Policy brief:
MOBILE SURVEILLANCE: ARMENIA, GEORGIA, AND UKRAINE

European standards

Surveillance measures are necessary for a proper investigation and prosecution of serious crimes and the protection of national security by means of intelligence. At the same time, surveillance measures mean the intrusion in a very intimate part of our lives – personal communications. Establishing a fair balance between security and freedoms while avoiding abuses of power lie at the core of preservation of the rights for privacy and freedom of expression.

Article 8 of the European Convention on Human Rights provides for the protection of the right to respect private and family life, home and correspondence. The interference is legitimate only if:

- It is in accordance with the law.
- It pursues a legitimate purpose, *i.e.* the interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or for the protection of the rights and freedoms of others.
- It is necessary in a democratic society.

The European Court of Human Rights (hereinafter – ECtHR) decides the surveillance-related cases, indicating that democratic societies are threatened by highly sophisticated forms of espionage and terrorism, needing means to defend themselves against such threats. Typical tension with regard to surveillance measures relates to the issue of the lawfulness of bulk (mass) surveillance compared to a targeted one. For the latter measures the ECtHR developed the minimum requirements that should be set out in law to avoid abuses of power:

1. the nature of offences which may give rise to an interception order;
2. the categories of people liable to have their communications intercepted;
3. a limited duration of interception;
4. the procedure to be followed for examining, using and storing the data obtained;
5. the precautions to be taken when communicating the data or other parties;
6. the circumstances in which intercepted data may or must be erased or destroyed;
7. arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and remedies provided by law.[1]

The ECtHR accepted that the nature of modern threats pushes governments to resort to cutting-edge technologies, including massive monitoring of communications,[2] which should be balanced by proper legal safeguards. The Court sets slightly different standard for bulk interception, commonly used by foreign intelligence gathering, the early detection and investigation of cyberattacks, counter-espionage and counter-terrorism. Standards 3-6 mentioned above are relevant for bulk surveillance with the process subjected to "end-to-end safeguards", meaning that:

- an assessment of the necessity and proportionality should be made at each stage of the process;
- requesting authority should identify the types or categories of selectors (search criteria);
- bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and
- the operation should be subject to supervision and independent *ex post facto* review.

[1] ECtHR, Big Brother Watch v. the UK, para. 335

[2] ECtHR, Szabo and Vissy v. Hungary, para. 68; [GC] ECHtR, Big Brother Watch v. the UK, para. 323

To facilitate the supervision, detailed records should be kept by the responsible agencies at each stage of the process. In terms of availability of effective remedy, it is either the subsequent notification of surveillance measures for the targeted interception or availability of judicial review at any moment of suspected surveillance measures.[3]

Lastly, the international transfer of data should be regulated by national law. The country should put in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material, restrict its onward disclosure and should also be subject to independent control.

Mobile Surveillance in Armenia, Georgia and Ukraine

Mobile devices serve as a universal tool of surveillance since our daily lives became closely intertwined with this type of communication.[4] Nowadays, messengers dominate interpersonal communications and have a very acute influence on digital rights. Our devices leave very different information available to bodies having access to the communication networks. It can be wiretapping, or more sophisticated means of spyware, or large-scale use of the data about communications (metadata).

Armenia, Georgia and Ukraine have implemented the above-mentioned standards with regard to surveillance measures and have their similarities and differences in general legal framework and practice. For all countries the general nature of offences giving grounds to use surveillance tools includes grave or particularly grave crimes. Peculiar development, in this regard, happened recently in Georgia – the scope of covered crimes was substantially extended, which endangers rights of Georgians.

It is relevant for all three countries that a reasonable suspicion that a particular person has committed or is connected with a certain grave or particularly grave crime is required for launching the surveillance measures. Special protection is afforded to journalists' sources, religious communications and conversations between client and his lawyer. For every country it was challenging to secure the necessary level of protection for these categories of people.

- In Ukraine, a number of cases indicated that current mechanisms protecting journalists' sources are insufficient and courts failed to properly balance the public interest against protection of confidentiality of sources. Additionally, problem of timely notification became more visible in the context of those cases.
- In Georgia, the symptoms of serious problems are revealed with massive leaks of personal data of clerical leaders, journalists and foreign diplomats.
- In Armenia, cases of the use of spyware against local politicians and lawyers show the new dimension of the risks of illegal surveillance.

The issue of duration of surveillance measures was important point of discussion of recent legislative changes in Georgia. Power to extend the surveillance measures as long as needed during investigation is condemned by both civil society and Venice Commission.[5] A similar case, basically, takes place in Ukraine, whereas in Armenia the maximum duration is 12 months.

---

[3] ECtHR, Roman Zakharov case, para. 234

[4] Annual 2021 Report of Electronic Communications Regulator: https://nkrzi.gov.ua/images/upload/142/10078/report-12-05-2022_for_print_ToPrint.pdf

[5] Venice Commission, Urgent opinion on the Draft Law on the Amendments to the Criminal Procedure Code adopted by the Parliament of Georgia on 7 June 2022, issued on 26 August 2022 pursuant to Article 14a of the Venice Commission's Rules of Procedure, 26 of August, 2022, available at: https://bit.ly/3DqZ8Pu

Aspects of using, storing and destroying data collected by means of surveillance are generally similar across countries. Prosecutors play a crucial role in securing the legality of the measures. Lawfully collected information can be used during the trial as evidence. Data that is irrelevant for investigation shall be destroyed under prosecutor's control and shall not be spread before the destruction. It should be impossible to recreate destructed information. Destruction shall be carried out in a specially equipped room and duly protocoled.

After the end of the investigation people have a right to know about interference with their right to privacy via the notification by the responsible agencies. As a rule, definite moment of subsequent notification may depend on achievement of investigation goals, security environment, threats to health and life of engaged persons. It has to be stressed that timely notification to the person concerned is a necessary condition for the effective use of remedies against surveillance measures. As follows from the case-law of the ECtHR, notification is not an absolute requirement; narrow exceptions are possible provided that a state has a general complaints procedure to an independent oversight body with adequate powers and scope of review. None of three counties have such mechanism available.

Judicial control constitutes a basis for the oversight of surveillance measures in all covered countries. However, in practice it may be insufficient, as highlighted by Venice Commission for Georgia – courts do not have enough time to review requests for surveillance measures; the judges lack technical expertise with regard to proposed technologies and experience a very high workload, leading to the high approval rate of motions for covert measures.

Moreover, in Ukraine and Georgia, authorized bodies have autonomous access to communication networks that warrant stronger safeguards against abuse and, unfortunately, judicial review, as provided at the moment, proves to be insufficient.

Parliamentary control in all countries is quite nominal and focuses on rather general review of periodical reports than oversight over the specific cases with the subsequent amendments of legislation.

To enhance the human rights protection framework in the surveillance sphere, **all three countries** should take into account the following recommendations:

1. obligatory judicial review of surveillance measures should be supported by stronger safeguards, such as an independent review mechanism, *i.e.*, including an expert oversight body, which should:
    - have unlimited access to any type of data intercepted, grounds for conducting such interception and details on the fate of the collected data;
    - be independent and supplemented by the necessary financial, logistical and expert resources to meaningfully address the surveillance issues;
    - guarantee that individuals would get an access to justice by means of timely notification.
2. develop better tools to protect journalistic sources, including better training for both prosecutors and judges;
3. work out the procedural guarantees on the extension of surveillance measures, which ensure that it is justified and not excessive;
4. properly address new challenges of spyware and platforms, ensuring compliance of new surveillance forms with the mechanisms provided by the future EU Media Freedom Act and the Second Protocol of Budapest Convention.

