed since 2017, the following sections contain updates.

6.1 Armenia

The Cyber Barometer found that over ninety percent of the Armenian population aged 18-65 has internet access, a similar percentage to enterprise staff. While online activities are widespread, cybercrime awareness is comparably lower. Although respondents consider it the most worrying crime type, they classified their reporting activity to the authorities as low. The cyber security situation is perceived to have deteriorated during the COVID-19 pandemic as well as due to the military conflict. Recommendations include raising awareness, building capacity at public institutions and strengthening legislation and regulations on cyber security.[1]

In the Republic of Armenia, the principle legal instruments regulating the obligations of Internet Service Providers are the Law on Electronic Communications[40] and the decisions and regulations of the Public Services Regulatory Commission (PSRC),[41] such as the Regulation on Licensing, Regulation on Radio Frequency Usage Authorization, Regulation on Numbering Resource Usage Authorisation as well as licenses for network operation of the Internet Service Providers. PSRC decisions typically involve hearings, as well as meetings open to the public.

The PSRC's regulatory competencies include 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. It does not guide the planning of network topologies.

Any person who is seeking to provide public electronic communication services by making use of the network infrastructures of the existing operators only has to notify the PSRC prior to deployment of its services. Under specific conditions, a license may need to be obtained.[42]

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.

The principle of *network neutrality* is supported in the government's *principles of internet governance*[43] and the PSRC requires ISPs to inform subscribers of any discriminatory network traffic management policies.

[40] Law of the Republic of Armenia on Electronic Communications. https://www.arlis.am/Annexes/4/elektr_com_en.pdf

[41] Public Services Regulatory Commission of the Republic of Armenia. http://www.psrc.am

[42] Republic of Armenia Law on Licensing. http://www.parliament.am/law_docs/270601HO193eng.pdf

[43] On Approving the Principles of Internet Governance, Government of the Republic of Armenia. http://igf.am/wp-content/uploads/2015/03/IG_Principles_EN.pdf

Except in emergency circumstances, a court order is required for blocking, deletion or prevention of certain types of information being hosted or made accessible online.

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

Content blocking is typically done by deregistering sites using .am or .հայ top-level domains.[44]

In accordance with Article 49 (Confidentiality of customer information) of the Law on Electronic Communications,[45] every operator and service provider shall regard and treat as confidential all information regarding services used by their customers. This duty is enforced by the 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 an actor has failed to comply with the relevant provisions of the law. In relevant cases, the PSRC may change, suspend, or request for judicial termination of a license.

An ISP may respond to requests for access to subscriber data only within the legal scope of Article 49. 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 a request for access to subscriber data.

The PSRC regulations specify that business records of phone calls (time, duration, caller phone number and correspondent phone number) must be retained for two years. Enforcement measures and penalties starting at approximately € 10,000 are available to the PSRC when a communications provider does not conform with the requirements to retain phone call records. Additionally, the Personal Data Protection Law[46] mandates that service providers store only personal data required for billing purposes, overseen by the Personal Data Protection Agency.

For IP connections there is no obligation on the ISPs, although the main operators have signed MOUs with the Investigative Committee, standardizing cooperation and undertaking an obligation to keep records of internet traffic data.[7] In 2019, the PSRC proposed additional data-retention requirements, but these have not been effectuated following public debate.

---

[44] Internet Society of Armenia. http://www.isoc.am

[45] See footnote 46 for source. Article 49. Confidentiality of customer information:

«1. Every operator and service provider shall be obliged to treat and keep as confidential information regarding the type, location, purpose, destination, quantity, and technical conditions of services used by its customers.

2. An operator or service provider shall be entitled to disclose such information:

(1) in cases and in the manner provided for by law, in connection with surveillance, inquest, or criminal prosecution with regard to a criminal offense or threat to national security;

(2) upon the written consent of the customer;

(3) where the disclosure is necessary in defense of the operator or service provider (proceedings are pending against that operator or service provider). The customer may request that such disclosure be made on a confidential basis at an in-camera proceeding.

3. An operator or service provider shall not be liable for any damage caused as a result of disclosure of information made pursuant to part 2 of this Article.»

[46] Law of the Republic of Armenia on Protection of Personal Data.
http://www.foi.am/u_files/file/PersonaldataprotectionlaW_ENG.pdf

In accordance with Article 50 (Interception, recording or disclosure of messages)[47] 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 (although national security services may intercept for a limited amount of time in case of an imminent threat). In 2020, the legal framework was expanded to allow law enforcement to seek and obtain a warrant to tap phones for surveillance purposes.[48]

Therefore, in accordance with the procedures prescribed by the law, all operators and service providers must grant law enforcement access to any equipment, facilities, switches, routers or other similar. The PSRC regulations and, if applicable, license pre-conditions specify that an ISP must provide the technical ability to perform lawful interception. The PSRC may impose a penalty of at least € 10,000 for non-conformance with these requirements.

The Personal Data Protection Law[46] applies to the processing and security of personal data held by ISPs for business purposes. The Personal Data Protection Agency checks and enforces compliance and is responsible for the recognition of electronic systems for processing personal data and checking the devices, including software.[9]

If an ISP becomes aware of a data breach, it should fix this, inform the subject and in some cases report to the Personal Data Protection Agency. Additionally, if the data breach resulted from a criminal offence, the ISP has the right to inform the police. In general, should an ISP become aware of a crime conducted on or via its infrastructure, the ISP similarly has a right to inform the police not the obligation to do so – except for the general obligation deriving from the Criminal Code to report (serious) crimes.[49]

The *2020 National Security Strategy of the Republic of Armenia*[50] addresses the need to ensure open and safe information and cyber domains. *Armenia's Digitization Strategy 2021-2025*, aiming to improve digital government and e-commerce use, includes certain cyber security and data protection measures. For the longer term, strategic aspects related to digital infrastructure as well as cyber security have been addressed in the *Armenia Digital Agenda*.[51]

---

[47] See footnote 40 for source. Article 50. Interception, recording, or disclosure of messages:
«1. A person other than a party to a message transmitted by any electronic communications means may intercept, record, or disclose the content of such message only upon the written consent of the parties to the message or upon a court order in cases and in the manner provided for by law.
2. In addition to the provisions of part 1 of this Article, operators of public or private electronic communications networks and providers of public or private electronic services as well as their employees or representatives may intercept or redirect messages or signals, without disclosing them, where such interception or redirection of signals is conditioned by the exercise of their official duties.
3. In cases and in the manner provided for by law, all operators and service providers shall be obliged to provide access to law enforcement and national security personnel to any communications equipment, facilities, switches, routers, or other similar equipment, including wiretapping devices.»

[48] Parliament gives police authority to conduct phone tapping surveillance, Armenpress. https://armenpress.am/eng/news/1002039.html

[49] As discussed in the CoE's Cyber Barometer for Armenia, section 6.7.9.

[50] National Security Strategy of the Republic of Armenia. https://www.mfa.am/filemanager/security%20and%20defense/Armenia%202020%20National%20Security%20Strategy.pdf

[51] Armenia Digital Agenda 2030: Long-Term Strategy Presented, Government of the Republic of Armenia. https://www.gov.am/en/news/item/9211/

Incidents and emergencies

The Armenian informal CERT, CERT-AM,[52] collects and analyses information about cyber incidents and is operated by civil society. As such, it is not a fully operational government CERT.[53] Therefore, Armenia is the only EAP country with no representation in the international FIRST network,[54] which aims to globally connect (cyber) incident response and security teams.

Since the previous edition of this report, in 2017, Armenia has seen two states of emergency impacting the liabilities of ISPs, namely the COVID-19 pandemic and a military conflict. At time of writing, both these states of emergency have been lifted.

Under Article 4(4) of the Law on Electronic Communications,[40] the Armenian government is empowered to assume responsibility for the operation and management of any or all electronic communications networks or services during a state of emergency.

During these two states of emergency, authorities were permitted to designate government-approved sources of content related to the emergency, delete certain content deemed to be contradictory or incendiary, as well as order its expeditious removal under threat of fines.[55]

Additionally, during half of 2020, telecommunications companies were temporarily obliged to provide subscriber location metadata in order to facilitate COVID-19 contact tracing.[56]

6.2 Azerbaijan

The Cyber Barometer found that in Azerbaijan, with its digital divide between the capital and other areas, over seventy percent of respondents have internet access. Regarding cybercrime, botnets and phishing were the most prevalent offences in 2021, whereas the national CERT succeeded in increasing public awareness of online fraud in that year. Focus group participants noticed the increase of online crime during the COVID-19 pandemic. In general, over seventy percent of respondents have heard of cybercrimes taking place, but less than one-sixth of them consider themselves to be a relevant target – what the Barometer calls the *perception gap.* Recommendations include raising awareness and cyber security competence, unifying legal frameworks pertaining to cybercrime and developing a national cyber security strategy.[2]

No information was provided by the authorities of Azerbaijan directly in relation to this study.

The main authority responsible for the telecommunications area is currently known in English as the Ministry of Digital Development and Transport (DDT).[57] The DDT is responsible for policy planning and state regulation, control and coordination in the telecommunications area.

In 2021, the DDT established two regulatory authorities: the Information and Communication Technologies Agency (ICTA) and the Innovation and Digital Development Agency (IDDA).

[52] CERT-AM. https://www.cert.am

[53] This was discussed and confirmed by participants of the CoE's 2022 Criminal Justice Forum in Yerevan.

[54] FIRST Members around the world. https://www.first.org/members/map

[55] What to expect during state of emergency, Government of the Republic of Armenia. https://www.gov.am/en/news/item/9730/

[56] Armenia: Parliament Passes Bills to Access Mobile Phone Data to Identify Covid-19 'Contact Circles'. https://hetq.am/en/article/115353

[57] Ministry of Digital Development and Transportation of the Republic of Azerbaijan. www.mincom.gov.az

According to the DDT, whereas until 2000 a licensing regime for ISPs had existed – which still applies to mobile operators – now, any natural or legal person in the country is free to engage in the activity[58] although international connectivity is routed through two designated providers.

