The Pegasus Project and Azerbaijan - what does domestic legislation tells us about privacy of users in Azerbaijan

Background

Members of opposition political parties, independent journalists, political and human rights activists have long faced systematic pressure and persecution orchestrated by the government of Azerbaijan. The unprecedented crackdown against civil society that began in 2013, marked a new chapter, in the history of Azerbaijan's civil society. One, marred by arrests and prosecution of high-profile activists, rights defenders, and journalists.

This systematic pressure and harassment was not only offline. It was only a matter of time, that the internet too would become a place to target activists, journalists, and human rights defenders, holding them accountable for their online criticisms on bogus accusations that often ended with lengthy jail sentences, forced apologies on public televisions (see The State of Internet Freedom in Azerbaijan report), detentions and further forms of persecution.

In a country where almost all avenues for freedom of expression and activism were eliminated, the internet, specifically online media platforms and social media networks became new targets. To monitor discussions online, prevent citizens from accessing independent news online, or social media platforms, and to further curb freedoms online, the government of Azerbaijan embarked on a shopping spree, becoming a client of companies selling sophisticated surveillance equipment and technology.[1]

By 2021, the government of Azerbaijan has successfully deployed Remote Control System (RCS), Deep Packet Inspection (DPI), phishing and spear-phishing attacks often with home grown malware. The most recent addition to a wide variety of authoritarian technology deployed in Azerbaijan is Pegasus spyware.

The Pegasus Project

On July 18, 2021, an international consortium of more than 80 journalists from 17 media outlets revealed the Pegasus Project. Spearheaded by Forbidden Stories, a Paris based journalism non-for-profit, with technical support of Amnesty International Security Lab, the Pegasus Project is a global investigation into an Israeli surveillance company, the NSO Group, and its most sought after hacking software called Pegasus.

According to the investigation, the NSO Group sold Pegasus to at least ten government clients including in Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Azerbaijan, Rwanda, Saudi Arabia and the UAE. Among the targets were journalists, human rights defenders, political opponents, business people, and heads of states.

> "Forbidden Stories and Amnesty International had access to a leak of more than 50,000 records of phone numbers that NSO clients selected for surveillance," wrote Forbidden Stories sharing the findings of the investigation.

On the leaked phone records, at least 1000 were identified as belonging to users from Azerbaijan. One of the media partners in the investigation, the Organized Crime and Corruption Reporting Project (OCCRP) took on to investigate numbers that belonged to users in Azerbaijan, Kazakhstan, and Rwanda.

[1] Internal company documents show Azerbaijan's Ministry of National Security purchased Hacking Team's Remote Control System (RCS) surveillance spyware via a California-based intermediary called Horizon Global Group in 2013 for an initial payment of €320,000. https://www.occrp.org/en/daily/4136-azerbaijan-bought-hacking-team-s-surveillance-spyware-leaks-reveal

So far, OCCRP was able to identify 250 phone numbers targeted, which belonged to reporters,[2] editors, media company owners, activists, human rights defenders and their family members. As of July 27, OCCRP confirmed at least 80 cases of alleged surveillance.[3]

Following the release of the investigations, international organizations, such as Reporters Without Borders, said they will pursue legal action against those responsible for this massive surveillance.[4] In Azerbaijan, some of the targeted individuals intend to appeal to local courts and then to the European Court of Human Rights, on the grounds of infringements of their right to private life.[5]

While law enforcement authorities in Hungary[6], Israel[7], France[8], the USA[9], and Algeria[10] have launched probes into suspected unlawful surveillance via Pegasus spyware, the Azerbaijani law enforcement agencies are yet to respond.

What chance do those targeted in Azerbaijan stand in pursuing legal action against the governmnet of Azerbaijan? To answer this question, we look at the national legislation enabling the government to carry out surveillance en masse and citizens' rights to privacy.

Domestic frameworks

The right to private life is under the protection of comprehensive constitutional provisions, namely Article 32 of the Azerbaijani Constitution which guarantees that everyone has the right to the inviolability of private[11] and family life, including with respect to correspondence, telephone communications, post, telegraph messages and information sent by other means of communication. Article 32 further states that gaining, storing, using and spreading information about the person's private life without his/her consent is not permitted. These rights may ***be restricted, as prescribed by law,*** in order to prevent crime or to determine the truth in the course of investigation of a criminal case. Section eight of article 32 also indicates that the scope of the personal information, as well as the conditions of their processing, collection, sharing, use, and protection, is prescribed by law.