UKRAINE

Mobile devices serve as a universal tool of surveillance since our daily lives became closely intertwined with this type of communication.[6] Messengers dominate interpersonal communications and have a very acute influence on digital rights. Our devices leave very different information available to bodies having access to the communication networks. It can be wiretapping, or more sophisticated means of spyware, or large-scale use of the data about communications (metadata). Thus, we review laws and relevant cases connected with mobile surveillance covering direct access to conversations and metadata in Ukraine.

The Criminal Procedure Code of Ukraine (hereinafter – CPCU) serves as core legislation authorizing surveillance. Criminal procedure laws allow the interception of communications only:

- upon court's authorization;
- in case of investigation of **grave and particularly grave crimes;** *and*
- it is **exceptional** according to law and satisfies procedural requirements of the CPCU.[7]

Surveillance investigative powers are channeled to numerous agencies:

- National Police;
- Security Service of Ukraine;
- National Anti-corruption Bureau;
- State Bureau of Investigation (deals with the crimes committed by high-ranking officials – (except covered by National Anti-Corruption Bureau), by officials of the National Anti-Corruption Bureau of Ukraine and Specialized Anti-Corruption Prosecutor's Office, by persons, who have committed war crimes);
- Economic Security Bureau;
- State Criminal Enforcement Service.[8]

Since 2022 all mentioned agencies have autonomous access to the necessary communication networks and operators are to facilitate such access.[9] Autonomous access means that every authorized body has direct access to the networks (without the knowledge of operators), but the necessary judicial approval is nevertheless required.[10]

Older draft law №4004 could have enabled the very same access, but electronic communications operators were to bear the costs of setting up the surveillance equipment enabling autonomous access. Additionally, this draft law could widen the scope of data retention.[11] The ECtHR emphasized that a surveillance system designed in such fashion is more prone to abuse and should be balanced by stronger safeguards.[12]

Appeal courts or High Anti-corruption Court deal with authorization of surveillance measures. However, in exceptional circumstances such as threat to human life, those agencies are allowed to wiretap the mobile devices without court authorization. Nevertheless, these agencies have to confirm the legality of surveillance

---

[6] Annual 2021 Report of Electronic Communications Regulator: https://nkrzi.gov.ua/images/upload/142/10078/report-12-05-2022_for_print_ToPrint.pdf

[7] Article 246 of the Criminal Procedure Code of Ukraine

[8] Ibid.

[9] Article 121 of the Law of Ukraine on Electronic Communications

[10] Order of the SSU and State Service of Special Communications and Information Protection №460/781 on technical means to conduct operative-search, counter-intelligence, intelligence and investigative surveillance measures by authorized bodies in general electronic communications networks. General Technical Requirements: https://ssu.gov.ua/uploads/documents/2022/01/24/ztv-31122021.pdf

[11] Draft law №4004 on increasing the effectiveness of cybercrime combatting and electronic evidence: https://itd.rada.gov.ua/billInfo/Bills/Card/3765

[12] ECtHR, Roman Zakharov case, para. 270

measures in court within 24 hours. The Court's refusal to acknowledge those surveillance measures as legal leads to destruction of evidence.[13]

Process is rather short – court grants or refuses an access to communications within 6 hours after submission. The CPCU contains detailed requirements to such requests including ones that are aimed at guaranteeing the "last resort" character of surveillance measures.

As a rule, surveillance measures should not exceed 2 months in time but investigating authorities are practically capable of prolonging them as long as needed for the serious crime investigation – up to 18 months.[14]

Prosecutor plays a crucial role in securing the legality of the measures. Upon his reasoned decision, the surveillance measure might not be authorized.[15] The whole process of surveillance measures is protocoled and within 24 hours is reported back to prosecutor without confidential personal data.[16] Lawfully collected information can be used during the trial as evidence. Data that is irrelevant for investigation shall be destroyed under prosecutor's control and shall not be spread before the destruction. It should be impossible to recreate destructed information. Destruction is carried out in specially equipped room and is duly protocoled.

The CPCU provides for the protection of the information obtained as a result of surveillance measures, including criminal liability for disclosure of the data.[17] After the end of the investigation people have a right to know about interference with their right to privacy with notification by law enforcement agencies done no later than 12 months after the suspension of surveillance (including accidental gathering) or submission of appeal to the court by prosecutor.[18] Definite moment of subsequent notification may depend on achievement of investigation goals, security environment, threats to health and life of engaged persons.

Despite the overall availability of numerous safeguards against abuses, in practice there are many challenges to fully enjoy constitutional rights. Namely, cases of abuse of surveillance powers happen at different levels, they are investigated and some of them reach the courts. For instance, anti-corruption bodies bring the cases connected with bribery,[19] state prosecutes national police employees,[20] some of such cases were submitted quite recently.[21]

Journalists' rights. Some cases become very high-profile since they are connected with the work of investigative journalists and their attempts to spotlight serious corruption. However, law enforcement agencies often prefer using the framework for the communication data instead of wiretapping since operators are obliged to retain it for at least 3 years, providing more flexibility.

The National Anti-corruption Bureau published materials hinting that judges of the Kyiv Administrative Court tried to get access to communications data[22] of the journalist that investigated their activities. The state expressed deep concern over the potential abuses on the side of the judges on the Platform for the Protection of Journalism and Safety of Journalists[23] and promised to take all actions necessary, however eventually the case ended up nowhere so far.[24]

---

[13] Article 247 of the Criminal Procedure Code of Ukraine
[14] Article 248-249 of the Criminal Procedure Code of Ukraine
[15] Articles 110, 246, 249 of the Criminal Procedure Code of Ukraine
[16] Instruction on surveillance measures for criminal proceedings: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text
[17] Article 254 of the Criminal Procedure Code of Ukraine
[18] Article 253 of the Criminal Procedure Code of Ukraine
[19] https://suspilne.media/58273-spivrobitnika-sbu-suditimut-za-nezakonne-prosluhovuvanna/
[20] https://umoloda.kyiv.ua/number/0/2006/156191/
[21] https://www.gp.gov.ua/ua/posts/prosluxovuvannya-ta-nezakonne-stezennya-posadovcyu-stolicnogo-glavku-policiyi-povidomleno-pro-pidozru and https://dbr.gov.ua/news/organizovuvali_nezakonne_prosluhovuvannya_telefonnih_dzvinkiv_gromadyan_na_zamovlennya__slidcha_policii_na_lvivschini_postane_pered_sudom
[22] https://www.slidstvo.info/news/mediaspilnota-zaklykala-rozsliduvaty-sproby-suddiv-oasku-otrymaty-dostup-do-trafikiv-zhurnalistky-slidstva-info/
[23] https://rm.coe.int/ukraine-en-reply-judges-illegally-tried-to-gain-access-to-a-ukrainian-/1680a056a7
[24] https://helsinki.org.ua/articles/yak-aktyvistam-reahuvaty-na-tskuvannia-v-sotsmerezhakh/

One of the cases touched upon the threat to the freedom of expression and journalists' sources. The case that eventually ended in the ECtHR relates to the access to mobile communication data, namely location at the moment of calls within the identified period, of the prominent investigative journalist *Ms Sedletska*.[25] The ECtHR found a violation of the journalist's right to freedom of expression under Article 10 of the ECHR. Major deficiencies concerned the:

- lack of due reasoning on disclosure of the journalists' sources;
- unjustified and disproportionate access to communications for too long period (16 month);
- lack of procedural safeguards regarding timely notification on surveillance measures.

