PEGASUS SPYWARE

and its impacts on human rights

Information Society Department
DGI(2022)04

Authors:
Tamar Kaldani
Zeev Prokopets

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Layouts and Cover Page:
Information Society Department
Council of Europe

Images: Shutterstock

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors.

PEGASUS SPYWARE

and its impacts on human rights

Authors:

Tamar Kaldani
Introduction and Impacts Chapters

Zeev Prokopets
Mobile phones surveillance and spyware and Basic rules for better protection Chapters

Council of Europe

Contents

Abbreviations and shortenings

CoE	Council of Europe
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)
Convention 108+	Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223)
Court	The European Court of Human Rights
ECHR	The European Convention on Human Rights
EU	The European Union
PACE	The Parliamentary Assembly of the Council of Europe
UN	The United Nations

Introduction

Digital transformation and innovations in communication technologies enhanced connectivity, inclusion and access to services and concurrently have also increased opportunities for State surveillance and interference into individuals' human rights and fundamental freedoms. Recent revelations on the deployment of Pegasus spyware, including in a number of Council of Europe (CoE) states targeting journalists, human rights defenders and politicians have raised a significant public outcry. Usage of such an intrusive technology not only adversary affects the effective enjoyment of the right to privacy and freedom of expression but also the notion of personal autonomy and even the physical integrity of individuals. The surveillance practices disclosed so far could also damage the very principle of the rule of law and credibility of democratic institutions.

Concerns about national security and criminal activities may justify the exceptional use of communications surveillance technologies. Law enforcement and intelligence services have legitimate aims to obtain necessary information, including through wiretapping and metadata analysis or covertly directly from mobile devices, to prevent, investigate and prosecute crime or combat threats related to national security. However, the State's margin for appreciation even "in the area of national security is no longer uniformly broad'.[1] States are bound by international[2], regional[3], and national human rights instruments. As a corollary to the European Convention on Human Rights (ECHR) and relevant case law of the European Court of Human Rights, member States have negative obligations, that is, to refrain from interference with fundamental rights and positive obligations, that is, to actively protect these rights. This includes the protection of individuals from action by non-state actors as well.[4]

[1] Council of Europe / European Court of Human Rights, National Security and European Case-Law, 2013, page 2 - 168067d214 (coe.int)

[2] Such as Universal Declaration of Human Rights and International Covenant on Civil and Political Rights

[3] Such as the African Charter on Human and Peoples' Rights or the Inter-American human rights instruments and system.

[4] Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies), Paragraph 4.

Wide-scale usage of communication tapping, and secret surveillance always create the room for potential arbitrariness on behalf of state authorities, threatening the effective enjoyment of number of rights and fundamental freedoms, including the right to respect to private and family life and communication (Article 8 of the ECHR) and freedom of expression (Article 10). The consequences of mass or targeted surveillance tools such as Pegasus in authoritarian regimes could be catastrophic. High-technology surveillance tools are already in use in a number of authoritarian regimes and are used to track down opponents and to suppress freedom of information and expression.[5] Therefore, the development and deployment of surveillance technologies must be accompanied by decent and effective legal safeguards that ensure adequate protection for individuals and a fair balance between all interests concerned and the rights and freedoms at stake.

Unfortunately, the Pegasus spyware scandal is not the first revelation on mass surveillance and the use of intrusive technologies as espionage weapons against journalists, human rights defenders, and politicians. Both large-scale and targeted intrusion practices undermine the trust in state authorities allegedly using surveillance tools to target people against whom there is no ground for suspicion of any wrongdoing and present substantial dangers to democracy and the rule of law.

Allegations of arbitrary surveillance pertaining to a leaked list featuring more than 50,000 phone numbers, which was accessed by Forbidden Stories[6] and Amnesty International[7] in 2021, and recent alerts[8] indicating widespread use of the Pegasus spyware across the world, have triggered the launch of investigations and legal proceedings in a number of jurisdictions.

[5] PACE Resolution 2045 (2015) on Mass surveillance, paragraph 8.