In addition, there are normative legal acts recognizing the right to private life, including regulating the restrictions of private life in the telecommunications networks.

---

[2] Turan, Pegasus has been spying on Azerbaijani journalists and activists over years, July 19, 2021, https://www.turan.az/ext/news/2021/7/free/politics_news/en/5975.htm/001

[3] OCCRp, People Selected for Targeting by Azerbaijan, https://cdn.occrp.org/projects/project-p/?_gl=1*rnxzxn*_ga*MjEyNTY0MTgzMS4xNjI3NDE1OTE1*_ga_NHCZV5EYYY*MTYyNzQxNTkxMy4xLjEuMTYyNzQxNTkyNy40Ng..#/countries/AZ

[4] Turan, The organization in defense of press freedom "Reporters without Borders" is outraged by the fact that 200 journalists from 20 countries are being spied on with the help of the Israeli spy system Pegasus, July 2021, http://www.turan.az/ext/news/2021/7/free/politics_news/en/6042.htm/001

[5] Voice of America, Interview with Bakhtiyar Hajiyev, July 20, 2021, https://www.amerikaninsesi.org/a/bəxtiyar-hacıyev-avtoritar-rejimlər-hətta-ən-yaxın-çevrəsinə-güvənmir/5972455.html

[6] Al Jazeera, Hungary prosecutors open investigation into Pegasus spying claims, July 22, 2021, https://www.aljazeera.com/news/2021/7/22/hungary-prosecutors-open-investigation-into-pegasus-spying-claims

[7] Al Jazeera, Israel launches commission to probe Pegasus spyware: Legislator, July 22, 2021, https://www.aljazeera.com/news/2021/7/22/israel-launches-commission-to-probe-pegasus-spyware-legislator

[8] Euractive, France launches investigation into Pegasus spying allegations, July 22, 2021, https://www.euractiv.com/section/cybersecurity/news/france-launches-investigation-into-pegasus-spying-allegations/

[9] Reuters, FBI probes use of Israeli firm's spyware in personal and government hacks - sources, July 22, 2021, https://www.reuters.com/article/us-usa-cyber-nso-exclusive-idUSKBN1ZT38B

[10] The Star, Algeria launches probe into Pegasus spyware claim, July 22, 2021, https://www.thestar.com.my/tech/tech-news/2021/07/23/algeria-launches-probe-into-pegasus-spyware-claim

[11] Constitution of the Republic of Azerbaijan, https://static2.president.az/media/W1siZilsIjIwMTgvMDMvMDkvNHQzMWNrcGppYV9Lb25zdGl0dXNpeWFfRU5HLnBkZiJdXQ?sha=c440b7c5f80d645b

While mentioning a catalogue of rights for individuals in respect to right to privacy[12], article 3 of the basic law on private data - *the Law on Private Information,*[13] stipulates that the rules for the collection and processing of personal data, concerning intelligence and counterintelligence, and operation-search activities are regulated by other respective legal acts (discussed below).

The *Law on Private Information* obligates the operators, to create necessary conditions for intelligence, counterintelligence, and search operations in accordance with the legislation, to guarantee relevant organizational and technical issues, and comply with the confidentiality of the methods used to conduct these activities.[14]

Along with the *Law on Personal Data*, the *Law on Telecommunication* also determines the powers of state bodies, notably subjects of intelligence and counterintelligence search operations, to collect or intercept personal data from the telecommunication channels and networks.[15]

In Azerbaijan there are two types of oversight over citizens:

1. Extraction of information from telecom channels, i.e., interception; and
2. Surveillance.

The *Law on Operation-Search Activity*, oversees phone tapping and information extraction from communication channels.[16] Further, the third section of article 10 of the *Law on Operation-Search Activity* does not require a judicial act or supervision of higher authority while wiretapping and extracting information from technical communication channels unless there is a need to install technical devices such as voice, video or photo recorders at the place of residence of the individuals.

In other words, anyone in Azerbaijan can be subject to such form of oversight.

The *Law on Telecommunication* obligates network operators to install special equipment, provided by the State Security Service, Ministry of Internal Affairs and Special State Protection Service onto the telecommunication networks[17] enabling the Government to extract (intercept) data on anyone regardless of whether that person(s) is part of an investigation process or not.

The installment of special equipment within communication networks is regulated by the *"Rules for equipping telecommunications operators and providers with additional technical means for conducting search operations, reconnaissance and counter-intelligence activities"* issued by the Ministry of Transport, Communications and High Technologies on June 14, 2016.[18] The Rule obligates telecommunication operators and providers to create technical conditions for the conduct of relevant activities within the communication networks.