Back in July 2022 the Ministry of Justice explained measures taken to comply with the Court's decision in *Sedletska* case.[26] The Ministry referred to the Action Plan submitted to the Council of Europe Committee of Ministers in March 2022.[27] In the Action Plan the Ministry responded that the issue of potential legislative changes requires further assessment and anchored these promises in the Information Security Strategy. Basically, the Ministry relies on various types of training on protection of journalists' sources for both judges and prosecutors.

Quarantine applications. At the outset of the pandemic crisis Ukrainian authorities launched an app called "Diy.Vdoma" that aimed at ensuring compliance with self-isolation for people coming back to Ukraine from other countries.[28] This app collected a vast amount of sensitive data including geolocation, person's photos and health data that was transferred to various state bodies, including law enforcement. Eventually, the architecture around this app created substantial risks of abuse due to the abundance of sensitive data collected, lack of transparency, and concerns over its security.[29] Despite the added safeguards on anonymization and destruction of data in 30 days after self-isolation, the framework law[30] still allows for maintaining all the data for 30 days after the end of quarantine which is in place.[31]

Registration of SIM cards. In August 2021 parliament's digital transformation committee proposed a draft law on obligatory registration of SIM cards.[32] It might have constituted a serious blow to anonymity of communications and requires additional safeguards, as provided by the ECtHR in *Breyer* case.[33] However, as of October 2022 this draft law remains was not submitted to the parliament. No restrictions or initiatives undermining encryption technologies are observed.

Intelligence powers and security services. When it comes to investigation of crimes, Security Service of Ukraine has to follow the provisions of the CPCU mentioned above. The powers with regard to counter-intelligence activities are limited by judicial review.

Numerous attempts to reform the Security Service of Ukraine and intelligence services prove to be one of the most contentious issues for digital rights and mobile surveillance. For instance, a year ago the complex draft law[34] on the Security Service of Ukraine was very high on the agenda and widely supported by the G7.[35] In terms of digital rights this draft law posed numerous challenges – it substantially expands the SSU's powers and gives it extrajudicial access to communication data, including fact of communication, its length, routes.

---

[25] https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-208882%22%5D%7D
[26] https://rm.coe.int/0900001680a76632
[27] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680a5d6d4
[28] https://www.kmu.gov.ua/news/yak-pracyuye-zastosunok-dij-vdoma
[29] https://instingov.org/wp-content/uploads/2021/10/Report_ukarine-ukr-.pdf
[30] Law of Ukraine on protection against Covid-19: https://zakon.rada.gov.ua/laws/show/555-20#Text
[31] https://www.slovoidilo.ua/2022/08/19/novyna/suspilstvo/karantyn-ukrayini-prodovzhyly-kincya-hrudnya
[32] https://komit.rada.gov.ua/news/main_news/73970.html
[33] ECtHR, Breyer v. Germany, para. 83
[34] Draft law 3196-d on Security Service of Ukraine: https://itd.rada.gov.ua/billInfo/Bills/Card/4441
[35] https://www.radiosvoboda.org/a/news-posly-krain-g7-zakonoproiekt-sbu/31551035.html

While martial law is in action, the parliament strives to empower the agency in terms of counter-intelligence activities. Draft law №7684-d was submitted in the beginning of December 2022[36] and does not bring many changes in terms of surveillance measures. It provides for strict grounds for opening and closure of counter-intelligence cases, including spying, terrorist and subversive activities and other aims described in detail in Articles 6 and 8. This draft law provides for slightly longer timespan for urgent measures – 72 hours to subsequent court authorization. Respective measures are to be limited by 6 months. Other standards quite resemble ones provided by the CPCU.

The adoption of the Law on Intelligence in 2020 brought more clarity in terms of the role of the intelligence community in surveillance.[37] As a rule, any surveillance measure for intelligence purposes requires court authorization. In this case people are entitled equally to know that their rights were restricted and to challenge it in court. However, such disclosure is subject to completion of intelligence measures and to national security interests which was described by some non-governmental organizations as violating constitutional rights, not complying with quality of law demands being too vague.[38]

Intelligence bodies toolkit covers also investigative measures when it comes to combating terrorism and international crime networks, preventing subversive activities and other external threats. This implies the actual effects of criminal procedure legislation mentioned above. Intelligence agencies also have autonomous access to the communication networks.

After 24 February 2022 some members of parliament pushed for the drastic changes in laws regarding the intelligence community. However, only a couple of provisions have an impact on surveillance powers with the main challenge being the inconsistencies with criminal procedure laws and the lack of safeguards.

Martial law limitations. On February 24th Ukraine introduced martial laws due to the military aggression of the Russian Federation. Ukraine explicitly mentioned that it reserves the right to limit conventional rights, like the right to privacy and freedom of expression.[39]

The military aggression and, consequently, introduction of the martial law induced changes to laws regarding criminal process into the direction of simplified access to communications by prosecutors.[40] For the duration of the martial law, the prosecutor's order would be sufficient to get access to metadata.

The main challenge for mobile communications is that such simplified access opportunities provision is not bound by the martial laws and the doors for various simplified procedures are to remain. As we could see in cases regarding journalists, this instrument is particularly popular among law enforcement agencies. Despite such broadened powers those agencies still keep asking the court for permission to get access to such data and the instrument remains rather widespread.[41]

Russian surveillance techniques. Full-scale war brought very tangible risks of mobile surveillance. For instance, re-routing of traffic via Russian territory[42] bears substantial risks of bulk surveillance and physical risks for those remaining on those territories. Russia previously used a similar playbook in the occupied Crimea.[43]

Russia is requiring Ukrainians there to show a passport to buy a SIM card with a Russian phone number that makes it easier for Russian troops to keep tabs on people with their mobile devices, including location and internet browsing.

---

[36] Draft law 7684-d on improvement of counter-intelligence activities and capacity building to fight the military aggression against Ukraine: https://itd.rada.gov.ua/billInfo/Bills/Card/40931

[37] Law of Ukraine on Intelligence: https://zakon.rada.gov.ua/laws/show/912-20#n58

[38] https://acrec.org.ua/news/hromadians-ke-suspil-stvo-vymahaie-naklasty-pravo-veto-ta-povernuty-na-povtornyy-rozghliad-do-verkhovnoi-rady-ukrainy-zakon-pro-rozvidku/

[39] https://treaties.un.org/doc/Publication/CN/2022/CN.65.2022-Eng.pdf

[40] https://dslua.org/publications/yak-zakonodavchi-zminy-shchodo-rozsliduvannia-zlochyniv-vplynut-na-vashu-pryvatnist/

[41] https://texty.org.ua/d/cell_towers/

[42] https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02/

[43] https://hal.archives-ouvertes.fr/hal-03100247

Separately, the Russian side spread disinformation about the constant monitoring of private communications via social media and messengers.[44] This campaign was debunked and Ukrainians were provided with information about safer ways of communication even on temporarily occupied territories.[45] For instance, the use of VPNs and particular messengers (like Signal or WhatsApp) are recommended and some other – discouraged (Telegram).[46] The government is providing free access to certain VPN services[47] to help people in those areas connect to the global Internet.[48]

Ukrainian security forces occasionally publish interceptions of conversations made by Russian armed forces often revealing their acknowledgement of committed war crimes.[49] While martial law is applied, intelligence community authorities are allowed to conduct surveillance without court authorization on temporarily occupied territories.