The main legislative framework pertaining to ISPs and their obligations has been provided since 2005 by the Law on Telecommunications, which inter alia regulates the contractual identification of subscribers to any communications service.[59] Pursuant to its Article 33, ISPs have obligations to operate in accordance with legislation and the protection of the rights of their customers. In addition, Article 38 contains regulations on the protection on privacy in telecommunications. ISPs are to ensure confidentiality, while disclosure of information and interception is permitted only if provided by legislation, like it is in the case of subscriber data. Article 39 tasks providers to set up conditions for carrying out operative-search activities by authorized state agencies.[7] Authorities generally need a court order to obtain further access.[60]

Regarding personal data, the Law on Personal Data defines the concept narrower than, for example, the GDPR does, construing it as data enabling identification of a natural person.[9] The DDT maintains a state register of information systems of individual information. Collection and processing of personal data in information systems is allowed only after their registration.[61]

By default, ISPs are not liable for the content of data transmitted, unless further provided for by legislation. The authorities may order the removal or blocking of content, after which court approval must be sought[62] and the internet resource is added to a list of prohibited URLs.[63]

In the Cyber Barometer, a representative of the state security service stated that there exists a mandatory duty for them to perform penetration testing on all state services twice a year.[64] This is in line with the country's *Strategic Roadmap for Developing Telecommunications and Information Technologies*.[65]

Incidents and emergencies

A national CERT – CERT.AZ has been established under the Cyber Security Service.[66] In several Cyber Barometer focus groups, it was mentioned by professionals as a popular agency to report cyber incidents to.[2] Both CERT.AZ and the government CERT[67] are members of FIRST.[54]

According to Article 5 of the Telecommunications Law, in the event of a military or emergency situation, general telecommunications networks may be managed centrally by the authorities.

[58] Information Technologies: Internet, Ministry of DDT. https://mincom.gov.az/en/view/pages/10/

[59] https://cert.az/t/u/document/2019/07/12/telekommunikasiyaqanun3.doc

[60] As discussed in the CoE's Cyber Barometer for Azerbaijan, section 6.8.2.1.

[61] 'The rules of state registration of personal data information systems and the cancellation of state registration', Decision № 149 of the Cabinet of Ministers of Azerbaijan Republic on 17 August 2010. https://mincom.gov.az/en/view/pages/10/

[62] Azeri court supports block on several media websites, Reuters. https://www.reuters.com/article/us-azerbaijan-media-idINKBN1882NT

[63] Law of the Republic of Azerbaijan on Information, Communication and Data Storage, article 13-3.6. https://e-qanun.az/framework/3525

[64] As discussed in the CoE's Cyber Barometer for Azerbaijan, section 6.7.2.

[65] https://monitoring.az/assets/upload/files/6683729684f8895c1668803607932190.pdf

[66] https://cert.az/en/

[67] https://cert.gov.az/en/

During the COVID-19 pandemic, administrative and criminal liabilities were introduced for the placement of certain information or failure to prevent it.[68] Following declaration of martial law in 2020, the DDT had seen the need to enforce a general reduction in internet connectivity.[69]

6.3 Belarus

Users in Belarus benefit from the country's well-developed ICT infrastructure, which has seen steady expansion in the fields of fibre-optic connectivity as well as a switch to digital television. Access to the internet has increased in recent years, up to 85 percent of the population. According to official statistics, the mobile phone penetration rate was over 120%, due to a near-full coverage the country's territory.[70] Social media are being utilized by almost 4 million people, over 40% of the population.[71] According to the Ministry of Internal Affairs of Belarus, cybercrime increased with 25% in 2020 alone, with Minsk being the centre of growth and phishing being the primary crime, followed by malware, online fraud and attacks on banks.[72]

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

- Law on Telecommunications (2005/2021);[73]
- Decree on Licensing (2010);[74]
- Decree on Measures improving Use of the National Segment of the Internet (2010);[75]
- Decree on Peculiarities of the Use of the National Segment of the Internet (2019);[76]
- Resolution on the Rules for the Provision of Telecommunication Services (2006);[77]
- Order on determining ISPs authorized to provide services to state bodies, etc. (2010)[78]

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:

---

[68] Legal news, Deloitte Legal. https://www2.deloitte.com/content/dam/Deloitte/az/Documents/legal/24%20March%202020%20Legal%20News.pdf

[69] Azerbaijan lifts restriction on internet access, Ministry of DDT. https://mincom.gov.az/en/view/news/1050/azerbaijan-lifts-restriction-on-internet-access-

[70] May 17 is World Telecommunication and Information Society Day, Infopolicy. http://www.infopolicy.biz/?p=16960

[71] Digital 2021 – Belarus, We Are Social/Hootsuite. https://datareportal.com/reports/digital-2021-belarus

[72] Belarus reports increase in cybercrime. https://smartpress.by/news/2754

[73] Law of the Republic of Belarus of 19 July 2005: 'On Telecommunications.' Amended in 2021. https://oac.gov.by/public/content/files/files/law/laws-rb/2005-45-z.pdf

[74] Decree of the President of the Republic of Belarus of 1 September 2010, № 450 'On licensing of certain types of activities.' https://oac.gov.by/public/content/files/files/law/decrees-rb/2010-450.pdf

[75] Decree of the President of the Republic of Belarus of 1 February 2010, № 60 'On measures to improve the use of the national segment of the Internet.' https://oac.gov.by/public/content/files/files/law/decrees-rb/2010-60.pdf

[76] Decree of the President of the Republic of Belarus of 18 September 2019, No 350 'On the peculiarities of the use of the national segment of the Internet.' https://oac.gov.by/public/content/files/files/law/decrees-rb/2019-350.pdf

[77] Resolution of the Council of Ministers of the Republic of Belarus of 17 August 2006, № 1055 'On Approval of the Rules for the Provision of Telecommunication Services.' https://www.etalonline.by/document/?regnum=c20601055

[78] Order of the Operations and Analysis Center under the President of the Republic of Belarus № 60, dated 2 August 2010, 'On approval of the Regulation on the procedure for determining ISPs authorised to provide Internet services to state bodies and organisations using information that constitute state secrets in their activities.' https://oac.gov.by/public/content/files/files/law/prikaz-oac/2010%20-%2060.pdf

- Law on Mass Media (2008)[79] amended in 2021;[80]
- Decision regulating the Procedure for Limiting Access to Internet Resources (2018).[81]

The Ministry of Communications and Informatization oversees the ISPs in the following ways, either directly or through the State Inspectorate for Telecommunications:[82]

- Development and implementation of telecommunication development programmes;
- Coordination of creation and development of telecommunication networks;
- Long-term planning of the use of the radio-frequency spectrum for civil purposes;
- Monitoring and centralised management of the public telecommunication network;
- Establishment of a unified procedure for interaction of telecommunication networks;
- Determining requirements for telecommunication networks to ensure their functioning and protection from unauthorised access to them and messages transmitted thereon;
- Regulation of the activities of telecommunication operators;
- Allocation and withdrawal of numbering resources;
- International cooperation such as coordinating with international organisations and telecommunications administrations, ensuring the fulfilment of treaty obligations;
- Development and adoption of regulatory legal acts.

In 2022, new powers were being added to further manage digital development processes, digital transformation of the state administration and all branches of the national economy.[83]

The Operations and Analysis Center (OAC) under the President regulates efforts to assure the cyber security in the national segment of the internet,[84] overseeing ISPs in the following ways:

- Coordinating government agencies and Internet Service Providers on information security when using resources of the national segment of the internet;
- Setting requirements on the provision of data services and IP-telephony;
- Licensing data services and IP-telephony;
- Determining the telecommunication operators authorised to pass inter-network traffic;
- Determining the operators authorised to link international traffic and foreign networks;
- Defining terms for connection to telecommunication networks and the order thereof;
- Regulating tariffs for telecommunication services and data transmission;
- Countering unfair competition, protecting the rights of operators and service providers;
- Taking measures to resolve disputes between telecommunication operators;
- Representing the country in international organisations on internet security issues;
- Exercise other powers in accordance with the law.

[79] Law of the Republic of Belarus of 17 July 2008 'On Mass Media' (Articles 38, 51-1).
https://etalonline.by/document/?regnum=h10800427

[80] 2021 amendment to the law referred to in the previous footnote.
https://president.gov.by/en/events/aleksandr-lukashenko-signs-mass-media-law

[81] Decision of the Operations and Analysis Center Under the President of the Republic of Belarus, the Ministry of Communications and Information of the Republic of Belarus of 19 February 2015, № 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, update 3 October 2018, No 8/10/6'.
https://oac.gov.by/public/content/files/files/law/resolutions-oac/2018-8-10-6.pdf

[82] List of Supervisory Bodies and Area of their Control (Supervisory) Activity, approved by the Decree of the President of the Republic of Belarus, № 510 of 16 October 16 2009, amended on 28 February 2022.
https://cis-legislation.com/document.fwx?rgn=29463

[83] On the state administration agency in the sphere of digital development and informatization.
https://president.gov.by/en/documents/decree-no-136-of-7-april-2022

[84] Operations and Analysis Center under the President of the Republic of Belarus.
https://president.gov.by/en/statebodies/the-operational-and-analysis-center-under-the-president

When applicable, the OAC acts as a focal point towards the responsible Ministry, for example when supervising the fulfilment by licensees of licensing conditions.[84]

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, owners of internet resources are required to analyse the content of their information to prevent materials aimed at illicit drug trafficking.[85] 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 services. This is also decided upon by competent authorities. Liability for content is limited, since ISPs are to act on authorities' orders only.

The Law on Telecommunications[73] (Article 54) guarantees the secrecy of telephone and other messages transmitted over telecommunication networks and provides an obligation on operators and providers to ensure this secrecy, except in cases provided for by legislative acts.

Similarly, the requirement to protect the secrecy of subscriber information is reflected in the Decree on Information Protection.[86] Information on the facts of providing services may only be provided to subscribers or their representatives, except where provided for by the law.