[6] https://forbiddenstories.org/case/the-pegasus-project/

[7] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[8] See as an example: https://www.politico.eu/article/europe-pegasus-spyware-eu-probe-nso/ https://www.euronews.com/next/2022/05/02/pegasus-spyware-spain-s-prime-minister-and-defence-minister-s-phones-infected-by-spying-so

https://www.frontlinedefenders.org/en/statement-report/report-jordanian-human-rights-defenders-and-journalists-hacked-pegasus-spyware

https://www.hrw.org/news/2022/01/26/human-rights-watch-among-pegasus-spyware-targets

In March 2022 European Parliament established a new Committee of inquiry to investigate the compliance of usage of Pegasus and other surveillance spyware with EU law and fundamental rights.[9] The Committee will call for relevant documents and seek testimony from numerous stakeholders, including Member States' intelligence services, elected politicians, and senior officials. Within 12 months, the Committee is expected to present recommendations for further action to be taken by the European Commission and national governments.[10] Speaking to the PACE Committee on Legal Affairs and Human Rights on the 14th of September 2021, the UN high commissioner for human rights asked states to place a moratorium on the sale of such technology and "rein in the surveillance industry".[11]

The present report is developed for the CoE. It explains how Pegasus spyware works and analyses the impact on human rights and fundamental freedoms, in particular the right to privacy and freedom of expression. Furthermore, the report underlines the chilling effect that Pegasus spyware has or potentially could have on other human rights and fundamental freedoms, including the right to dignity, freedom of assembly, freedom of religion, and even the physical and psychological integrity of an individual. The report places a special emphasis on the legal instruments and well-established standards that the CoE has at its disposal to uphold fundamental rights and ensure stronger protections against mass or targeted unlawful and unjustified surveillance. The report also provides basic rules of thumb for better protection to minimise potential exposure not only to Pegasus but also to other malicious attacks.

https://scroll.in/latest/1022972/pegasus-case-supreme-court-panel-seeks-response-from-dgps-of-all-states-on-spyware-purchase

https://citizenlab.ca/tag/nso-group/

[9] Press release on the launch of the EP inquiry committee - https://www.europarl.europa.eu/news/en/press-room/20220412IPR27112/ep-inquiry-committee-for-pegasus-and-other-spyware-launched

[10] https://www.aldeparty.eu/renew europe welcomes the inquiry committee on pegasus spyware scandal

[11] Speech of the UN high commissioner for human rights - https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe

1. Mobile phones surveillance and spyware

In the last few decades, governments and associated agencies have invested enormous efforts and substantial funds to ensure they can hack into every telecom network and device. National security agencies used to have agreements with technology vendors under which the companies would give the agencies special access to their products via backdoors. Some of these agreements are still intact. Recently, awareness of digital security and privacy is rising (Edward Snowden's revelations about mass U.S. government surveillance was the first wakeup call) and major companies no longer willing to provide governments with backdoors.

Companies like Apple (and many others) invest record budgets in security, develop features like end-to-end encryption (and others) and put expert engineering teams to continuously work on identification and timely fixes of security vulnerabilities. There are also bug-bounty programs in which companies invite hackers to break into their products. These programs offer quite attractive rewards for the detection of zero-day vulnerabilities,[12] which can go up to $100,000, and the problem is that zero-day vulnerabilities worth millions on the black market.

These developments left governments unable to listen in, and desperate for a solution. The needs of these governments and their virtually unlimited budget created an "industry" and a market, in which hackers are continuously looking for exploitable vulnerabilities and vendors are tirelessly working on fixing those same issues. The hackers that find the vulnerabilities sell this information either to the vendors or to the highest bidder on the black market, the buyers on the black market are the organisations that create spyware and then sell it to governments and sometimes to other organisations.