Spyware. Worldwide trend of spyware spread has hit the Ukrainian agenda too. Israel has allegedly blocked the purchase of Pegasus by Ukraine.[50] There are no confirmed cases of the use of this spyware in Ukraine; however, Ukrainian authorities should be also vigilant about this trend, what kind of risks its deployment carries and how to regulate it.

In conclusion, Ukraine has a rather robust basic framework authorizing the surveillance measures. However, the main challenges to digital rights remain at the enforcement stage that cases against major investigative journalists prove. Firstly, more detailed procedure on separation of accidentally gathered information, its isolation and destruction are necessary. Secondly, better training for both prosecutors and judges may partially contribute to improvement in guaranteeing digital rights.

Stronger safeguards are essential to protect the digital rights of Ukrainians. Sooner or later some law enforcement and intelligence agencies will experience a further substantial transformation. In this process it is crucial not to miss on provision of procedural safeguards, including the right to know about the limitations of their rights. Judicial review of surveillance measures should remain the rule and legislative changes enabling prosecutors to get access to metadata shall not extend beyond the martial law time. Additionally, cases against journalists also proved that framework for subsequent notification and supervision over authorization of surveillance measures did not function well. It hints to the need to enable a proactive surveillance check mechanism against courts or other independent supervisory body. Recalling that both law enforcement and intelligence bodies have autonomous access to electronic communication networks, additional independent supervision mechanism would make sense.

International element of the surveillance measures seems to be lacking important tools stemming from Budapest Convention[51] and its newly adopted additional protocol.[52] Procedures for expedited preservation of computer data, expedited disclosure of stored computer data or emergency mutual assistance would empower law enforcement agencies with proper legal tools to investigate crimes.

Bearing in mind the new challenges of spyware, the Ukrainian government should take note of the recent European Media Freedom Act that provides for strict control over the deployment of spyware.[53]

---

[44] https://voxukraine.org/en/fake-all-calls-will-be-recorded-social-media-will-monitor-communication/

[45] https://www.facebook.com/100069034355657/posts/pfbid0FXQXJS8gp2GzCMtaish48aaC97MBfiXPB4xZk6NvnDNLiWmY5FjAdZF2N5Lm42bHl/

[46] https://internetua.com/yaki-mesendjeri-bezpecsni-a-yaki-ni-u-mincifri-dali-rekomendaciyi

[47] https://tech.liga.net/ua/ukraine/novosti/ukraintsy-na-vremenno-okkupirovannyh-territoriyah-mogut-besplatno-polzovatsya-vpn-cherez-diyu

[48] https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html

[49] https://www.npr.org/2022/04/26/1094656395/how-does-ukraine-keep-intercepting-russian-military-communications

[50] https://www.theguardian.com/world/2022/mar/23/israel-ukraine-pegasus-spyware-russia

[51] https://rm.coe.int/1680081561

[52] https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b

[53] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5504

GEORGIA

The Criminal Procedure Code of Georgia (CPCG) regulates the types of secret investigative measures, principles of their conduct, entities authorized to carry out the measures, the procedures of storing and processing obtained data, suspension and termination of investigative measures, the process of destroying obtained information and rules on providing subjects of the investigative measures with relevant information.[54]

According to the CPCG the covert wiretapping and recording of telephone communication may be carried out only when investigating a crime provided by the CPCG. They may be carried out only in respect of particular categories of crimes and if they are necessary to achieve a legitimate goal in a democratic society, in particular, to ensure national or public security, to prevent disorder or crime, to protect the country's economic interests and the rights and freedoms of other persons. Covert investigative measures may be conducted only when the evidence essential to the investigation cannot be obtained through other means or when those other means require unreasonably excessive efforts; the extent (intensity) of implementing a covert investigative measure must be proportionate to its legitimate goal.[55]

CPCG provides an exhaustive list of covert investigative measures, that includes, the covert eavesdropping (wiretapping) and recording of telephone communication and its meta data.[56]

As stated in CPCG, covert investigative actions can be carried out under a court ruling. The prosecutor should submit a reasoned motion to a court seeking prior authorization of the measure; a judge should make an assessment of the motion based on a number of requirements and may allow the covert measure for a limited period of time.[57] However, exception to the rule is allowed in the case of urgent necessity, when a delay may cause destruction of the facts important to the case (investigation), or make it impossible to obtain those data, a covert investigative action may be carried out/commenced without a judge's ruling, under a reasoned resolution of a prosecutor.[58] *Ex post* judicial review is ensured within a short time-limit - a prosecutor must file a motion with a district (city) court to recognize as lawful the covert investigative action carried out in the case of urgent necessity/in progress not later than 24 hours from the time of commencing the covert investigative action.[59] A prosecutor has to prove the existence of circumstances that required an urgent carrying out/commencement of the covert investigative action without a court ruling.

Covert measures may be conducted not only within an ongoing criminal investigation, but also in other legal contexts, in particular within the framework of "operational-search activities"[60] and counter-intelligence activities.[61] According to the Law of Georgia on Counter-Intelligence Activities, special services authorized to undertake intelligence activities are entitled to interfere in the private lives of individuals without court order except for electronic surveillance and control of correspondence which may only be carried out based on a judicial order.[62] These regulations contradict the standards set by the Constitution of Georgia[63] as it allows interference in two crucial areas of private life – privacy of communication and personal space without a court order/authorization. Based on the existing legislation, information on counter-intelligence activities is classified.

---

[54] IDFI, Secret Surveillance in Georgia - Analysis of the Legislation and Practice, 2020, available at: https://bit.ly/3BmwqN1

[55] Article 143^2 of the Criminal Procedure Code of Georgia.

[56] Article 143^1 (1) of the Criminal Procedure Code of Georgia.

[57] Article 143^3(1)(2)(5)(10)(12) of the Criminal Procedure Code of Georgia.

[58] Article 143^3 (6) of the Criminal Procedure Code of Georgia.

[59] Id.

[60] Articles 7 and 14 of Law of Georgia "On operational-search activities".

[61] Article 9 of Law of Georgia "On counter-intelligence activities".

[62] Article 11 of Law of Georgia "On counter-intelligence activities".