---

[12] According to article 7 of the *Law on Personal Data,* individuals have the rights to require a legal justification for the collection, processing and transfer of their personal information to third parties, and information on the legal consequences for the subject of the collection, processing and transfer of such information to third parties; to get acquainted with the content of personal information collected about himself/herself in the information system; to learn the purpose, the period and methods of collecting and processing personal information about himself/herself; to demand clarification and destruction of personal data collected and processed in the information system, except for the cases established by the legislation; to demand a ban on the collection and processing of personal data about himself/herself and etc.

[13] Law on Private Data, http://e-qanun.az/framework/19675

[14] Article 10.5, Law on Personal Data

[15] Article 39, Law on Telecommunication (article 10.5 of the Personal Data is repeated in the article 39 of the Law on Telecommunication)

[16] Article 10, Law on Operation-Search Activity, http://e-qanun.az/framework/2938

[17] Under the Telecoms Law and the conditions of telecom licencing and registration, telecom operators and providers must cooperate with the law enforcement authorities and install special equipment and software programme allowing them access to information under the undisclosed technical rules adopted by the Presidential order on October 2, 2015. The Law on Telecommunication, article 39., Paragraph 1 of the article states: "operators, providers are obliged to create conditions for conducting search operations, intelligence and counter-intelligence activities in accordance with the law; to provide telecommunications networks with additional technical means in accordance with the conditions established by the relevant executive authority; to resolve organizational issues; and to keep secret the methods used in conducting these events." Paragraph 2 of the article states: "The operator, the provider shall be liable for the violation of these requirements in accordance with the law."

[18]

http://e-qanun.az/framework/33275

The Rule defines that Telecommunication Control System (hereinafter - TCS) - is a special hardware and software that provides confidential control over the exchange of information of subjects *targeted by the relevant measures* (such as search and operation, intelligence and counter intelligence activites), as well as all statistical data of the network. TNS consists of data extraction facilities, transport network, and control centres.

The Rule also indicates that relevant measures in the communication networks are carried out in accordance with the requirements of the laws of the Republic of Azerbaijan "On Operation-Search Activity" and "On Intelligence and Counterintelligence Activity".[19]

However, while *the* Law *on Operation-Search Activity* may allow secret surveillance and seizure of private information, there are no rules or procedures within the national legislation for secret surveillance and intercepting information by government agencies. There are also no clearly defined rules on determining the grounds for such surveillance and interception activities, their duration, and whether such activities can be stopped by a court or other higher state authority.

Further, when analysing the national legislation, it becomes clear, that a number of rules about organization of search operations by law enforcement agencies, as well as the placement of surveillance and tapping devices within the telecommunication infrastructure have not been published. For example, the "Rules for ensuring information security in the implementation of search operations in communications networks" approved by the Presidential Decree No. 638 on October 2, 2015, is not disclosed.[20]

As mentioned, earlier, interference with the right to personal data within telecommunication networks is carried out by the representatives of the search and operation, intelligence, and counterintelligence authorities. The technical and organizational conditions for the provision of search operation, intelligence and counterintelligence activities within communication networks are determined by the State Security, and in cases where relevant to the Ministry of Internal Affairs, together with the Special State Protection Service of Azerbaijan.

Infringement of privacy is prohibited under the Criminal Code (Article 156). Illegal collection of information, documents containing such information, visual materials, audio recordings, as well as their sale or transfer to another person is punishable by a fine in the amount of 1,000 to 2,000 AZN (approximately 600-1200USD); by public works ranging from 240 to 480 hours; or by correctional labor for up to one year. In cases where the same offense was/is committed by an official using his/her official status, the crime is punishable by restriction of liberty for a period of up to two years or by imprisonment for a term of up to two years with or without deprivation of the right to hold a certain position or engage in certain activities for up to three years.[21]

The Criminal Procedural Code provides that the investigation of the infringement of privacy ais carried out in the form of a public-private prosecution upon the complaint of the victim or by the initiative of the prosecutor when the committed crime affects the interests of the state or society.[22]

Compliance with international standards

The right to protection of personal data is not an autonomous right among various rights and freedoms covered by the Convention. The Court has nevertheless acknowledged that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, home and correspondence, as guaranteed by Article 8 of the Convention (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], 2017, § 137; Z v. Finland, 1997, § 95).

---

[19] Article 1.5.7. "Rules for equipping telecommunications operators and providers with additional technical means for conducting search operations, reconnaissance and counter-intelligence activities", issued by the Ministry of Transport, Communications and High Technologies, June 14, 2016

[20] The Presidential Decree No. 638, October 2, 2015, http://e-qanun.az/framework/30840

[21] The Criminal Code of Azerbaijan, http://e-qanun.az/framework/46947

[22] The Criminal Procedure Code of Azerbaijan, http://e-qanun.az/framework/46950

According to the Court's established case-law, the requirement that any interference must be "*in accordance with the law*" will only be met when three conditions are satisfied: the impugned measure must have some basis in domestic law and, with regard to the quality of the law at issue, it must be accessible to the person concerned and have foreseeable consequences.[23]

Non-availability of any official information or confirmation on the scope and form of the surveillance and interception of mobile devices through the Pegasus spyware may also raise specific issues concerning the difficulties on recognizing the victims' status within the framework of national laws.

However, relevant case-law of the ECtHR is relatively flexible on the subject of recognition of the victim's status. The ECtHR therefore accepts that an individual could, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures had been in fact applied to him or her.[24]

Further, considering that domestic legislation does not require any judicial act or does not provide any independent oversight over the interferences to right to privacy, there is little information about the form and scope of the interception and surveillance of individuals' privacy within telecommunications networks in Azerbaijan. This is also contrary to the well-established standards of the ECtHR concerning the issue of personal data collection by means of various methods of secret surveillance. The fact that various government institutions are vested with powers and authority – as provided by domestic laws -- to listen to anyone at any time on telecommunication networks, in itself does not meet the requirements of the qualitative law enshrined in the case-law of the European Court.

The ECtHR considers the requirements of the Convention, notably in regard to foreseeability, to not be exactly the same, in the special context of interception of communications for the purpose of police investigations.

According to the ECtHR case law, the Convention's "quality of law" concept, requires, that domestic laws - notably those allowing state interference with rights and freedoms - satisfy the requirements that domestic laws, should be sufficiently accessible and foreseeable.

The requirement of foreseeability means that the national law must be sufficiently clear in its terms, in order to give citizens an adequate indication on the circumstances and conditions for which public authorities were empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, and to give the individual adequate protection against arbitrary interference (Malone v. the United Kingdom, 2 August 1984, §§ 67 and 68, Series A no. 82. See also Kennedy v. the United Kingdom, op. cit., § 152).[25]

As a result, Azerbaijani law enforcement agencies under the criminal procedure code, (as discussed avove) should open a criminal investigation into the interception of the personal data of those targeted through the Pegasus spyware, in line with national law. Individuals identified so far in the Pegasus Project may be required to open and prosecute the relevant criminal case and seek compensation for the material or moral damage caused to them. But the past experience has shown that local remedies in these matters are not effective in convincing investigation, prosecution and demanding for a compensation.

---

[23] Kennedy v. the United Kingdom, op. cit., § 151; Rotaru v. Romania, op. cit., §52; Amann v. Switzerland, op. cit., § 50; Iordachi and Others v. Moldova, op. cit.; Kruslin v. France, § 27; Huvig v. France, § 26; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, op. cit., § 71 ; Liberty and Others v. the United Kingdom, op. cit., § 59, etc.

[24] National security and European case-law, Council of Europe / European Court of Human Rights, 2013, para., 9., https://rm.coe.int/168067d214

[25] National security and European case-law, Council of Europe / European Court of Human Rights, 2013, page 2, https://rm.coe.int/168067d214

In this regard, within the framework of the European Court's supervision function under the Convention's standards, the ECtHR's authority to verify the compliance of online surveillance regimes with the Convention's standards would provide effective protection.

In recent Grand Chamber judgment in the case of Big Brother Watch and Others v. the United Kingdom (application nos. 58170/13, 62322/14 and 24969/15) the ECtHR held unanimously, that there had been a violation of Article 8 of the European Convention (right to respect for private and family life/communications) in respect of the regime for obtaining communications data from communication service providers noting that assessment of interceptions and obtaining of private information from the telecommunications networks should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorization at the outset when the object and scope of the operation were being defined; and that the operation should be subject to supervision and independent ex post facto review.

We conclude, that based on the above analysis of the loose interpretation and at times overt national legislation, it is important to take these cases of surveillance and interception to the ECtHR for the purpose of assessing the country's legal framework and its (in)applicability with the ECtHR's case law.