This market is no different from any other market and is essentially driven by demand and supply, as long as the demand is there (and actually growing) the supply will follow, and there will always be someone to provide the goods. One of the most successful (and therefore notorious) suppliers is NSO group, an Israeli spyware vendor and the creator of Pegasus. Pegasus is a spyware that can be stealthily installed on a smartphone and gain access to everything on it, including its camera and microphone. Pegasus is designed for devices

[12] Zero-day vulnerabilities are exploitable vulnerabilities that the vendor is not aware of, and therefore, there are no patches or fixes available or underway.

running Android, iOS, Windows, Blackberry and Symbian operating systems and turns them into surveillance devices. NSO says it sells Pegasus only to governments and only for the purposes of tracking criminals and terrorists.

How it works

The Pegasus spyware can infect the phones of targets through a variety of mechanisms. Some approaches may involve a message (SMS, iMessage, WhatsApp, email) that includes a link to a website. When clicked, this link delivers malicious software that infects the device.

Others use the zero-click attack or zero-click exploit where vulnerabilities in messaging services for example allows for infection by simply receiving a message, while no user interaction is required.

Apart from zero-click exploits, Pegasus uses “network injections”. A target’s web browsing can leave them open to attack without the need for them to click on any malicious link. This approach involves waiting for the target to visit a website that is not fully secured during their normal online activities. Once they visit an unprotected site, the injection software can intercept the transaction and trigger an infection.

However, this technique is more difficult to carry out than attacking a phone using a malicious URL or a zero-click exploit, since the target’s cellphone use must be monitored until the moment at which its internet traffic is unprotected. This is normally done through the target’s mobile operator, which some governments can access or control. This reliance makes it difficult or impossible for governments to target people outside their jurisdiction. Zero-click exploits have no such limitations.

On top of these mechanisms, there is also a manual option, if an agent is able to gain physical access to the target’s phone, the spyware can be installed manually. In all approaches, the goal is to get full control of the mobile device’s operating system, either by rooting (on Android devices) or jailbreaking (on Apple iOS devices).

Usually, rooting on an Android device is done by the user to install applications and games from unsupported sources, or enable functionality that was blocked by the manufacturer.

Similarly, a jailbreak can be deployed on Apple devices to allow the installation of apps not available on the Apple App Store, or to unlock the phone for use on alternative cellular networks.

Rooting and jailbreaking both remove the security controls embedded in Android or iOS operating systems and eventually allows the OS to run modified code.

In the case of spyware, once a device is unlocked, the intruder can deploy further software to secure remote access to the device's data and functions. The user is likely to remain completely unaware, unless noticeable misbehaviors occur (see Tells of infection).

Earlier versions of Pegasus were installed on smartphones through vulnerabilities in commonly used apps or by spear-phishing, which involves tricking a targeted user into clicking a link or opening a document that secretly installs the software.

Since 2019, Pegasus users have been able to install the software on smartphones with a missed call on WhatsApp and could even delete the log of the missed call, making it impossible for the phone's owner to know anything ever happened. Another way was by simply sending a message to a user's phone that produces no notification. Both of these specific vulnerabilities were fixed shortly after the discovery; however, new undiscovered vulnerabilities keep the zero-click exploit alive and kicking.

This means the latest version of this spyware does not require the smartphone user to do anything. All that is required for a successful spyware attack is having a particular vulnerable app or operating system installed on the device.

Implications

Once installed, Pegasus can theoretically harvest any data from the device and transmit it back to the attacker. Pegasus can run any code it desires on the target's device, use device's camera and mic by remote commands in real time, extract contacts, call logs, web searches, web browsing history, text messages, photos, videos, settings, location records, as well as information from apps such as iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram, Skype and others.

Pegasus also monitors the keystrokes on an infected device, all written communications, including passwords are visible to the attacker.

Tells of infection

If you have a reason to believe you are being monitored, here is a list of “tells” that might suggest your phone is infected:

1. Your phone suddenly becomes slower than usual.
2. Your phone occasionally shuts down by itself.
3. You need to charge your phone’s battery more often than usual.
4. You find unusual and unfamiliar folders or files on your device (mostly Android).
5. You’re often redirected to unknown sites.
6. Excessive pop-up ads appear while browsing.
7. Sudden increase in data usage.
8. Your phone has new/unfamiliar applications installed.