In accordance with Article 18 of the Law on Information,[87] information on the private life of an individual and personal data is information whose dissemination and/or provision is limited with no-one having the right to demand its provision from an individual or to receive it in a manner contrary to the will of the individual, except when provided by the law. Such private information includes personal and family secrets, the privacy of telephone conversations, postal and other communications, as well as data concerning health. Collection, processing or storage of such information shall be carried out only with the written consent of this individual, unless otherwise provided by legislative acts. Article 32 also contains a provision requiring measures to protect personal data from unlawful processing or disclosure, whereas a proposed data protection law would introduce security standards and sanctions related to breaches.[9]

Applicable rules and regulations to the retention of traffic data (including calls) are as follows:

- Decree on Interaction with Bodies that carry out Operational Search Activity (2010);[88]
- Decree on Urgent Measures to Counter Illicit Drug Trafficking (2014);[85]
- Resolution on Storage of Data about Resources visited by Internet Users (2015);[89]
- Decree on Measures improving Use of the National Segment of the Internet (2010);[75]
- Decree on Peculiarities of the Use of the National Segment of the Internet (2019);[76]

[85] Paragraph 8 of the Decree of the President of the Republic of Belarus of 28 December 2014, № 6 'On Urgent Measures to Counter Illicit Drug Trafficking': *«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.»*

[86] Presidential Decree of the President of the Republic of Belarus of 16 April 2013, № 196 'On some measures to improve the protection of information'.
https://oac.gov.by/public/content/files/files/law/decrees-rb/2013-196.pdf

[87] Law of the Republic of Belarus of 10 November 2008, № 433-3 'On information, informatization and protection of information.' https://oac.gov.by/public/content/files/files/law/laws-rb/455-3.pdf

[88] Decree of the President of the Republic of Belarus № 129 of 3 March 2010 'On approval of the Regulation on the procedure for interaction of telecommunication operators with bodies that carry out operational search activity.' https://oac.gov.by/public/content/files/files/law/decrees-rb/2010-%20129.pdf

[89] Resolution of the Ministry of Communication and Informatization of the Republic of Belarus № 6 dated 18 February 2015 'On approval of the Instruction on the procedure for the formation and storage of information about information resources visited by users of Internet services.'
https://cis-legislation.com/document.fwx?rgn=74044

- Regulation on Technical Means for Operational-Search Activities (2016).[90]

Internet Service Providers and phone operators must store identification and usage data of subscribers and their devices when providing services. Hotspots and internet cafés have to carry out user identification and store information about services provided. As of 2019, website owners must verify profiles of online commentators, including name, date and place of birth, mobile phone number, email and IP address.[91] Such data is retained for at least a year, as per Paragraph 6 of the Decree on Measures improving Use of the National Segment of the Internet.[75] Access to stored data is made in accordance with Articles 209-212 of the Criminal Procedure Code.[92] Non-compliance is penalized in Article 23.4 of the Administrative Code.[93]

In accordance with clauses 75-77 of the Decree on Licensing,[74] a license violation by a licensee can be followed by an instruction to eliminate it within a certain amount of time, where non-compliance may lead to a suspension or finally a termination of the license. Article 12.7 of the Administrative Code[93] provides for an administrative fine if there is no crime in these acts. Furthermore, as of 2021, the Law on Telecommunications[73] includes a provision for authorities to shut down or limit the operation of telecommunications facilities.

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

- Decree on Interaction with Bodies that carry out Operational Search Activity (2010);[88]
- Law on Operational Investigative Activity (2015).[94]

In accordance with this Decree (Articles 10-11), the cost of the required equipment is borne by the ISPs and the law enforcement agency. The operational search activity is sanctioned by the prosecutor or their deputy, whereas implementation decisions shall be made by an official of the body that carries out the search. The decision to conduct an operational search must be motivated in accordance with the Law on Operational Investigative Activity[94] (Article 19).

Current requirements for the security of data held by ISPs for business purposes are general and are provided for in Chapter 7 of the Law on Information.[87] The obligation to report a 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.[92]
ISPs can be asked or made to take down illegal content upon a request to do so in accordance with the decision of the Operations and Analysis Center.[81] In 2019, a new Information Security Concept was adopted which also addresses illegal and harmful content and its dissemination.[95]

In 2021, the Law on Mass Media[79] was amended,[80] expanding the list of information, the dissemination of which by the media as well as through internet resources is prohibited. Restriction of access to certain internet resources and online media can be ordered by the Prosecutor's Office as well as decided by the Interagency Commission on Information Security.

---

[90] STB 2271-2016, 'Telecommunication networks. System of technical means for ensuring operational-search activities. Technical requirements.'
https://www.belaruslaws.com/m-223-stb-rb.aspx?section=5230

[91] The Council of Ministers approved the procedure for identification of internet commentators in Belarus.
https://devby.io/news/sovmin-commentators

[92] Criminal Procedure Code of the Republic of Belarus, 16 June 1999.
http://etalonline.by/?type=text&regnum=HK9900295#load_text_none_1_3

[93] Code of the Republic of Belarus on Administrative Legislation of 21 April 2003.
https://www.etalonline.by/document/?regnum=hk0300194

[94] Law of the Republic of Belarus № 307-Z of 15 July 2015 'On the operational investigative activity.'
https://cis-legislation.com/document.fwx?rgn=77612

[95] Belarus President approves information security concept.
https://president.gov.by/en/events/belarus-president-approves-information-security-concept-20711

Although a full cyber security strategy has not been published, aspects are included in the concepts of information security[95] and national security maintained by the Security Council.[96]

Incidents and emergencies

ISPs share with each other information about ongoing threats or incidents. State authorities and ISPs are given the opportunity to use an automated system for exchanging such information. The national Computer Emergency Response Team, CERT.BY, is a member of the international FIRST network[54] and has a website[97] where any stakeholder can leave a report.

The Law on the State of Emergency[98] does not mention the internet specifically, although Article 13 enables content limitations on mass media, which require a presidential decree. As the Law on Mass Media[79] [80] considers websites to be a type of mass media, consequently the government can block access to online resources.[99] During the COVID-19 pandemic, Belarus did not introduce official emergency measures;[100] travel restrictions were lifted early 2022.[101]

6.4 Georgia

The Cyber Barometer found that nearly eighty percent of the population regularly use the internet, on average for over four hours a day. A similar percentage agree that cybercrime represents a real threat, considering online intimidation and abuse the most pressing issues, followed by data breaches and identity theft. Nearly ninety percent of the population, however, believe they have not recently been targeted by cyber criminals. Similarly, almost half of all enterprises surveyed do not spend money on cyber security, although one-third of them do conduct staff awareness training. According to business focus group participants, the infrastructure in Georgia has considerably improved, to be one of the most advanced sections of the private sphere, with big ISPs embracing international security standards and the country gradually implementing the EU's NIS Directive. Recommendations include capacity building within public and private sectors and further increasing citizens' basic cyber hygiene.[3]

[96] Security Council of the Republic of Belarus. https://president.gov.by/en/president/glavnokomanduyushchiy/sovet-bezopasnosti

[97] CERT.BY. https://cert.by/?lang=en

[98] Law of the Republic of Belarus № 117-Z of 24 June 2002, amended 14 July 2021 'On the state of emergency'. https://cis-legislation.com/document.fwx?rgn=1988

[99] When the national security is threatened, the Ministry of Internal Affairs can block access to internet resources – Kazakevich, Belta. https://www.belta.by/society/view/pri-ugroze-natsbezopasnosti-mvd-mozhet-blokirovat-dostup-k-internet-resursam-kazakevich-398355-2020/

[100] COVID-19 and the Belarusian economy, CASE Belarus. https://case-belarus.eu/covid-19-and-the-belarusian-economy-4-issues/

[101] COVID-19 in Belarus, Ministry of Foreign Affairs. (e.g.) https://netherlands.mfa.gov.by/en/covid_19/

The Georgian National Communications Commission, abbreviated to GNCC or ComCom,[102] has been the regulatory authority of broadcasting and electronic communications since 2000. The country's principle legal instruments regulating obligations of Internet Service Providers are:

- Law on Electronic Communications (2005, amended 2011, 2013);[103]
- Resolution on Electronic Communications (2006).[104]

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 a declaration, the form of which is approved by the GNCC.

The Law on Electronic Communications[103] describes the role of the Commission in Article 11:

- Independently regulate the activities of authorised persons and the use of the radio-frequency spectrum and number resource by license holders as defined in this law.
- Main tasks of the GNCC:
    - Developing a competitive environment in electronic communications;
    - Ensuring a wide range of affordable quality service to end-users, including persons with disabilities;
    - Assisting implementation of networks and investing in innovative technologies.
- Main functions of the Commission:
    - Authorization of activities in the field of electronic communications;
    - Management of exhaustible resources and ensuring their effective use;
    - Ensure competition through analysis of the market and assigning obligations;
    - Ensuring certification, standardization and proper maintenance of equipment;
    - Oversee technical, economic and legal regulations for interconnection;
    - Resolve disputes between authorized persons, and with their consumers;
    - Overseeing compliance with licensing and licensing conditions;
    - Transparent relations with society;
    - Coordination of electromagnetic compatibility towards international contexts;
    - Representation in international organizations for electronic communications;
    - Determining rules for amateur radio communications and such radio stations;
    - Resolving disputes between license owners and/or permission holders;
    - Approvals regarding the portability system for subscriber numbers;
    - Deciding on effective regulations in response to changing market conditions;
    - Control of degrees of protection of digitally exchanged classified information.

As a regulatory body, the GNCC has no law enforcement powers, such as the authority to compel an ISP to respond to requests for access to subscriber data, but as of 2019 it can, for example, enforce non-discriminatory traffic management.[105] Violations of the Law on Electronic Communications are treated in accordance with the Administrative Offences Code.[106] Sanctions include warnings in writing or, for repeat offenders, a fine in the amount of 0.5% of the licensee's yearly income – limited between 3,000 GEL and 30,000 GEL (Article 45) – and a

[102] About Communication Commission. https://comcom.ge/en/the-commission/about-commission

[103] Law of Georgia on Electronic Communications, 20 November 2013. https://matsne.gov.ge/en/document/view/29620

[104] Georgia National Communications Commission Resolution № 3, 17 March 2006, 'On provision of services and protection of consumer's rights in electronic communications.' https://comcom.ge/uploads/other/1/1033.pdf

[105] Georgia National Communication Commission Regulation on Rules for Determining and Checking the Quality of Internet Service Provision, 28 May 2018. https://comcom.ge/ge/legal-acts/resolutions/2018-4-.page

[106] Administrative Offences Code of Georgia. https://matsne.gov.ge/en/document/view/28216

suspension or ultimately the cancellation of the authorisation to operate (Article 19). A 2020 amendment introduced a regime for appointing a special manager to a penalized company.[107]

The Law on Freedom of Speech and Expression[108] protects ISPs against intermediary liability. However, 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 or an order by Parliament.[109]

The Resolution on Electronic Communications[104] contains rules and regulations regarding blocking, deletion or prevention of certain types of information being hosted or made accessible through an ISP (Articles 10 and 25). ISPs are not legally obliged to report illegal content, but if such content is identified it must be removed. Additionally, they must adopt measures to prevent the use of their network for the intimidation or insulting of consumers and, where applicable, must ensure the presence of mechanisms to restrict access to adult content.[110]

The Constitution[111] (Article 15) and the Law on Electronic Communications[103] (Article 8) include privacy guarantees for users and their information. The obligations of ISPs to protect the secrecy of the communications of their subscribers are reflected in the Resolution on Electronic Communications,[132] which states that providers shall ensure the confidentiality of transmitted information, while its disclosure is permitted only in accordance with the law. Furthermore, the Law on Protection of Personal Data[112] allows the Office of the Personal Data Protection Inspector to verify the legality of data processing by private organizations and to impose fines.