[63] In 2015, the Social Justice Center (former "Human Rights Education and Monitoring Center" (EMC)) filed an appeal at the Constitutional Court of Georgia claiming that the Law on Counter-Intelligence Activities (namely section 2 of Article 11 and section 1 one Article 15) was unconstitutional, the Constitutional Court has not rendered a decision on the case yet, constitutional complaint is available at: https://constcourt.ge/ka/judicial-acts?legal=2044

Relevant documents, case materials and other data constitute state secrecy and supervision or control over them is limited.[64]

In April 2022, individual members of the parliamentary majority initiated draft amendments to the CPCG on the use of covert investigative measures in criminal proceedings. Those amendments include the wider scope of crimes covered by potential covert surveillance measures, the longer period for such measures, risks of indefinite prolongation of certain surveillance activities. The bill was criticized at the local[65] and international level.[66] CSO stipulated that the legislation on wiretapping would deteriorate further if the draft law was adopted.

In June 2022, the Parliament of Georgia adopted a draft law amending Georgia's procedure for the use of covert investigative measures in a hasty procedure. Civil Society Organizations (CSOs) have called on the president to veto the amendments.[67] The President of Georgia vetoed those amendments considering that they excessively extended the powers of the law-enforcement authorities and then requested an urgent opinion of the Venice Commission on the draft law of Georgia on the Amendment to the CPCG on 1st of July, 2022.

Venice Commission delivered the urgent opinion on 26th of August according to which, the draft law required both impact assessment and more detailed justification.[68] The opinion concluded that the overall oversight mechanism of secret surveillance measures in Georgia seems to be inadequate and there is a need for a comprehensive revision of existing covert surveillance systems.[69]

On 6th of September, 2022, The Parliament of Georgia, without taking into consideration the assessment of the Venice Commission and critical views of the local organizations, overruled the veto and amendments to the Criminal Code of Georgia went into force. Notably, the President still did not sign the amendments thus the chairman of the parliament signed and published the law. As a consequence:

a) the list of crimes eligible for investigation by means of covert measures was extended;
b) the overall maximum duration of covert measures was prolonged from … to …;
c) the notification of persons concerned about the use of covert measures in certain cases may be postponed as many times as deemed necessary.[70]

The newly enacted amendments do not provide sufficient safeguards against unjustified intrusion into the private lives of individuals and the potential abuse of power. It can be assumed that the aim of these changes were not to improve the balance between conflicting values, rather to worsen it.

---

[64] Article 159(13) of the Rules of Procedure of the Parliament of Georgia.

[65] https://transparency.ge/en/post/legislation-wiretapping-deteriorates-further

[66] https://www.eeas.europa.eu/delegations/georgia/remarks-ambassador-carl-hartzell-following-amendments-criminal-procedure-code_en?s=221

[67] Statement of the CSOs of Georgia. June 9, 2022. link.

[68] https://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2022)028-e

[69] Venice Commission, Urgent opinion on the Draft Law on the Amendments to the Criminal Procedure Code adopted by the Parliament of Georgia on 7 June 2022, issued on 26 August 2022 pursuant to Article 14a of the Venice Commission's Rules of Procedure, 26 of August, 2022, available at: https://bit.ly/3DqZ8Pu

[70] According to current legislation, the notification about the use of covert investigative measures in certain cases may be postponed for as many times as is necessary to avoid a threat to State security, public order and in interest of legal proceedings.

Offenses that May Give Rise to Surveillance Measures. Covert investigative actions can be carried out if an investigation has been initiated and/or criminal prosecution is conducted due to an intentionally grave and/or particularly grave crime or to any of the crimes provided for by the CPCG. Recent amendments in the CPCG extended the scope of crimes covered by the provisions relating to the secret investigative measures to a large number of crimes which are not in the "grave crime" category.[71]

It is also noteworthy that from 2019 covert investigative actions can be carried out concerning all official misconduct. As a result of legislative changes, such interference in private life is even allowed when a person allegedly committed a crime by negligence.

A body with an Exclusive Authority to Carry out the Covert Wiretapping and Recording of Telephone Communication and its Authority. In 2017, the Parliament of Georgia adopted legislative changes, which introduced new regulations of organizing technical infrastructure for conducting secret electronic surveillance. The amendments were heavily criticized by various stakeholders, as enacted provisions failed to ensure the genuine independence of the newly created Operative-Technical Agency (OTA) from the State Security Service.[72] The Public Defender of Georgia, political parties and up to 300 citizens, filed an appeal against the mentioned regulations (the constitutionality of several norms related to the covert investigative activities, computer data, data bank and supervision are being questioned) at the Constitutional Court of Georgia but after more than 5 years, the court has not rendered a decision yet.[73]

OTA is a body with an exclusive authority to carry out the covert wiretapping and recording of telephone communication and other covert investigative actions.[74] The agency is an institution with a special regime status.[75] Illegal interference in the activities of the OTA is prohibited by the law,[76] but the legislation does not provide for the corresponding guarantees - proper mechanisms of control and supervision.

The legislation allows OTA to gather information from any source of communication – it has the power of obtaining information in real-time with the use of stationary or semi-stationary technical means and, for this purpose, if necessary, to place without free of charge, a lawful interception management system and/or devices related to it/necessary for its functioning and software.[77] In addition, OTA is responsible for copying and storing communications metadata in the centralized bank of Data.[78]

The most problematic issue is that the OTA is in the sphere of governance of the State Security Service, the Head of the State Security Service determines the basic structure of the OTA and the competence of its organizational subdivisions and territorial bodies.[79] It remains fully dependent institutionally, financially and organizationally on the State Security Service.[80] Therefore, the agency which is authorized to conduct covert investigative measures and has real-time access to extremely sensitive data, operates under the administration

---

[71] Article 143^3 (2)(a) of the Criminal Procedure Code of Georgia.

[72] IDFI, Secret Surveillance in Georgia - Analysis of the Legislation and Practice, 2020, available at: https://bit.ly/3BmwqN1

[73] https://constcourt.ge/ka/judicial-acts?legal=1958&fbclid=IwAR21z4JieIiUKsHgc_ix7F5VZObq4HruAgek_u66PTaRPsjlj0i48sua7Jg

[74] Article 143^1 (1)(a-d) of the Criminal Procedure Code of Georgia.

[75] Article 3(2) of Law of Georgia "On a legal entity of public law, the Operational-Technical Agency of Georgia".

[76] Article 5(2) of Law of Georgia "On a legal entity of public law, the Operational-Technical Agency of Georgia".

[77] Article 8^1(1)(a) of Law of Georgia "On Electronic Communications".

[78] Article 11 and article 15 of the law of Georgia on "Law of Georgia "On a legal entity of public law, the Operational-Technical Agency of Georgia."

[79] Article 22(1) of Law of Georgia "On a legal entity of public law, the Operational-Technical Agency of Georgia".

[80] Public Defender's statement on Alleged Illegal Wiretapping, 3rd of August, 2021, available at: https://bit.ly/3trRNdx

of the State Security Service, which is equipped with investigative powers and has been accused of illegal surveillance many times.

It is pertinent to note that, among other things, the State Security Service has the competence to carry out operational-search activities, counter-intelligence measures as well as investigative and covert investigative measures.[81]

The Constitutional Court of Georgia in its judgment of 14 April 2016 noted that the law-enforcement bodies have a professional interest to have as much information as possible, as it would simplify the investigation of an already committed crime and contribute to preventing future crimes. Therefore, direct and permanent access of such state bodies to providers of electronic communication services and electronic communication itself greatly increases temptation and risks.[82] The risks of abuse of the powers increase unless there are adequate mechanisms of supervision. So, the technical ability of the Operational-Technical Agency to monitor the communications in real-time poses a threat that the State Security Service will acquire total control.