If you notice some of these behaviors on your phone, the relatively easy way to determine if your phone is infected is to use the Amnesty International Mobile Verification Toolkit (MVT). This tool can run under Linux or MacOS and can examine the files and configuration of your mobile device by analysing a backup taken from the phone.

While the analysis won’t confirm or disprove whether a device is compromised, it detects indicators of compromise, which usually provide enough evidence of infection.

In particular, the tool can detect the presence of specific software processes running on the device, as well as a range of domains used as part of the global infrastructure supporting the spyware network.

2. Impact on the Right to Privacy

As described above and according to the product description,[13] the use of Pegasus does not require cooperation with telecommunication companies, and it can easily overcome encryption, SSL, proprietary protocols, and any hurdle introduced by the complex communications worldwide. It enables monitoring of the voice and VoIP calls in real-time. It provides remote, covert, and unlimited access to the target's mobile devices and thus their relationships, virtual identities, location, phone calls, text and voice messages, emails, photos, videos, and other files, contacts, passwords, environmental wiretap, plans and activities that reveal most sensitive information (*inter alia* about health, sexual life, political opinion, religious or other beliefs) not only about the targeted individuals but also their children and family members, colleagues, friends, clients, beneficiaries and other contacts.

This Modus Operandi of the Pegasus clearly reveals its capacity to be used for targeted as well as indiscriminate surveillance. This is a prima facie interference with Article 8 of the ECHR and undermines standards and approaches[14] established by the European Court in its extensive case law related to targeted communication surveillance and indiscriminate/bulk interception of communication data.

First and foremost, any interference in privacy can only be justified under Article 8.2 if it:

a) is in accordance with the law, which should be accessible, foreseeable, precise and sufficiently clear concerning rules, circumstances and conditions on which the surveillance is authorised and carried out. Law must also provide adequate and effective guarantees and supervision to prevent abuse and effective remedies for individuals in case of abuse;[15] The law must also be compatible with the principle

[13] Pegasus product description is available at: https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf

[14] See also most recent cases: Big Brother Watch and Others v. the United Kingdom [GC], no. 58170/13, 25 May 2021; Centrum för rättvisa v. Sweden, [GC], no. 35252/08, 25 May 2021;

[15] See also Roman Zakharov v. Russia [GC], no. 47143/06, 4 December 2015; Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016; Iordachi and Others v. the Republic of Moldova, no. 25198/02, 10 February 2009; Rotaru v. Romania [GC], no. 28341/95, 4 May 2000; Kennedy v. the United Kingdom, no. 26839/05, 18 May 2010; Association of European Integration and Human Rights and Ekimdzhiev v. Bulgaria, no. 62540/00, 28 June 2007.

of the rule of law, which is expressly mentioned in the Preamble to the ECHR and inherent in the object and purpose of Article 8.

b) pursues one or more of the legitimate aims to which Article 8.2 refers *inter alia* national security, public safety … the prevention of disorder or crime,… ….". The notion of national security should be clearly interpreted by domestic law and provide the scope of crimes/offences threatening the national security as well as other severe or exceptionally severe crimes allowing authorities to use secret surveillance measures to effectively prevent/investigate those crimes.

c) is necessary in a democratic society in order to achieve legitimate aims. State authorities are under an obligation to ensure effective mechanisms (including national courts, supervisory/monitoring mechanisms, public scrutiny) for avoiding arbitrariness and securing a fair balance between the right to privacy and the legitimate aim pursued by the interference. The strict necessity should only be confirmed if the envisaged action is suitable to protect/preserve objectively a democratic institution and subjectively is also susceptible to produce vital intelligence in/for an ongoing investigation

In the cases of Roman Zakharov v. Russia and Szabó and Vissy v. Hungary, the Court also noted that where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The Court was firm in reiterating its standards established in earlier case law on the subject matter that in order to effectively assess the necessity and reasonableness of any intrusion in the private life or communication, any communication tapping or secret surveillance should be authorized by an independent and impartial domestic authority being vested with the relevant mandate. The authorisation authority's must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security. It must also ascertain whether the requested interception meets the requirement of "necessity in a democratic society," as provided by Article 8.2 of

the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example, whether it is possible to achieve the aims by less restrictive means.[16] When it comes to targeted communication tapping, the Court has developed the following minimum requirements[17] that should be set out in domestic law in order to avoid abuses of power:

(i) the nature of offences which may give rise to an interception order;

(ii) a definition of the categories of people liable to have their communications intercepted;

(iii) a limit on the duration of interception;

(iv) the procedure to be followed for examining, using and storing the data obtained;

(v) the precautions to be taken when communicating the data to other parties; and

(vi) the circumstances in which intercepted data may or must be erased or destroyed.

In the case of Roman Zakharov v. Russia, the Court confirmed that the same six minimum safeguards also applied in cases where the interception was for reasons of national security; however, in determining whether the impugned legislation was in breach of Article 8, the Court also had regard to the arrangements for:

a) supervising the implementation of secret surveillance measures, any notification mechanisms and

b) the remedies provided for by national law.

As to the approach of the Court in recent case law related to bulk interception,[18] the Court considers that the process must be subject to "end-to-end safeguards" to minimize the risk of the bulk interception power being abused, meaning that, at the domestic level, an

[16] See also Klass and Others v. Germany, no.37138/14, 6 September 1978

[17] See also cases of Huvig v. France, no 11105/84, 24 April 1990; Kruslin v. France, no 11801/85 24 April 1990; Valenzuela Contreras v. Spain, no. 27671/95, 30 July 1998, Weber and Saravia v. Germany no. 54934/00, 29 June 2006.

[18] See for example, Big Brother Watch and Others v. the United Kingdom [GC], no. 58170/13, 25 May 2021/

assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken and to the legitimate aim pursued; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In that regard, particular emphasis was placed by the Court on clearing and approving the selectors used by the authorities during bulk interception by national courts or independent bodies vested with the relevant mandate. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime.[19]

Along with Article 8 of the ECHR, European Court judgments, Resolutions of the Parliamentary Assembly, including Resolution 2045 (2015) on Mass Surveillance[20], and Declarations[21] and Recommendations[22] of the Committee of Ministers, Convention 108[23] - the only legally binding international treaty in the data protection field with global relevance[24], sets the basic principles for data protection, safeguards for individuals, and supervision over the data processing operations, which are particularly important in the context of Pegasus or other surveillance technologies.

Although the right to the protection of personal data is not an autonomous right among the various Convention rights and freedoms, the European Court has 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. Article 8 is the main vector through which personal data is protected in the Convention system, even though

[19] See also the report of the Venice Commission, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process - https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e

[20] http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692

[21] See for example Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168068460

[22] See for example Recommendations No. R (87) 15 Regulating the use of personal data in the police sector https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804e7a3c

[23] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

[24] Convention 108 is ratified by 55 parties, including 9 non-Council of Europe members.

considerations related to this protection may also come into play under other provisions of the Convention and its Protocols.[25]

Modernised Convention 108+ opened for signatures and ratifications in October 2018, reaffirmed the importance of the original principles and laid down new ones, including transparency, accountability, privacy by design and data protection impact assessment that are particularly relevant in the context of Pegasus spyware. Convention 108+ requires improved data quality, increased protection for sensitive data, high level data security, greater fairness, transparency and accountability from public authorities and private companies, including developers and service providers, who should proactively demonstrate compliance with the data protection rules. It establishes stronger requirements regarding the lawfulness of the processing, proportionality, purpose limitation and data minimisation, recalling that data processed should be adequate, relevant, and not excessive. The proportionality principle also applies in respect of the means and methods deployed during the surveillance.

The Convention 108+ empowers individuals with stronger control over their data and enhanced rights. Along with other obligations, data controllers must implement the "privacy by design" in product or service development as well as examine prior the likely impact of data processing on human rights and fundamental freedoms.