Article 5 of the Resolution states that service providers must store the user's identity, provided services and cost of the service for at least one year. This also holds for mobile phone services. However, public internet access points do not necessarily gather such data about customers.

Cooperation between large ISPs and law enforcement is partly codified in a 2010 Memorandum of Understanding, leading to the creation of specialized rapid-contact points.[7] Working through the MOU, updated in 2015, is considered to be effective by both ISPs and law enforcement.[7]

As part of the country's (cyber)security efforts, the Operational-Technical Agency (OTA) is responsible for surveillance across telecommunications networks, which may include directing ISPs to purchase specific equipment, and accessing their infrastructure after a court order.[113] OTA also has the right to request content data, traffic data and geolocation data in real-time.[9]

---

[107] Joint Opinion of the Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the recent amendments to the Law on electronic communications and the Law on broadcasting, adopted by the Venice Commission at its 126th plenary session. https://www.venice.coe.int/webforms/documents/?opinion=1008

[108] Law of Georgia on Freedom of Speech and Expression, 15 July 2004. https://matsne.gov.ge/en/document/view/33208?publication=5

[109] Mdzinarashvili v. Georgian National Communications Commission, Ruling by the Constitutional Court of Georgia, N1/7/1275, 2 August 2019. https://constcourt.ge/en/judicial-acts?legal=1931

[110] Georgia National Communications Commission Regulation of posting of information that poses a threat to children on the Internet, 28 February 2020. https://www.comcom.ge/ge/legal-acts/resolutions/2020-1-.page

[111] Constitution of Georgia, 24 August 1995, amendment on internet rights added in 2018. https://matsne.gov.ge/en/document/view/30346?publication=36

[112] Law of Georgia on Personal Data Protection 28 December 2012. https://matsne.gov.ge/en/document/view/1561437

[113] Amendments to the Law of Georgia on Information Security, EY, 20 January 2022. https://www.ey.com/en_ge/news/2022/01/amendments-to-the-law-of-georgia-on-information-security

Incidents and emergencies

In 2020, a five-year strategy was adopted to further develop Georgia's broadband infrastructure.[114] Georgia has developed a number of strategies on cyber security. The recent National Cyber Security Strategy (2021-2024)[115] and its Action Plan were adopted in 2021.[116] In 2022, private entities obtained a more formal responsibility in matters of cyber security.[117]

According to Article 25 of the Law on Electronic Communications,[103] service providers are obliged to protect the integrity of the network and prevent unauthorized access, offer filtering software and inform consumers about any existing risk of unauthorized access to the network. Information about ongoing threats or incidents is shared between ISPs informally, as of yet there is no uniform mechanism for exchanging such data. ISPs have an obligation regarding international call terminations for financial fraud prevention as imposed by the GNCC.

The national CERT is the Digital Governance Agency's CERT-GOV-GE, a member of FIRST,[54] whereas the civil Georgian Research and Educational Networking Association (GRENA) maintains CERT-GE since 2007, catering to educational institutions, non-profits and others.[118]

Since the previous edition of this study, internet access has been added to the Constitution as a fundamental right.[111] This may be restricted for national security reasons. Under martial law or a state of emergency, the government may assume control over the domestic internet.[119]

6.5 Moldova

The Cyber Barometer found that in Moldova, the population in general is quite active online, but relies on intuition when working with internet resources and therefore feels unprepared for dealing with cyber threats. Over half of participants found that the COVID-19 pandemic exacerbated cybercrimes, with data breaches and identity theft being regarded as the most dangerous type of cybercrime. Respondents from companies considered ransomware and CEO fraud as significant business risks, as well as commercial espionage. People and businesses are ready to involve law enforcement in case of cybercrime, but do not tend to do so unless they feel the crime is serious enough. Almost one-fifth of enterprises is familiar with the concept of a national CERT. Top recommendations included raising awareness, fostering community outreach and further embracing international security frameworks and standards.[4]

In 2007, the Electronic Communications Act[120] mandated the government to harmonize national legislation with European standards. The law established the National Regulatory Agency for Electronic Communications and Information Technology (ANRCETI), allowing Internet Service Providers to start operating without a license, simply by notifying the Agency, which is responsible for monitoring ISPs' compliance with the law and keeping a public register.

[114] Decree № 60, Ministry of Economy, 10 January 2020. http://www.economy.ge/uploads/files/2017/legislation/sainformacio_teqnologiebi/fartozolovani_qselebis_ganvitarebis_strategia_da_misi_ganxorcielebis_geqma.pdf

[115] Resolution of the Georgian Government № 482, 30 September 2021, 'On Approval of the National Cyber Security Strategy 2021-2024 and its Action Plan.' https://nsc.gov.ge/pdf/615c4f0c234b8.pdf

[116] Georgia Adopts Cybersecurity Strategy for 2021-2024, Civil. https://civil.ge/archives/446772

[117] This was discussed and confirmed by participants of the CoE's 2022 Criminal Justice Forum in Tbilisi.

[118] GRENA CERT-GE. https://www.grena.ge/eng/cert

[119] On Martial Law, Legislative Herald of Georgia. https://matsne.gov.ge/document/view/28336?publication=3

[120] Electronic Communications Act № 241-XVI of 15 November 2007. https://en.anrceti.md/files/filefield/3.1.1%20Electronic%20Communications%20Act_1.doc

The principal legislation regulating the obligations of Internet Service Providers is the Cybercrime Law.[121] Other relevant legislation is published on the ANRCETI website:[122]

- Law on Access to Information (2000);
- Law on Informatics (2000);
- Law on Basic Principles Regulating Entrepreneurial Activity (2006);
- Law on Personal Data Protection (2007);
- Law on Access to Properties and Shared Use of Infrastructure Associated with Public Electronic Communications Networks (2016);
- Law on Postal Communications (2016).

The enforcement measures and penalties that can be applied to sanction businesses such as ISPs for non-conformance with the required legal obligations are specified in the Civil Code.[123]

The Cybercrime Law strongly advocates public-private cooperation.[7] Article 5 states that : *«in the framework of cybercrime prevention and fighting activities, the competent authorities, service providers, non-governmental organizations and other civil society representatives cooperate through information exchange, experts, through joint investigation of cases and identification of offenders, training personnel, through initiatives to promote programmes, practices, measures, procedures and minimum standards for the security of information systems, information campaigns on cybercrime and other risks to computer users, etc.»*

According to Article 6 of the Cybercrime Law, ISPs must make users aware of the legal conditions of access and use, violation of which entails disciplinary, civil, administrative or criminal liability under law. Article 7 requires ISPs to report certain violations to competent authorities, including illegal access to information, attempts to introduce illegal programs, violation by responsible persons of the applicable rules of information (system) protection, disruption of the functioning of the information systems as well as other computer crimes.

Furthermore, Article 7 of the Cybercrime Law requires ISPs to facilitate the monitoring, surveillance and storage of traffic data for 180 days and to ensure its unencrypted availability for 90 days. There appears to be no obligation to monitor for illegal content, however, if an ISP detects such content, the Cybercrime Law does require them to report it to the authorities.

It is a common practice for ISPs in Moldova to keep customer data for at least twelve months.[4] The Law on Electronic Commerce[124] specifies the rules applying to the retention of data by ISPs for business purposes, as well as its required security. The Cybercrime Law specifies rules that apply when an ISP becomes aware of a data breach or other crimes conducted on or via its infrastructure. The main obligation is to report this in accordance with Article 7 of that law.

ISPs are required to respect the privacy of personal data as covered by the Law on Personal Data Protection. The 2007 law[125] was updated in 2011 to reflect EU Directive 95/46/CE and

[121] Law № 20-XVI dated 3 February 2009 on preventing and fighting cybercrime, amended in 2012, 2013 and 2018. http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=333508

[122] Legislation: Laws, ANRCETI. http://en.anrceti.md/fileupload/1?page=1

[123] Civil Code of the Republic of Moldova, № 1107-XV, 6 June 2002, amended on 11 November 2021. https://cis-legislation.com/document.fwx?rgn=3244

[124] Law on Electronic Commerce, № 284-XV, dated 22 July 2004 transposes Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce). https://europa.eu/capacity4dev/file/111993/download?token=YkIAnq10

[125] Law on Personal Data Protection, № 17-XVI, 15 February 2007. Note: replaced in 2011 and 2021. http://en.anrceti.md/files/filefield/3.1.7%20%20Law%20on%20Personal%20Data%20Protection_0.doc

again in 2021 to incorporate portions of the GDPR.[126] The National Center for Personal Data Protection (NCPDP) is given the role of Moldova's national DPA with wide competences,[9] similar to those available under the GDPR, including blocking the processing of specific personal data.

Legal interception is performed on the basis of the Criminal Procedure Code.[127] Its Article 132 lists a series of crimes under which the interception and communication recording of suspects and others may be ordered, as well as special measures for communications interception and recording of victims and similar parties, on their request, for as long as they agree to allow it.

The cost of equipment required to facilitate legal interception is borne by the ISP.

As per the Criminal Procedure Code, the prosecutor serves warrants for interception, certified by an investigative judge, whose decision shall contain a statement with respect to criminal liability of the person who will technically perform the special investigative measure. The interception shall be carried out by the criminal investigative body or an investigative officer.