According to the Venice Commission's urgent opinion, "it remains unclear if the OTA operates on the basis of clear and strict regulations prescribing rigorous separation of data gathered for different purposes. Moreover, there appears to be no appropriate system of accountability and oversight regarding this technical agency and the State Security Service in general… With the exclusive role of the OTA in implementing covert measures, the boundary between the legal regimes on covert measures becomes blurred. As a result of this technical overlap, the covert investigative measures may be used by the State Security Service in a wider, non-criminal context, such as broader "intelligence" gathering."[83] The independence and oversight mechanisms of OTA were questioned by other international actors over the past years.[84]

Although the law indicates so,[85] the OTA can't be deemed to be an independent body. Ensuring genuine independence of OTA constitutes a significant challenge.

Categories of Individuals Liable to be Subjected to Covert Investigative Measures. In order to conduct a covert investigative measure, law stipulates that there must be a reasonable cause to believe that a person, against whom a covert investigative action is to be carried out, has committed the above mentioned crimes, or a person receives or transmits information that is intended for, or is provided by, a person directly related to the crime, or a person directly related to the crime uses the communication means of the person.[86]

According to the CPCG, covert investigative actions against a clergy person, an attorney, a doctor, a journalist and a person enjoying diplomatic immunity, may be carried out only where this is not related to obtaining information protected by law in the course of their religious or professional activities, respectively.[87] The mentioned individuals are enjoying immunity as the law provides for the principle of protecting privileged information.

Despite that, thousands of files containing personal data of clerical leaders, journalists and foreign diplomats obtained via allegedly illegal surveillance were disclosed in 2021.[88] The investigation has been launched, but nothing has been established yet. The journalists had addressed the European Court of Human rights (ECHR) and after that, the Prosecutor's Office of Georgia recognized them as the victims of the crime.

---

[81] Article 12 of Law of Georgia "On State Security Service of Georgia".

[82] The judgment №1/1/625,640 of Constitutional Court of Georgia adopted on 14th of April 2016.

[83] Venice Commission, Urgent opinion on the Draft Law on the Amendments to the Criminal Procedure Code adopted by the Parliament of Georgia on 7 June 2022, issued on 26 August 2022 pursuant to Article 14a of the Venice Commission's Rules of Procedure, 26 of August, 2022, available at: https://bit.ly/3DqZ8Pu

[84] U.S. Department of State Country Report 2019, available at: https://bit.ly/2Wt9Dvc; Freedom House, Georgia Country Report 2018, available at: https://bit.ly/2OyBUfw

[85] Article 5 of Law of Georgia "On a legal entity of public law, the Operational-Technical Agency of Georgia".

[86] Article 143^3 (2) of the Criminal Procedure Code of Georgia.

[87] Article 143^7 (2) of the Criminal Procedure Code of Georgia.

[88] IDFI responds to the Leak of surveillance files, available at: https://bit.ly/3LaCeO5

Duration of the Covert Surveillance Measure. New legislative changes concerned the duration of covert investigative measures. According to the amendments, the covert investigative measure may be conducted in three stages, where each stage has the maximum duration of 90 days, this gives a total of 270 days.[89] In addition to this general procedure, further extensions are allowed for another period of 90 days in the context of international criminal cooperation. However, with regard to a certain number of crimes extensions can be authorized as many times as it is deemed necessary for the investigation.[90]

As stated in the urgent opinion of the Venice Commission, the possibility of numerous extensions of covert measures for certain crimes – as many times as it will be necessary for the investigation – appears excessive.[91]

Before changing the regulation, the overall duration of the covert investigative measure was not exceeding six months. The Parliament has not provided the proper explanation to justify such a heavy interference in the private lives of individuals.

Storing, Registering and Destroying the Information Obtained as a Result of a Covert Surveillance Measure. Pursuant to the CPCG, a body carrying out covert investigative actions and relevant investigative authorities are responsible for appropriately safeguarding the information obtained as a result of covert investigative actions.[92] The body carrying out a covert investigative action must keep a record of the data related to covert investigative actions.[93]

The OTA is authorized to store the identifying data of electronic communication for a maximum period of 12 months.[94] This period can be extended only once, for 3 months.[95]

CPCG envisages the obligation to immediately destroy the information after the termination or completion of covert measures, unless the information is of value to the investigation. The materials shall be immediately destroyed, if they are obtained as a result of operative-investigative actions and do not concern a person's criminal activities, but include details of that person's or any other person's private life and are subject to destruction under Article 6(4) of the Law of Georgia on Operative-Investigative Activities.[96] Materials obtained as a result of covert investigative actions, which are recognized by a court as inadmissible evidence, shall be immediately destroyed six months after the court of final instance renders a ruling on the case. Until destruction, these materials shall be kept in a special depository of a court. No one may access these materials, or make copies of them or use them, except for the parties, who use them for the purpose of exercising their procedural powers.[97]

There were numerous instances where illegal telephone recordings, video footage depicting scenes of private lives were made public. So, these leaked materials indicate that this system has some serious problems in practice.

Supervision over Covert Investigative Measures. CPCG provides legal mechanisms to execute proper judicial control over the procedure for applying covert investigative measures. However the poor quality of

---

[89] Article 143^3 (12^1) of the Criminal Procedure Code of Georgia.

[90] Article 143^3 (12^7) of the Criminal Procedure Code of Georgia.

[91] Venice Commission, Urgent opinion on the Draft Law on the Amendments to the Criminal Procedure Code adopted by the Parliament of Georgia on 7 June 2022, issued on 26 August 2022 pursuant to Article 14a of the Venice Commission's Rules of Procedure, 26 of August, 2022, available at: https://bit.ly/3DqZ8Pu

[92] Article 143^5(1) of the Criminal Procedure Code of Georgia.

[93] Article 143^5(2) of the Criminal Procedure Code of Georgia.

[94] Article 15(1) of Law of Georgia "On a legal entity of public law, the Operational-Technical Agency of Georgia".

[95] Id, Article 15(2).

[96] Article 143^8(1) of the Criminal Procedure Code of Georgia.

[97] Article 143^4(2) of the Criminal Procedure Code of Georgia

judicial supervision is noticed by the Venice Commission, as it refers to such factors in the urgent opinion as (i) the practice of allocating very little time to examining such requests, (ii) the high workload of a judge, and (iii) the high approval rate of motions for covert measures.[98] Another issue mentioned in the opinion is the technical knowledge and expertise which a judge should possess in order to efficiently examine the requests in this specialized area. Moreover, it is unclear to what extent in practice judges examine primary materials of the case and what sort of justification the prosecuting authorities have to provide in order to obtain a court authorization.[99]

The control and supervision of covert investigative activity is also carried out by the Personal Data Protection Service (PDPS) in accordance with the Law of Georgia "On Personal Data Protection".[100] It should be noted that the PDPS does not have the authority to oversee the processing of the data defined as a state secret for the purposes of state security (including economic security), defense, intelligence and counterintelligence activities.[101] This may be considered a serious limitation in practice, because at the technical level, the covert measures are implemented by the OTA.[102] PDPS lacks the ability to detect facts of covert surveillance and wiretapping carried out without a court order and a prosecutor's decision. As stated in the 2021 annual report of the State Inspector's Service[103] (until February 2022, this agency was responsible to monitor the covert investigative activities), the Service lacks legislative mechanisms and leverage to investigate the facts of covert surveillance and wiretapping carried out in alleged breach of legislative requirements in this area.[104]

The legislation also provides for parliamentary control: the Trust Group is authorized to inspect the activities of the Operative-Technical Agency no more than twice per year.[105] However, the existing rules of overseeing the activities of OTA are vague and do not allow for detailed oversight of its activities.[106] Trust Group's access to the information regarding covert activities and methods (including normative acts) is limited[107] and this approach contradicts the recommendations of the Council of Europe, according to which, in order to effectively carry out its functions, the oversight body should have unlimited access to any type of information.[108]

Within the current legal regime, Trust Group does not have the authority to really look into the activities of the State Security Service, so without having a realistic picture, Trust Group lacks the ability to exercise effective control.

For years, the Public Defender has been referring to insufficient safeguards of privacy and high risks of arbitrary actions on the part of the government.[109] Pursuant to the annual report of Ombudsman, current

---

[98] Venice Commission, Urgent opinion on the Draft Law on the Amendments to the Criminal Procedure Code adopted by the Parliament of Georgia on 7 June 2022, issued on 26 August 2022 pursuant to Article 14a of the Venice Commission's Rules of Procedure, 26 of August, 2022, available at: https://bit.ly/3DqZ8Pu

[99] Id.

[100] Article 143^8(1) of the Criminal Procedure Code of Georgia.

[101] Article 3(3)(C) Law of Georgia on Personal Data Protection.

[102] Venice Commission, Urgent opinion on the Draft Law on the Amendments to the Criminal Procedure Code adopted by the Parliament of Georgia on 7 June 2022, issued on 26 August 2022 pursuant to Article 14a of the Venice Commission's Rules of Procedure, 26 of August, 2022, available at: https://bit.ly/3DqZ8Pu

[103] On 30 December 2021, the Parliament of Georgia adopted a law by which it abolished the State Inspector's Service – a body established in 2018 with a mandate to monitor the lawfulness of personal data processing and covert investigative measures as well as to carry out the investigation of alleged crimes in law-enforcement agencies. Two separate institutions were created: the Personal Data Protection Service and the Special Investigation Service.

[104] Annual Report 2021 of the State Inspector's Service, p. 285, available at: https://bit.ly/3UaNXAp

[105] Article 159(1) of the Rules of Procedure of the Parliament of Georgia.

[106] IDFI, Secret Surveillance in Georgia - Analysis of the Legislation and Practice, 2020, available at: https://bit.ly/3BmwqN1

[107] Article 159(3) of the Rules of Procedure of the Parliament of Georgia.

[108] Council of Europe, Democratic and effective oversight of national security services, 2015, available at: https://rm.coe.int/16806daadb

[109] Report of the Public Defender of Georgia, 2021, available at: https://bit.ly/3QTL97I

legislation forms the basis for uncontrolled interception since it allows the security agencies to have uncontrolled, direct connection to the servers of mobile operators.[110]

In conclusion, legislation of Georgia regulating the surveillance of mobile communications was mostly in line with the requirements of human rights and right to privacy in particular. However, the recent amendments to the CPCG have raised major legal concerns and the legitimacy of these concerns were confirmed by the opinion of the Venice Commission.

Legislation of Georgia regarding the technical implementation of the surveillance measures is a major threat to the right to privacy in Georgia. Namely, OTA, which is a state agency under the State Security Service of Georgia, has the direct technical access to the infrastructure of the telecommunication companies. In addition, law entitles the OTA to create the Central Bank of the metadata, where all the metadata, created by mobile communications throughout the territory of Georgia, is stored for at least one year. PDPS has the major responsibilities in terms of technical oversight of OTA, however powers of the PDPS are limited and there are major concerns regarding its effectiveness on the technical level.

During the recent years major incidents of possible illegal surveillance were detected. It seems the law enforcement agencies are unwilling or unable to properly investigate the incidents. Compatibility of the current legal framework for surveillance with the requirements of the right to privacy is questioned, respective applications to the ECHR are sent.

[110] Report of the Public Defender of Georgia, 2021, available at: https://bit.ly/3QTL97I

ARMENIA

The Armenian legislation quite clearly defines the surveillance of phone and electronic communication. Only a few structures, including the RA National Security Service, the Police, and the Anti-Corruption Committee, have extensive wiretapping capabilities.

On the other hand, there are no clear-cut mechanisms that would allow to make this sector transparent and accountable to the public.

The latest developments suggest that things are changing in the country, and apart from the traditional wiretapping of phones, more sophisticated, digital tools are emerging, making the control over citizens deeper and more comprehensive. This, in turn, raises concerns on whether these tools will be used within the law, in line with the requirements of democracy and civil liberties.

Legislative and institutional regulations. The main legislative regulation is carried out within the framework of the Law on Operational Intelligence Activities, which was adopted in 2007 and has been revised and supplemented several times since then.[111]The law determines the state bodies that have the right to monitor phone communication. According to Article 14 of the Law (Types of operational intelligence measures), these are the Police, National Security Bodies, and the Anti-Corruption Committee. Apart from that, the bodies of the penitentiary service have the right to conduct wiretapping, but only in the premises of the penitentiary institutions of the RA Ministry of Justice.

It should be noted that the RA Anti-Corruption Committee is a newly established structure in the law enforcement system: it was established and has been operating since October 23, 2021.

Until January 2020, the Police did not have either the opportunity to conduct wiretapping on their own. They used the capacities of the National Security Service (hereinafter – NSS), which made the NSS extremely influential in the field of wiretapping. Moreover, the data collected for the Police actually appeared at the disposal of the NSS as well. The RA National Assembly initiated changes in the Law on Operational Intelligence Activity, which turned the Police into an independent structure in this matter, creating some counterbalance to the NSS. However, during the discussions at the National Assembly it became clear that the Government had a completely different approach to this issue – to create a separate independent organization and transfer the right of wiretapping to it.[112]

According to Article 26 of the Law, digital, including telephone communication surveillance embraces the following:

1. in the case of a fixed or mobile telephone network the content of telephone conversation, text, image, audio, video and other messages, the subscriber's incoming and outgoing calls, the telephone numbers indirectly related to the subscriber, the time of starting and ending the telephone communication, and in case of call forwarding or transferring, the phone number to which the call was transferred;
2. in the case of Internet communication, including telephone communication via Internet and electronic messages transferred via Internet, the content of the communication, incoming and outgoing calls via Internet (each data in such a form that allows or may allow to identify the communicator);
3. when implementing the operational intelligence measures envisaged by this Article, the telecommunication organizations are obliged, upon the request of competent authorities, to provide technical facilities and create other conditions necessary for the conduct of operational intelligence measures.

According to Article 9 of the Law, the implementation of digital, including operational intelligence measure of wiretapping is ensured only by the general operational technical department functioning within the system of the Republican National Security Body of the Republic of Armenia. That body is directly managed by the head of the NSS. And the head of the General Department is appointed and dismissed from the position by the Prime

[111] https://www.arlis.am/documentView.aspx?docid=128809

[112] The police have been allowed to tap phone conversations, https://www.irazek.am/hy/news/14110

Minister. The General Department ensures the necessary operational and technical conditions for telecommunication operator.

The surveillance of digital and telephone communication by the police, penitentiary service or the Anti-Corruption Committee is carried out by creating operational and technical conditions, including the provision of channels and resources by the General Department. At the same time, the law requires that the National Security Service excludes the supervision and corroboration of these data, information and reports, if the wiretapping party is not the NSS itself.

Wiretapping can be carried out only in cases where there are apparent grounds to suspect that the person to whom they can be applied has committed a serious or particularly serious crime, and it is reasonably impossible for the body conducting the operational intelligence measure as assigned by the Law to obtain the necessary information in any other way.

It is noteworthy that the collection of such data is prohibited when the targeted person is communicating with his/her lawyer, representative or legal representative. If such data are obtained for any independent reason, then the information containing legal secret is subject to immediate destruction.

Article 32 of the Law states that wiretapping is carried out on the basis of a court decision. In cases when delay in implementing an operational intelligence measure such as digital, phone communication surveillance, may result in an act of terrorism or in events or actions threatening the state, military or environmental security of the Republic of Armenia, the General Department ensures the implementation of these measures. However, the body that applies to the General Department must within 48 hours submit to the General Department the excerpt of the decision of the court on permitting or denying permission to undertake those measures.

Article 39 reads that the term for the decision to conduct an operational intelligence measure is calculated starting from the day of its adoption and cannot exceed 2 months. The decision period may be extended. Moreover, each court's permission can be given for a period not exceeding two months. And the overall term cannot last more than 12 months.

The developments in Armenia. In recent years, along with the increase in the possibilities of digital surveillance, there has also been an increase in cases that may be considered as abuses of law. In 2020, under the circumstances of the COVID-19 pandemic, the government made several attempts to oversee people's social connections and movement through phones.

On March 31, 2020, the National Assembly adopted the proposal to amend the draft laws "On the Legal Regime of the State of Emergency" and "On Electronic Communications."[113] According to those amendments, the Government was awarded the right to receive from all mobile operators, collect and process in one place information on all the residents of the country, namely the metadata of phone calls and short messages and the location data collected by mobile operators. Based on those data, a system was created that was supposed to identify the possible circle of people infected with coronavirus. The NSS was appointed as the coordinator of the project, and the technical implementer was an undisclosed private company. On September 25, when the state of emergency was lifted, all collected data were destroyed in the presence of the mobile operators' representatives.[114]

A number of issues, however, lacked transparency:

- **a.** No public oversight mechanism was created. No guarantee was given that the system had not been used for other purposes, such as identifying specific people and their connections.
- **b.** It remained unclear who created the system.

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

[114] "Statement on destruction of information and storage devices [in Armenian]," Government of Armenia, September 25, 2020, https://www.gov.am/u_files/file/Haytararutyunner/Ardzanagrutyun.pdf

c. According to the law, the data collected by the system were to be destroyed at the end of the state of emergency. Since there was no independent supervision over the system, there is no guarantee that the data were indeed fully destroyed, and moreover that the system is any longer functioning.

On November 24, 2021, several dozen people in Armenia received emails from Apple, which alerted that they had been allegedly attacked by a state-sponsored hacking group. CyberHUB-AM is aware of more than twenty such cases in Armenia. This was global in nature: the alert disseminated by Apple did not refer only to Armenia. It is worth reminding that a few hours before receiving the emails, Apple had announced that it was suing the Israeli NSO Group, which creates and sells spyware to government agencies for intelligence operations. The program's name is Pegasus, and most probably the email was addressed to the potential victims of this program.

Some announced publicly that they had received similar emails. Artur Vanetsyan, former head of the National Security Service, currently one of the leaders of "With Honor" opposition parliamentary bloc, was one of them.[115] The other one was Davit Sanasaryan.[116] Later, lawyer Anna Karapetyan informed about a similar thing.[117] According to cyber security expert Ruben Muradyan, he had discovered Pegasus on Vanetsyan's and his relatives' phones 2 months earlier.[118] It should be noted that before that Armenia had never appeared on the list of countries that use Pegasus at the state level. There is also an assumption that it was used by the special services of a third country. Given the list of possible infected users and the fact that everyone received the email with an alert at the same time, it can be assumed that Apple could have included several waves of attacks in one phase of warning campaign. It is quite possible that we are dealing with several cases where the infections, for example, could be conditioned by external and internal political reasons, since all the users infected with the spyware could hardly be of interest to one party that carried out an attack.

If in the case of Pegasus there were doubts that some of those who received notifications could be a target of a domestic attack, but there were no real clues, the situation changed at the end of the year. On December 16, 2021, for the first time, Armenia as a state directly appeared on the list of countries that use spyware to infect and spy on people's phones within the country. This was discovered by Facebook[119] and CitizenLab.[120] The target were politicians and people related to media. Spyware for Android and iPhones produced by Macedonian company Cytrox was used. The virus was disseminated through fake links mimicking real websites, for example, youtu-be[.]net. There were also cases of infection attempts through SMS and messages sent via messengers. Later, Google, referring to this topic, clearly stated that, in their view, this had been carried out by the state structures of the Republic of Armenia: "Consistent with findings from CitizenLab, we assess likely government-backed actors purchasing these exploits are operating (at least) in Egypt, Armenia, Greece, Madagascar, Côte d'Ivoire, Serbia, Spain and Indonesia."[121]

Of course, there is no clear evidence on the use of Pegasus by Armenian state structures. The beneficiary of the use of Predator is not clearly known either. On the other hand, according to Point 3 of Article 7 of the Law on Operational Intelligence Activity":

> "*The use of special technical and other means envisaged (developed, planned, adjusted) for obtaining confidential information and implementation of operational intelligence measures by state authorities, subdivisions or natural and legal persons not authorized under this Law shall be prohibited*."

---

[115] Artur Vanetsyan's post – https://www.facebook.com/avav111/posts/4128774197228456
[116] Davit Sanasaryan's post – https://www.facebook.com/sanasaryan/posts/10226843862500815
[117] Anna Karapetyan's post – https://www.facebook.com/anna.karapetyan.1238/posts/4762248813827737
[118] Ruben Muradyan's post – https://www.facebook.com/ruben.muradyan/posts/4521469627973414
[119] Threat Report on the Surveillance-for-Hire Industry, December, 2021, https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf
[120] Pegasus vs. Predator, 16 December, 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/
[121] Protecting Android users from 0-Day attacks, May 19, 2022, https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/

This implies that there has been published a report on a crime, on the basis of which a criminal case should have been initiated. Nevertheless, the Police or NSS have not disseminated such information.

It turns out that one of the major problems today is the lack of any mechanism of public oversight in this field. There is no possibility to oversee the activities of power structures, as all the work is basically a state secret. According to the Law on Operational and Intelligence Activities, during the entire implementation period of operational intelligence measures the information with regard to forces, means and resources, methods, plans, results of those measures, financing thereof, as well as secret staff members of bodies carrying out operational intelligence activity, including persons cooperating or having cooperated, on a confidential basis, is deemed to be a state secret. And Armenia, in fact, has no efficient public oversight mechanisms that would allow to make accountable those structures that operate under the umbrella of state secrecy. Thus, civil society has no toolkit to monitor the situation or influence it.