It is important to recall that parties to the Convention 108+ will no longer be able to exclude from the scope of application of the Convention certain types of processing such as national security and defence. The possible exceptions to a limited number of principles such as transparency are subject to the conditions set by the Convention, and in any case, independent and effective review and supervision should be guaranteed. The Convention 108+ also reinforces investigative and corrective powers and the independence of the data protection authorities. It also enhances their international cooperation and opportunities for joint actions and investigations, including against unlawful and unjustified usage of sophisticated surveillance technologies.

[25] Guide to the Case-Law of the of the European Court of Human Rights – Data Protection, First edition - 31 December 2020, page 4. Guide to the Case-Law - Data protection (coe.int)

In order to protect individuals and the society as a whole from unlawful interference with human rights and notably with the right to privacy the standards established by Convention 108+ could as of now be used and implemented by state authorities carrying out similar activities.

3. Impact on the Freedom of Expression

An investigation report released by a global consortium[26] revealed that 200 journalists worldwide had been targeted using Pegasus spyware. The Office of the UN Special Rapporteur for Freedom of Expression also noted the number of victims of attempted spying through Pegasus, including Mexican journalists, human rights defenders and opposition leaders.[27] "The numbers vividly show the abuse is widespread, placing journalists' lives, those of their families and associates in danger, undermining freedom of the press and shutting down critical media," - said Secretary-general of Amnesty International.

The right to freedom of expression and information, as guaranteed by Article 10 of the Convention, constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and the development of every individual. Freedom of expression is applicable not only to "information" or "ideas" that are favorably received or regarded as inoffensive or as a matter of indifference but also to those that offend, shock or disturb the State or any sector of the population. Any interference with the right to freedom of expression of journalists and other media actors therefore has societal repercussions as it is also an interference with the right of others to receive information and ideas and an interference with public debate.[28]

While the right to freedom of expression is not absolute, an interference with this right is only permitted if it is prescribed by law, pursues one of the legitimate aims set out in Article 10,

[26] https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

[27] Press release R303/21 https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1218&lID=1

[28] Recommendation CM/Rec(2016) 4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors - https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415d9#_ftn1

paragraph 2 of the Convention, is necessary in a democratic society – which implies that it corresponds to a pressing social need – and is proportionate to the legitimate aims pursued.

The surveillance of journalists and other media actors, and the tracking of their online activities, can endanger the legitimate exercise of freedom of expression if carried out without the necessary safeguards. They can also threaten the safety of the persons concerned and undermine the protection of journalists' sources. In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain adequate and effective safeguards against abuse, including independent supervision, since such systems designed to protect national security entail the risk of undermining or even destroying democracy on the ground of defending it.[29]

The European Court has always subjected the safeguards for respect of freedom of expression in cases under Article 10 of the ECHR to special scrutiny. The safeguards to be afforded to the press are of particular importance, and the protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the media in informing the public about matters of public interest. As a result, the vital public watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information may be affected adversely.

Allegations revealed that Pegasus was used to target journalists and their confidential sources. This has a detrimental impact not only for confidential sources and whistle-blowers but also on the media outlets, whose reputation could be negatively affected in the eyes of future potential sources, and on members of the public, who have an interest in receiving information imparted through anonymous sources.

The European Court in a number of decisions[30] has addressed the risks related to bulk interception through a strong selector connected to journalists. The Court considered that such interference will be commensurate with that occasioned by the search of a journalist's home or workplace; regardless of whether or not the intention is to identify a source, the use of selectors or search terms connected to a journalist would very likely result in the acquisition

[29] Ibid

[30] See, inter alia, Goodwin v. the United Kingdom, no.17488/90, 27 March 1996; Sanoma Uitgevers B.V. v. the Netherlands [GC], no. 38224/03, 14 September 2010.

of significant amounts of confidential journalistic material which could undermine the protection of sources to an even greater extent than an order to disclose a source. Therefore, in the case of Big Brother and others v. the United Kingdom[31] the Court considered that before the intelligence services use selectors or search terms known to be connected to a journalist, or which would make the selection of confidential journalistic material for examination highly probable, the selectors or search terms must have been authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether they were "justified by an overriding requirement in the public interest" and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest. Court also noted that even where there is no intention to access confidential journalistic material, and the selectors and search terms used are not such as to make the selection of confidential journalistic material for examination highly probable, there will nevertheless be a risk that such material could be intercepted, and even examined, as a "bycatch" of a bulk interception operation.