Incidents and emergencies

In 2018 the National Cyber Security Strategy for 2019-2024 was adopted by Parliament, including the Action Plan concerning its implementation.[128]

Although Moldova has regular procedures in place for blocking access to internet resources, including safeguards to protect children,[129] during the COVID-19 pandemic, the Security and Intelligence Service (SIS) used emergency laws to order ISPs to block access to websites.[130]

In 2022, Moldova declared a state of emergency due to the military situation in its neighbouring country. ANRCETI approved a decision requiring internet providers to block access to certain online resources and for operators to remove specified information.[131]

Moldova has two CERTs operating on national scale. MD-CERT, established in 2007, handles incidents in the research and education network. CERT-GOV-MD, established in 2010, has the responsibility for handling information security incidents and offering cyber security services to public administration authorities. The latter is listed in the international FIRST community.[54]

6.6 Ukraine

Due to the volatile situation, most of the updated information pertains to the preceding years. Kindly note that the Cyber Barometer was completed before the military escalation in 2022.

---

[126] Law on Personal Data Protection № 133 of 8 July 2011, amended by № 175 of 11 November 2021. https://www.legis.md/cautare/getResults?doc_id=128924&lang=ro

[127] Criminal Procedure Code of the Republic of Moldova, № 122-XV, 14 March 2003. https://www.legis.md/cautare/getResults?doc_id=129481&lang=ro#

[128] Decision № 257 of 22 November 2018 regarding the approval of the Information Security Strategy. https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro

[129] Moldova has started to increase internet safety, Digital Report. https://digital.report/v-moldove-pristupili-k-povyisheniyu-bezopasnosti-interneta/

[130] Moldova authorities issue takedowns orders on 52 websites accused of spreading 'fake news', International Press Institute. https://ipi.media/alerts/moldova-authorities-issue-takedowns-orders-on-52-websites-accused-of-spreading-fake-news/

[131] Moldova telecom authority orders ISPs to block disinformation sources, Telecompaper. https://www.telecompaper.com/news/moldova-telecom-authority-orders-isps-to-block-disinformation-sources--1411466

The Cyber Barometer found that in Ukraine, over three-quarters of the population use the internet. The President has created a Ministry of Digital Transformation to increase digital skills of the people and their government. A significant growth in internet usage was registered during the COVID-19 pandemic. The vast majority of citizen respondents are familiar with the notion of cybercrime, although less than thirty percent of companies consider it a top-5 risk. Citizens feel data breaches and identity theft are the most dangerous types of cybercrime, followed by online intimidation or abuse and ransomware. Enterprises worry about ransomware as well, but even more about CEO fraud. Recommendations include upgrading the skillset of law enforcement and increasing awareness of the need for cyber security.[5]

ISP activities are carried out subject to the inclusion in the telecommunications register, as maintained by the National Commission for the State Regulation of Communications and Informatization (NCCIR)[132] and, where specified by law, with the appropriate license or permit. Telecommunications operators – who construct and operate electronic networks – are required to obtain a license for the operation of their network.[133] Since 2019, in most cases where no radio equipment is installed, a license is not required. One administrative sanction is exclusion from the telecommunications register and the subsequent cessation of information exchanges.

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

- Telecommunications Law (2022);[133]
- Resolution on Telecommunications Services (2012);[134]
- Decree on a Register of Electronic Communications Providers (2022);[135]
- Decree on Licensing Conditions for Telecommunications Networks;[136]
- Decree on the Rules for carrying out activities in the field of Telecommunications.[137]

A number of legislative and regulatory acts established the potential duty of the ISP to block or delete information from the internet segment or restrict user access to certain resources:

- Constitution of Ukraine (Article 34 and its 2012 court interpretation);[138]
- Cyber Security Strategies of Ukraine;[142] [159]
- Decree on the Application of Personal Sanctions;[139]
- Copyright Law;[140]

[132] Decree of the President of Ukraine, № 1067/2011 of 23 November 2011, 'On the National Commission for the State Regulation of Communications and Informatization.'
http://zakon.rada.gov.ua/laws/show/1067/2011

[133] Law on Telecommunications, № 1089-IX, 16 December 2020, amended through 3 May 2022.
https://zakon.rada.gov.ua/laws/show/1089-20

[134] Resolution of the Cabinet of Ministers of Ukraine on the approval of the rules for providing and receiving telecommunication, № 295, 11 April 2012, with changes through 2013-2021.
http://zakon.rada.gov.ua/laws/show/295-2012-%D0%BF

[135] Decree of the NCCIR on the issue of keeping a register of suppliers of electronic communications networks and services, № 30, 20 April 2022. https://zakon.rada.gov.ua/laws/show/z0502-22

[136] Decree of the NCCIR on licensing conditions for carrying out activities in the field of telecommunications for the provision of services for technical maintenance and operation of telecommunications networks, broadcast television and radio broadcasting networks, wire radio broadcasting and television networks, № 513, 11 November 2010, as amended by Decision № 561 of the NCCIR, 26 November 2019.
https://zakon.rada.gov.ua/laws/show/z1292-19

[137] Decree of the NCCIR on rules for carrying out activities in the field of telecommunications, № 541, 19 November 2019. https://zakon.rada.gov.ua/laws/show/z1309-19

[138] Constitution of Ukraine. http://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

[139] Decree of the President of Ukraine, № 133/2017, 15 May 2017, 'On the application of personal special economic and other restrictive measures (sanctions)'. http://www.president.gov.ua/documents/1332017-21850

[140] Law on Copyright and Neighboring Rights (1993), № 3793-XII, amended through 15 December 2021.
http://zakon.rada.gov.ua/laws/show/3792-12

- Law on State Support of Cinematography.[141]

Since the adoption of its first cyber security strategy in 2016, Ukraine has considered the fight against cybercrime to *'involve blocking by telecommunications operators and providers of a specified information resource after court decision (and a) procedure for ordering operators and providers on urgent recording and further storage of computer data and traffic data.'*[142]

A number of rules for instant blocking, removing or preventing hosting of certain categories of information is defined by law, particularly for blocking information based on copyrights and related rights. According to Article 18.3(13) of the revised Telecommunications Law, telecommunications providers are obliged to restrict access of subscribers to resources through which distribution of child pornography is carried out, on the basis of a court decision. Criminal accounts distributing such CSAE materials may be subject to ordered termination. In 2019, an obligation to report online bullying was introduced in the Code of Administrative Offences.[143]

The Decree on Personal Sanctions prohibits ISPs from providing certain users access to specific resources, according to a list maintained by the National Security and Defence Council (NSDC). Conversely, online access to resources owned by a sanctioned person may also be restricted.

Per Article 125(4) of the Telecommunications Law, providers of electronic communication services are not responsible for the content of information transmitted by their networks, except for specific cases provided for by the Law on Electronic Commerce.[144]

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 this to the competent authority.

A responsibility of a hosting provider or website owner comes in the event of failure to comply with the requirement for termination of copyright infringement and related rights using the internet, according to procedures established in Article 52(1) and 52(2) of the Copyright Law, where termination is requested by the copyright owner, or ordered by the court, respectively. Additionally, there is an obligation to monitor hosted information for such infringements.

Article 119 of the Telecommunications Law defines the general framework for protection of subscriber information. Additionally, the following Acts specify duties to protect personal data:

- The Law on Access to Public Information (Articles 7 and 10);[145]
- The Law on Information;[146]
- The Law on Protection of Personal Data.[147]

[141] Law on state support of cinematography, № 1977-VIII, 23 March 2017, amended 17 December 2021. https://zakon.rada.gov.ua/laws/show/1977-19

[142] Decree of the President of Ukraine, № 96/2016, 15 March 2016, 'On the cyber security strategy of Ukraine.' (Article 4.5) http://www.president.gov.ua/documents/962016-19836

[143] Code of Ukraine on Administrative Offences (1984), № 8073-X, amended through 14 April 2022. https://zakon.rada.gov.ua/laws/show/80731-10

[144] Law on Electronic Commerce, № 675-VIII, 3 September 2015, amended through 16 December 2020. https://zakon.rada.gov.ua/laws/show/675-19

[145] Law on Access to Public Information (2011), № 2939-VI, amended through 27 January 2022. http://zakon.rada.gov.ua/laws/show/2939-17

[146] Law on Information (1992), № 2657-12, amended through 16 November 2021. http://zakon.rada.gov.ua/laws/show/2657-12

[147] Law on Protection of Personal Data (2010), № 2297-17, amended through 1 July 2022. http://zakon.rada.gov.ua/laws/show/2297-17

Operators must retain and ensure the integrity of subscriber data, content and traffic data; however, user registration is not obligatory. The data may only be shared after a court order.

Furthermore, the Criminal Procedure Code of Ukraine[148] (Article 162) states that secrets protected by law, which are contained in things and documents, include: *'6) a person's personal correspondence and other records of a personal nature; 7) information held by operators and telecommunications providers about the connection, the subscriber, the provision of telecommunication services, including the receipt of services, their duration, content, transmission routes, etc.; 8) personal data of a person, which are in their personal possession or in the personal data base that is located at the owner of personal data.'*

Operators, telecommunications providers bear responsibility for the safety 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 from electronic versions of databases.

The rules applying to the interception of internet data and/or call content are defined in Articles 263-265 of the Criminal Procedure Code.[148] Telecommunications operators are obliged to establish, for their own means, 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.

In practice, based on the definition of the investigating judge within the framework of a criminal case, intercepted data is provided to authorised bodies of the National Police, Security Service or Anti-Monopoly Committee. The order of the investigating judge is made on the proposal of the prosecutor. The cost of the required equipment and transmission is borne by the ISP.