4. Impact on Human Rights Defenders

Along with journalists, Pegasus revelations confirm that human rights defenders are one of the key targets being subjected to secret surveillance. Various international[32] and civil society organizations expressed deep concerns towards targeting, intimidating, and retaliating against human rights defenders and called to provide a safe and enabling environment and ensure their protection, which, among other recommendations, called on States to refrain from using surveillance technologies to target human rights defenders. [33]

Surveillance technologies are often used to target human rights defenders to dissuade them from continuing their human rights work, to infiltrate their networks, and to gather information for use against other targets. Intrusion with the privacy of human rights

[31] Ibid

[32] Resolution adopted by the General Assembly on 16 December 2021 on the Seventy-sixth session, on the report of the Third Committee (A/76/462/Add.2, para. 114)] 76/174. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/403/46/PDF/N2140346.pdf?OpenElement

[33] https://www.frontlinedefenders.org/en/statement-report/action-needed-address-targeted-surveillance-human-rights-defenders

defenders negatively affects not only the personal privacy of the individuals but threatens to pose the harm to their inner and outer circle, compromise their dignity and reputation, and expose them, their family members and beneficiaries to the greater risks of threats, aggression and violence.

A digital forensic investigation carried out by Front Line Defenders and Citizen lab has uncovered specific gender-related dangers. Pegasus spyware on the mobile devices of four Jordanian human rights defenders, including a woman human rights defender, lawyer and journalist working against corruption.[34] Another set of cases of hacking of two women human rights defenders from MENA region using Pegasus spyware was identified by Access Now and Front Line Defenders.[35]

The impact of targeted surveillance on women can be given that political, societal, and gender power asymmetries often grant authorities opportunities to weaponize the information they extract through defamation, blackmail, and doxing. This can include the publishing of private and intimate photos and conversations online.[36] As a result, women, targets of surveillance, live in a perpetual state of fear and become socially isolated and restricted in their social lives, work, and activism. As expressed by one of the victims - "personal freedoms are over for me, they no longer exist. I am not safe at home, on the street, or anywhere."[37]

5. Impact on other Human Rights and Fundamental Freedoms

Human rights and fundamental rights are interconnected and mutually reinforcing. Therefore, intrusive surveillance technologies have a chilling effect on other human rights and fundamental freedoms and not only on the right to privacy and freedom of expression.

[34] https://www.frontlinedefenders.org/sites/default/files/jordanpegasusreport.pdf

[35] https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/

[36] Ibid

[37] https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

For example, the right to health may also be affected by digital surveillance practices as individuals may refrain from sharing sensitive health-related data with health professionals, fearing that confidentiality could be compromised. Freedom of religion could also be impacted, especially if the seal of confession and privileged communication with religious ministers are intercepted. Individuals could also refrain from exercising their right to freedom of assembly and association with others, including the right to form or join a not-for-profit organization with political, philosophical, religious or trade union aims.

Targeted or mass surveillance also creates a climate of self-censorship. Fearing that each action and move is under scrutiny, people will be less likely to communicate about specific topics online or offline. The chilling effect of surveillance could also lead to social isolation. Targets, as well as their relatives and friends, might refrain from interactions in fear of being harmed or surveilled**.** More importantly, real-time access to location and communication data could also pose a life-threatening risk to the individual and endangers its physical and mental integrity.