Legislation further establishes cases according to which the ISP must provide information to law enforcement and supervisory bodies for the performance of their tasks and powers:

- Clause 1 of the Decree on the NCCIR (2011);[132]
- Clauses 2 and 3(10) of Article 18 of the revised Telecommunications Law (2022);[133]
- Articles 2 and 23 of the Law on the National Police (2015);[149]
- Paragraphs 2 and 6 of the Regulation on the National Police (2015);[150]
- Part 1 of Article 8 of the Law on Operational and Investigative Activities (1992);[151]
- Part 2 of Article 93 of the Criminal Procedure Code (2012);[148]
- §3 of Part 1 and §1 of Part 2 of Article 25 of the Law on the Security Service (1992);[152]
- §5 of Part 2 of Article 7 of the Law on Counterintelligence Activities (2003);[153]
- Articles 22 and 22-1 of the Law on the Antimonopoly Committee (1993);[154]

[148] Criminal Procedure Code of Ukraine (2012), amended through 8 June 2022. http://zakon.rada.gov.ua/laws/show/4651-17/paran1602

[149] Law on the National Police of Ukraine, № 580-VIII, 15 July 2015, amended through 14 April 2022. http://zakon.rada.gov.ua/laws/show/580-19

[150] Decree of the Cabinet of Ministers № 877 of 28 October 2015 'On the approval of the Regulations on the National Police.' https://zakon.rada.gov.ua/laws/show/877-2015-%D0%BF#Text

[151] Law on Operational and Investigative Activities (1992), amended through 16 November 2021. http://zakon.rada.gov.ua/laws/show/2135-12

[152] Law on the Security Service of Ukraine (1992), amended through 23 September 2021. http://zakon.rada.gov.ua/laws/show/2229-12

[153] Law on Counterintelligence Activities (2003), amended through 17 September 2020. http://zakon.rada.gov.ua/laws/show/374-15

[154] Law on the Antimonopoly Committee of Ukraine (1993), amended through 23 September 2021. http://zakon.rada.gov.ua/laws/show/3659-12

- Law on Combating Terrorism (2003);[155]
- Law on Intelligence (2020).[156]

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

Under Article 105(8) of the revised Telecommunications Law, ISPs have a legal obligation to retain records of provided communications services during the statute of limitations period, but the NCCIR has no right to require the ISP to fulfil a request for access to such information. According to the accompanying Resolution on Telecommunications Services,[134] Article 39(4), ISPs must keep records of and provide information on telecommunications services provided, in accordance with procedures established by law. The general limitation period is three years.

Incidents and emergencies

During the COVID-19 pandemic, the Ministry of Digital Transformation used mobile provider data to monitor compliance with quarantine requirements.[157]

The new laws on Telecommunications and on Intelligence allow the government – under certain conditions – to restrict internet access and increase surveillance and interception. In a state of emergency or war, ISPs need to comply with the National Center for Operational and Technical Management of Electronic Communications Networks of the Special Communications Service. During crises, this Center has also kindly requested that certain users *not* be disconnected.[158] In 2021, the new Cyber Security Strategy of Ukraine[159] was approved[160] by the National Coordination Center for Cyber Security at the National Security and Defence Council of Ukraine. Early February 2022, the accompanying implementation plan was adopted by the President.[161]

CERT-UA[162] has been established as Ukraine's national CERT, located within the State Service of Special Communications and Information Protection. It is a member of the FIRST network[54] and it is well-known by IT and ISP professionals as a major source of cyber threat information.[5]

[155] Law on the Fight Against Terrorism (2003), № 638-IV, amended through 22 May 2022. https://zakon.rada.gov.ua/laws/show/638-15

[156] Law on Intelligence (2020), amended through 14 April 2022. https://zakon.rada.gov.ua/laws/show/912-20

[157] 'The Ministry of Digital Transformation has created a map demonstrating non-compliance with the rules of self-isolation by people who returned from countries where the coronavirus is raging', Ukrinform. https://www.ukrinform.ua/rubric-society/3002056-v-ukraini-stvorili-mapu-samoizolacii-de-najbilse-porusen.html

[158] 'Mobile operators agree to provide communication to Ukrainians even if no funds in their accounts', Interfax. https://interfax.com.ua/news/economic/801345.html

[159] 'A secure cyberspace is key to the succesful development of the country', Cybersecurity Strategy of Ukraine (2021-2025). https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

[160] 'The working group at the National Coordination Center for Cybersecurity at the National Security and Defence Council of Ukraine approved the draft Cybersecurity Strategy of Ukraine for 2021-2025', National Security and Defence Council. https://www.rnbo.gov.ua/en/Diialnist/4838.html

[161] 'The President gave effect to the Implementation Plan of the Cyber Security Strategy of Ukraine', State Service of Special Communications and Information Protection, 2 February 2022. https://cip.gov.ua/ua/news/prezident-nadav-chinnosti-planu-realizaciyi-strategiyi-kiberbezpeki-ukrayini

[162] CERT-UA, Computer Emergency Response Team of Ukraine. https://cert.gov.ua

7 Analysis and recommendations

For the original study, the EAP countries were sent questions on ISP liabilities. Not all countries were able to answer all questions back then. Following this updated situation report, some answers were amended, based on this research. The distinction is made typographically.

Example:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Topic	Answered & up-to-date	*(no info)*	Answered & up-to-date	*Amended as per research*	Answered & up-to-date	*Amended as per research*

In this example, Armenia, Belarus and Moldova responded in 2017 and their answers were verified or considered up-to-date in 2022 (barring minor changes). The information on Georgia and Ukraine has been *updated* as per the research for chapter 6. Azerbaijan, in this example, did not respond and in 2022, researchers were unable to draw further conclusions on the topic.

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. 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. As such access needs to be balanced with safeguards – depending on the type of data and type of access required – these safeguards will be further explored in section 7.3.

In the next paragraphs, the analysis has been broken into several sub-sections, considering different types of access that may be required, ranging from subscriber identification to real-time interception of content data. Data preservation and content blocking 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 (MOU) can be put in place between the law enforcement authorities and ISPs.

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Retention Obligation	MOU[163]	*(no info)*	Legal Obligation[164]	*Legal Obligation*[165]	Legal Obligation[166]	Legal Obligation[167]

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.

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.[168] 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

[163] 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. Retention duration is defined in the MOU, which is not available online.

[164] 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.

[165] Pursuant to Article 5 of the Resolution on Electronic Communications,[104] which states that service providers must store the user's identity, provided services and cost of the service for at least one year. This also holds for mobile phone services.

[166] Article 7 of the Cybercrime Law[121] states that *«Service providers are required to keep records of service users, … 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.»* As found in the CoE's Cyber Barometer 2021-2022, it is common practice for ISPs in Moldova to keep customer data for at least twelve months.

[167] Under Article 105(8) of the revised Telecommunications Law,[133] ISPs have a legal obligation to retain records of provided communications. According to the Resolution on Telecommunications Services,[134] Article 39(4), ISPs must keep records of and provide information on telecommunications services provided, in accordance with procedures established by law. The general limitation period is three years.

[168] See for example Article 16 and 17 of the Council of Europe Budapest Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

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. It 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 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*[169]	Yes	*Yes*[165]	Yes[170]	Yes[171]
Legislative Basis	Yes[172]	*(no info)*	Yes[173]	*(no info)*	Yes[174]	*Yes*[175]
Enforcement Authority	SNS	*(no info)*	KGB, OAC[176]	*(no info)*	Prosecutor's Office, Police	Prosecutor's Office[177]
Access to Preserved Data	Court Order	*(no info)*	Prosecutor's Order[178]	*(no info)*	Court Order	Police, AMK or SSU 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 7.3.

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 *(lawful*

[169] Although no information, or different information, was provided in response to the original questionnaire, this finding was later determined by CoE's Law Enforcement Cooperation Study of 2020.[7]

[170] Article 7(c) of the Cybercrime Law.

[171] The original response to this question in the questionnaire indicated that there are no rules, however subsequent questions about legislative basis and enforcement authority were populated as described in this summary table. This is consistent with the findings in the CoE's Law Enforcement Cooperation Study.[7]

[172] RA Law on Electronic Communications,[40] Article 50.

[173] Presidential Decree № 129[88] and Law of the Republic of Belarus on Telecommunications.[73]

[174] As per the Cybercrime Law of 2009.[121]

[175] A duty to preserve the data obtained during the investigative measures is established by part four of Article 263 of the Criminal Procedure Code of Ukraine.[148]

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

[177] 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.

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

interception) and secondly, the rules that obligation on ISPs to provide the technical ability and access to their networks 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, sometimes amended with findings of later CoE studies:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Basis for Legal Interception	Law[179]	*Law[180]*	Law[181]	*Law[182]*	Law[183]	Law[184]
Requirement to Provide Abilty	License Condition[185]	*Law*[186]	Law[173]	*Law[113]*	Law[187]	Law[188]

In the original study, the EAP 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.).

These were their responses, which were verified and further amended for this update:

[179] Article 50 of the Law on Electronic Communication.

[180] As per Article 259 of the Code of Criminal Procedure.

[181] Article 31 of the Law of the Republic of Belarus № 307-3 of 15 July 2015 'On Operational Search Activities', Article 214 of the Code of Criminal Procedure (Monitoring and Recording Communications), Presidential Decree № 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 № 45-3 of 19 July 2005 'On Telecommunications'.

[182] Law of Georgia on Operative-Investigative Activities, Articles 4 (Legal grounds) and 7 (Measures).

[183] Although the response to the question stated "there are no rules for interception of internet data and/or call content ('legal interception')," the response to the next question cited Article 132(8) of the Criminal Procedure Code № 122-XV, which provides a legal basis for interception and communication recording.

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

[185] PSRC regulation, license pre-condition: 'operator (ISP) has to cooperate with National Security Agency'.

[186] Article 39 of the Telecommunications Law.

[187] Criminal Procedure Code № 122-XV dated 14 March 2003, Cybercrime Law № 20-XVI dated 3 February 2009 and Law № 59 dated 29 March 2012 on Special Investigative Activity.

[188] The Telecommunications Law of Ukraine 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.

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Way of Legal Interception	Black Box[189]	*(no info)*	Black Box[191]	*(no info)*	*(no info)*[190]	*(no info)190*
Cost borne by	ISP	*(no info)*	ISP/LEA[191]	*(no info)*	ISP	ISP[192]

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 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 as 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 if they are obliged to monitor these.

Since, in the EU, 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 ISP 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 up to state actors to determine the legality of content, and, similarly, responses to such cases of illegal content (such as the takedown,

[189] A response later in the questionnaire indicated this.

[190] When asked, the country declined to provide information on how interception is performed in practice.

[191] The operator carries out on its own expense and from other sources not prohibited by law, acquisition, installation, maintenance and repair of a 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 OAC (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, № 129). KGB and OAC, 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 OAC (p.11 of the Regulation).

[192] Procedure for covering expenses is not legislatively determined, in practice it is at the ISP's expense.

making inaccessible, or deletion of material or blocking of access) are mandated by competent authorities exclusively. The responses and updated findings can be summarized as follows:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
ISP liability for user content	None[193]	*No*	Upon notice by authority	*No (Law on Freedom of Expression)*	No specific regulation[194]	*No, with an exception*[195]
Basis for blocking/ takedown	Court order	*Authorities, followed by court order*	Request from authorities such as OAC	*Court order, order of Parliament*[109]	Unclear[196]	*Court order*[197]
Obligation to monitor	None	*No*	None, but must prevent drug trafficking	'For safety of consumer-transmitted info'[198]	None	*For (further) copyright*[199] *infringement*
Obligation to report illegal content	None; right to inform police	*(no info)*	In Criminal Procedure Code, and for 'resource owners'[200]	Obligation to respond to reports.[201]	For limited types of content, such as malware[202]	*Yes*[203]
ISP roles defined	No	*(no info)*	Partly (reporting regime)	No	No	No

[193] Based on Law on Electronic Communications as well as net neutrality requirements of the PSRC.

[194] Article 11 the Cybercrime Law provides that its violation attracts disciplinary, civil, administrative or criminal liability under the law. There is no mention of a regime governing third party content, however.

[195] Not as per Article 125(4) of the Telecommunications Law, barring specific cases provided for in the Law on Electronic Commerce.

[196] The Cybercrime Law does not mention a regime to take down content upon request of a national authority, however it is provided as a measure of international cooperation in Article 8(2) of the same law.

[197] Including specifically cases of CSAE, personal sanctions and copyright violations.

[198] Article 25 §3 of the Resolution on Electronic Communications.

[199] According to the Copyright Law, after such an infringement was identified and a takedown was ordered.

[200] Articles 166 and 170 of the Criminal Procedure Code oblige ISPs to report crimes via their infrastructure. Furthermore, according to paragraph 8 of the Decree of the President of '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.»*

[201] Article 25 §4 (e)-(g) oblige ISP to: *«ensure the operation of a transparent and effective mechanism for the consideration of consumers complaints in order to timely and legally solve (them); ensure the presence of a mechanism of restricted access to services intended for adults; respond to information received concerning the allocation of an inadmissible production and adopt appropriate measures to eliminate it.»*

[202] Article 7(1)b of the Cybercrime Law states that service providers must *«communicate to the competent authorities 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 (..) distributing information or rules of protection of the information system provided according to the status of the information or its degree of protection, (..) or other information crimes.»*

[203] 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 this to the competent authority.

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 such safeguards, and the adoption of the principle of proportionality, has been repeatedly recognised.[204] The requirements of national legislation, including legislation protecting the privacy of personal data, also need to be considered.

7.3.1 Confidentiality of subscriber identity and secrecy of communication

The original questionnaire requested information from the EAP 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 countries regarding the obligation on ISPs to protect their subscriber's identity. For this study, responses were verified and amended, as summarized in this table:

[204] 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.

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Protect Secrecy of Communication	Yes[205]	*Yes*[206]	Yes[207]	Yes[208]	Yes[209]	Yes[210]
Protect Subscriber Identity	Yes[211]	*Yes*[206]	Yes[212]	Yes[213]	Yes[214]	Yes[215]

Information was also collected on which agency is responsible for overseeing ISPs' obligation to protect the secrecy of communication and what enforcement measures are available to sanction ISPs for non-conformance. The findings are summarised in the following table:

[205] Article 49 of the Law on Electronic Communications (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.

[206] Article 38 of the Telecommunications Law.

[207] Article 54 of the Law on Telecommunications.

[208] Constitution of Georgia; Law 'On Protection of Personal Data'; the Law 'On Electronic Communications' Article 8(1) states: "Information on consumers of communications networks, as well as information transmitted through these networks, is secret and its protection guaranteed by the legislation of Georgia."

[209] Article 5 of the Electronic Communications Act 241-XVI of 15 November 2007.

[210] Article 7, 10 of the Law of Ukraine 'On Access to Public Information, Article 11 of the Law of Ukraine 'On Information' and Article 162 of the Criminal Procedure Code.

[211] Law on Electronic Communications, Article 49 (Privacy of Customer Information).

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

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

[214] Law on the Protection of Personal Data, № 133, 8 July 2011.

[215] Law of Ukraine 'On the Protection of Personal Data'. http://zakon.rada.gov.ua/laws/show/2297-17

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Overseeing Authority	*PSRC*[216]	*DDT*[217]	OAC, State Inspectorate[218]	DPA, GNCC[219]	ANRCETI[220]	Not defined[221]
Enforcement Measures	Administrative Sanctions[222]	*(no info)*	Administrative Sanctions[223]	Administrative Sanctions[224]	Civil Sanctions[225]	Administrative and Criminal Sanctions[226]

7.3.2 Lawful interception

The legal basis and practical aspects of lawful interception are discussed earlier in this report. This section examines the safeguards that are in place to protect customer confidentiality.

As mentioned in 4.3.3, and as further reported above, obligations on ISPs to provide the ability for interception to law enforcement agencies are frequently found in telecommunications legislation, or in licenses issued by public authorities. The right to communications privacy is often also subject of legislation and is usually safeguarded by countries in telecommunications legislation, the constitution, criminal procedure laws and case law. In certain cases, there are also specific requirements in telecommunications licensing regimes.

The original questionnaire requested information from EAP countries about what type of order is required to compel an ISP to facilitate legal interception of a subscriber's communication. This was further verified and amended as summarised in the following table:

[216] It is enforced by the PSRC in cooperation with law enforcement and personal data protection agencies.
[217] In October 2021, the Ministry of Digital Development and Transport (DDT) established two new regulatory authorities: the Information and Communication Technologies Agency and the Innovation and Digital Development Agency.
[218] 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 16 October 2009, № 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 for Telecommunications. If users are state organizations, the user databases that ISPs develop are cryptographically protected and licensed by the Operations and Analytisis Center of Belarus. Data integrity is controlled by the OAC as well.
[219] Office of the Personal Data Protection Inspector and the Georgian National Communication Commission.
[220] The original response contained a link to the website of the National Regulatory Agency for Electronic Communications and Information Technology of Moldova. http://en.anrceti.md/fileupload/1
[221] 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.
[222] 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, it may change, suspend, or request for judicial termination of a license.
[223] From delivery of an order, demand, fines up to suspension and withdrawal of license.
[224] Written warnings, followed by fines, followed by suspension or cancellation of authorization to operate. In 2020, a regime was introduced for appointing a special manager to a penalized company.
[225] A reference was made to the Civil Code of the Republic of Moldova, № 1107-XV, 6 June 2002.
[226] Administrative liability (penalties) are defined in parts 4 and 5 of Article 188-39 of the Code of Ukraine on Administrative Offences, and criminal liability in Article 182 (violation of privacy) of the Criminal Code.

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Order Required for Interception	Court Order, *warrant*[227]	*(no info)*[228]	Prosecutor Order[229]	*Court Order (after) OTA request*[230]	Prosecutor Order[231]	Court Order[232]

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 holding in place 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 with important indications of the responsible parties for crimes committed online, or through communications networks.

Data retention concerns so-called metadata, which includes traffic and location data, meaning information pertaining to the origin and destination of communications, location of the terminal equipment and not the content transmitted. In practice, the level of detail of such information that is recorded depends on the provider, cooperation levels and parameterization of networks. 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

[227] In 2020, the legal framework was expanded to allow LEA to seek and obtain a warrant to tap phones.

[228] However, Article 38 of the Law on Telecommunications clarifies that interception is permitted only if provided by legislation.

[229] 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.

[230] Although in the original study no response was recorded, in 2022 the Law on Information Security was amended to allow the Operational-Technical Agency to access ISPs' infrastructure after a court order. Furthermore, the agency may request content data in real-time, as was found in the CoE's 2020 *Regional Study on Personal Data Protection aspects of law enforcement action on cybercrime in the EAP region.*

[231] The prosecutor serves warrants for interception, as mandated in the Criminal Procedure Code № 122-XV, 14 March 2003 (Article 132 – Performing and certifying interception and recording of communications).

[232] Determination of the investigating judge as made on the proposal of the investigating prosecutor.

through the network. Although, in Europe, in many countries mandatory data retention schemes have been dropped, the regime is still widely used. However, there is a widespread practice to differentiate retention times of such data in relation to internet data networks as opposed to voice networks or phone services. This differentiation is usually motivated by both volume and costs involved, as well as privacy considerations.

The relevant data retention regimes in the EAP region can be analysed according to the responses of the questionnaire, with their updates and amendments by this study, as follows:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Legal basis of data retention	PSRC regulation (voice) and MOU (data, voluntary)	*(no info)*	Decrees & Resolutions[233]	*(no info)*	Law[234]	Law
Retention period (voice/phone)	2 years	*(no info)*	5 years	*(no info)*	180/90 days[235]	3 years
Retention period (internet data)	Voluntary (MOU)	*(no info)*	5 years	*(no info)*	180/90 days[235]	3 years
Definition of traffic data (internet)	Yes	*(no info)*	No[236]	*(no info)*	Yes[237]	No

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

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 such regulators a certain independence in assessing the needs of society and in safeguarding the various interests at stake, where the telecommunications infrastructure is concerned.

Regulatory authorities in the EAP region all have different tasks, and their responsibility in relation to data access for law enforcement, as well as their role in relation to legal interception

[233] Decree on Interaction with Bodies that carry out Operational Search Activity (2010); Decree on Urgent Measures to Counter Illicit Drug Trafficking (2014); Resolution on Storage of Data about Resources visited by Internet Users (2015).

[234] Cybercrime Law, Article 7.

[235] Traffic data: 180 days, relevant decryption keys: 90 days.

[236] 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 numbers, data allowing to identify the subscriber or his terminal, and for subscribers of the cellular mobile network also the details of the identity document (its name, series, number, date of issue and the issuing body of state).

[237] According to the Council of Europe International Cooperation Website (2017).

and privacy protection is varied, especially with the advent of specialized Data Protection Authorities. In practice, telecommunications regulators and agencies have different mandates.

The questionnaire related to this study originally asked about the tasks fulfilled by these authorities, which was amended in 2022. In short, their roles can be summarized as follows:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Separate regulator	PSRC	*Agencies of the DDT*[238]	No[239]	GNCC	ANRCETI	NCCIR
Access to data	Yes	*(no info)*	LEA & OAC	No (OTA)	Yes	No
Interception of content	License condition	*(no info)*	KGB & OAC	No (OTA)	Yes (also GPO/police)	No
Privacy and consumer rights	Yes (consumer protection)	*Yes*[240]	Ministry of Communi-cations, OAC	Yes	Yes	Yes
Cyber security strategy	Yes	*Yes*[241]	Yes	Yes	*Yes*[242]	*Yes*[243]

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.***

[238] In October 2021, the Ministry of Digital Development and Transport (DDT) established two new regulatory authorities: the Information and Communication Technologies Agency and the Innovation and Digital Development Agency.

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

[240] Enumerated in the Telecommunications Law.

[241] Strategic Roadmap.

[242] National Cyber Security Strategy for 2019-2024 and its Action Plan, as adopted by Parliament in 2018.

[243] Cyber Security Strategy of Ukraine (2021-2025) as approved by the National Coordination Center for Cyber Security in 2021, and its Implementation Plan, as adopted in 2022 by the President.

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 or 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;
- Content related to terrorist crimes.

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 and the related desk research, 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 to Monitor	No	*(no info)*	*Partial*[244]	*Partial*[245]	Yes[246]	Partial[247]
Obligation to Report	No[248]	*Partial*[249]	Yes[250]	No[251]	Yes[252]	*Yes*[253]

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

[244] Provided for in a number of cases, such as the prevention of illicit drug trafficking, supported by paragraph 4 of Article 22.16 of the Administrative Code of the Republic of Belarus. Also, according to paragraph 12 of Presidential Decree № 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 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.»*

[245] If an ISP is informed of illegal content, it must be removed. Additionally, they must adopt measures to prevent the misuse of their network for intimidation or insulting of customers.

[246] Provided for in Article 7(1)(b) of the Cybercrime Law of 3 February 2009: *«Service providers are required 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, or other computer crimes.»*

[247] Article 52(1) and 52(3) of the Law of Ukraine 'on copyright and neighboring rights' specify the duty of the hosting provider and the website owner to prevent and stop violations of copyright and related rights.

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

[249] There is a general obligation to report serious crimes, besides that, there is a facultative right to report.

[250] According to Paragraph 8 of the Decree № 6 of 28 December 'On Urgent Measures to Counter Illicit Drug Trafficking', owners of internet resources are required 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 to inform the internal affairs bodies of attempts to use their information resources to disseminate messages and/or materials aimed at illicit drug trafficking.»*

[251] The Georgia law 'On Electronic Communications' and Resolution № 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 GNCC of detected illegal content. However, if such a fact is revealed, the ISP must remove the content.

[252] Article 5 of the Cybercrime Law of 3 February states 2009 that *«in the framework of cybercrime prevention and fighting activities, the competent authorities, service providers, non-governmental organizations and other civil society representatives cooperate through information exchange, experts, joint investigation of cases and identification of offenders, training of personnel, initiatives to promote programmes, practices, measures, procedures and minimum standards for the security of information systems, cybercrime and risk information campaigns to users of computer systems, and other activities.»* Furthermore, Article 7 of the same law requires ISPs to report certain violations to competent authorities.

[253] General legislative provisions oblige an ISP to report a crime through its infrastructure to the authorities. In 2019, an obligation to report online bullying was introduced in the Administrative Code of Offences.

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 identifying the correct ISP/hosting company is exacerbated if content is held outside of the jurisdiction. Involvement in international cooperation initiatives such as INHOPE[254] can be helpful in such cases.

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 CSAE, viruses, hate speech, botnets and removal of illegal content from ISP services. In 2022, we also verified whether the EAP countries were members to Europol's international NoMoreRansom.org network.[39] The results are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Cooperation Agreements	No	*(no info)*	Yes[255]	*(no info)*	*(no info)*	No
No More Ransom.org	No	No	No	No	No	Yes

Finally, the questionnaire requested information on the mechanisms available to the participant countries to facilitate takedown of illegal content. The responses, with amendments as found during the subsequent desk research in 2017 and 2022, are summarised in the following table:

[254] https://www.inhope.org/EN/articles/who-we-are

[255] Paragraph 8 of Presidential Decree № 60 of 1 February 2010 'On Measures on Improving Use of the National Segment of the Internet'; Resolution of the Operations and Analysis Center under the President of Belarus № 4/11 of 29 June 2010; Presidential Decree № 6 of 28 December 2014.

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Illegal Content Takedown Requirement	Court Order	*Authorities, followed by court order*	*Authorities or at own request*[256]	Court Order, *Parliament Order*[109]	Court Order	Court Order, *Sanction*[257]
Fast Takedown Possible	Yes[258]	*(no info)*	Yes[259]	*(no info)*	*(no info)*	Partial[260]

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 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 for countermeasures to prevent fraud or financial damage

According to our Cyber Barometers implemented in 2021 and 2022, becoming a victim of fraud is a major concern to EAP citizens. 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 a consequence 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 original questionnaire requested information from the participant countries on whether ISPs are required to put in place measures for fraud prevention, or to counteract financial damage through the ISP infrastructure. The responses are summarised in the following table:

[256] 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.

[257] Personal sanctions apply not only to users but can also be directed at owners of online resources.

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

[259] In compliance with §12 of Resolution of the Operations and Analysis Center and Ministry of Communication and Informatization № 4/11 of 29 June 2010 on Adoption of the Statute Regulating 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' (RUE 'BelGIE') according to decisions of management of the Committee for State Control, Prosecutor General's Office, OAC and other 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: 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 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.*»

[260] Articles 52(1), 52(2) of the Law of Ukraine 'On Copyright and Neighboring Rights'.

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Obligation to Prevent Fraud or Financial Damage	No obligation	*(no info)*	In some cases[261]	In some cases[262]	*(no info)*	*(no info)*

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.***

7.6.3 Information sharing about ongoing threats or incidents

Where an ISP finds itself the target of a particular attack, or identifies a vulnerability that exposes its operations to attack or failure, there are advantages to sharing this information with other ISPs so that they can assess their exposure to a similar attack or vulnerability. This important type of information sharing can expedite the 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) have an important role to play here, but alternatives such as informal ISP Fraud and Security Forums, Information Sharing and Analysis Centres (ISACs) or bilateral communication can also be helpful where a national CERT is not fully operational, or the incident falls out of scope of the responsibilities of that CERT.

It can also be helpful in such informal Fraud and Security Forums or ISACs to involve law enforcement agencies, if they have a (cyber)crime prevention role, in a collaborative fashion.

By setting up regular meetings, properly configured communications channels and procedures, and perhaps joint exercises, trust and rapport can be built between key players pre-emptively. This will enhance the expedience and efficacy of this voluntary network should the need arise.

The questionnaire asked whether ISPs share information with each other about ongoing threats of incidents. It also requested information on 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 requested on whether ISPs making reports of various types (e.g., data breaches, security incidents, crimes) are provided with feedback (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:

[261] For those ISPs that provide services to state agencies, a range of normative and legal acts as developed by the Operations and Analysis Center is applicable, among which are (a) Presidential Decree № 196 of 16 April 2013 on 'Some Measures How to Improve Information Protection' and (b) Order of the OAC № 82 of 16 November 2010 on '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'.

[262] In respect to international call terminations, ISPs have particular obligations regarding financial fraud prevention, as imposed though a decision by the GNCC.

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Information Sharing	Informal[263]	*(no info)*	*(no info)*[264]	Informal[265]	*(no info)*	*(no info)*
Information sharing platform	Informal CERT[266]	*National CERT*[267]	National CERT[268]	*National CERT and civil CERT*[269]	*Government CERT and civil CERT*[270]	*National CERT*[271]
Feedback provided	No	*(no info)*	Yes[272]	*(no info)*	*(no info)*[273]	*Indirectly*[274]

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 ongoing threats or incidents. In some countries, in parallel with the EU's NIS Directive, there may be obligations to report such incidents to national CERTs, but when 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 can help them to provide better reports in future. It is therefore recommended that countries consider adopting a practice of providing feedback to reporting entities with whom ongoing relationships are expected, so that those entities can provide better reports in future if necessary.***

[263] Informally, each ISP has an address for reporting (i.e., abuse@isp.am).

[264] 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 about whether ISPs share information with each other about ongoing threats or incidents.

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

[266] Informally there is the non-governmental CERT-AM, which provides current information about incidents.

[267] CERT-AZ has been established under the Cyber Security Service and is identified in the Cyber Barometer of Azerbaijan as a popular agency to report cyber incidents to.

[268] 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, CERT-BY, has a website where an individual or legal entity can make a report.

[269] The National CERT is CERT-GOV-GE, whereas the Georgian Research and Educational Networking Association (GRENA) maintains CERT.GE since 2007, catering to educational institutions, non-profits, etc.

[270] In response to this question in the questionnaire a list of reporting points was provided, which did not provide information about whether there is an information sharing platform available. However, later desk research found that Moldova has two CERTs operating on a national scale: MD-CERT handles incidents in the research and education network since 2007, whereas CERT-GOV-MD has the responsibility for handling information security incidents and offering cyber security services to public administration authorities.

[271] CERT-UA has been established as Ukraine's national CERT and, according to the Cyber Barometer of Ukraine, it is well-known by IT and ISP professionals as a major source of cyber threat information.

[272] In compliance with Law of the Republic of Belarus № 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.

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

[274] As reported in the Cyber Barometer for Ukraine, CERT-UA is a major source of cyber threat information.

Recommendation 24: ***Technological platforms are available to assist with confidential or anonymized information sharing about ongoing 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

Increasing awareness is the foremost common recommendation in the EAP Cyber Barometers. 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 the requests received and so on. State agencies in turn can provide information to ISPs on changes to their regulatory regimes, requirements for information retention and so on.

The format of awareness initiatives can be wide-ranging, from ISP involvement in police or judicial training events to law enforcement involvement in private security conferences.

The original questionnaire sent out to the EAP countries requested information about whether either ISPs provide awareness information to state agencies and/or state agencies provide awareness information to ISPs. The responses are summarised in the following table:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
wareness Training Programmes	No such practice	*(no info)*	Yes[275]	*(no info)*	Yes[276]	*(no info)*

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 together to raise each other's awareness of the other's perspective in an appropriate forum.***

[275] Participation in joint conferences, including IT Security Conference that is positioned as a negotiation platform for private companies, state companies and LEA on discussion of issues of cybercrime.

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