The growing concerns about the politically motivated use of spyware, followed by the reports about the arbitrary detention, torture, and possibly even extrajudicial killings of political opponents, journalists and human rights activists[38] call for immediate, thorough, effective and independent investigations and strengthened legal safeguards, including independent, impartial, and effective supervisory mechanisms. Civil society organisations also call for a moratorium on the sale, transfer and use of Pegasus until compliance with human rights standards can be guaranteed. They urge states to implement legislation that imposes safeguards against human rights violations and abuses through digital surveillance and establishes accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy.[39]

[38] https://www.amnesty.org/en/documents/doc10/4516/2021/en/

[39] Ibid

6. Basic rules of thumb for better protection

There are no absolute solutions, especially when facing zero-click exploits. There are, however, measures you can take to minimise your potential exposure — not only to Pegasus but to other malicious attacks as well.

1. There are indications that infections, in some cases (mostly on Apple devices) were not persistent, meaning did not survive phone reset, but were re-introduced (as zero-click exploits) as needed. This means that frequent reset of your phone may remove non-persistent malware, at least temporarily.
2. Only open links from known and trusted contacts. Pegasus and other malware use iMessage and SMS to send links that lead to the download and installation of the spyware. The same applies to links sent via email or other messaging applications. Especially avoid “unsubscribe” links from suspicious sources, as one of the known methods is to send spam messages just to frustrate the target, then send another message telling them to click unsubscribe to stop receiving the spam. Many targets cheerfully click the unsubscribe link, which causes the actual infection.
3. Make sure your device is updated with the most recent software. These updates often include bugs and security vulnerabilities fixes. If you use Android, don’t rely on notifications for available updates, check for the latest version yourself, as your device’s manufacturer may not be providing updates.
4. As obvious as it may sound, you should limit physical access to your phone by enabling pin, finger or face-ID on the device.
5. As much as possible, avoid public and free WiFi services (including hotels). If you must use public WiFi, use VPN while on the public network and avoid accessing sensitive information.
6. Encrypt your device data and enable remote-wipe features where available. If your device is lost or stolen, your data still remain safe.
7. When communicating using end-to-end encrypted messaging apps, turn on disappearing messages.

8. Where possible, do not use your personal or work devices, SIM cards and email account to contact sensitive sources. If possible, buy devices and SIM cards and create a new email account specifically for communicating with them.
9. Your device can be used to locate you and your confidential source. If meeting in person, leave your phones behind and meet in a neutral location (noting the possibility of being monitored via CCTV) that cannot be associated with your or your source's home or work address.
10. Remove metadata from sensitive files and photos before sharing them with others. A file's metadata can provide information about the person who created or sent it and the device used.

ANNEX: More about NSO and Pegasus

- NSO group is an Israeli company, regulated by the Israeli government. Officially NSO group states that it sells only to government agencies, only to preapproved countries, and only for counterterrorism and law enforcement use.
- Countries which are known users of Pegasus (partial list): Mexico, the first NSO customer, used Pegasus back in 2011 to track notorious drug baron Joaquín "El Chapo" Guzmán, United Arab Emirates, Saudi Arabia, Spain, Poland, Panama, Netherlands, Morocco, India, Israel, Germany, Hungary, Bahrain, Azerbaijan, Armenia.
- The price point of Pegasus is quite high: an indication from 2016 suggests a $600K annual fee on top of a $500K setup fee for a system capable of tracking 10 targets simultaneously.
- NSO group 2020 revenue was $243M

This report provides a technical description of the Pegasus spyware and analyses the impact it may have on human rights and fundamental freedoms, in particular the right to privacy and freedom of expression. Furthermore, the report underlines the chilling effect that Pegasus spyware has or potentially could have on other human rights and fundamental freedoms, including the right to dignity, freedom of assembly, freedom of religion, and even the physical and psychological integrity of an individual. The report places a special emphasis on the legal instruments and well-established standards that the CoE has at its disposal to uphold fundamental rights and ensure stronger protections against mass or targeted unlawful and unjustified surveillance. It also provides the basic rules of thumb for better protection for individuals.

Tamar Kaldani has served as the Personal Data Protection Inspector and the State Inspector of Georgia and is currently the first Vice-chair of the Consultative Committee of Convention 108.

Zeev Prokopets is an Israeli executive, product designer, software developer and entrepreneur (Link7).

www.coe.int

The **Council of Europe** is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE