BACKGROUND BRIEFING

Requested by the PEGA committee

European Parliament

Briefing for the PEGA Committee Mission to Poland

19 - 21 September 2022

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 752.603 - September 2022

EN

Briefing for the PEGA Committee Mission to Poland

19 - 21 September 2022

Abstract

This briefing contains background materials for PEGA Committee mission to Poland.

Materials collected in the briefing indicate at a large scale legislative overhaul, deep politicisation of executive branch and undermining of judicial independence that led to a paralysis in resolving flagrant violations of law due to illegal acquisition and use of Pegasus spyware in Poland.

The briefing has been prepared by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the PEGA Committee.

This document was requested by the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware.

AUTHORS
Policy Department for Citizens' Rights and Constitutional Affairs, DG IPOL in cooperation with European Parliament's Liaison Office in Poland.

COORDINATION and ADMINISTRATOR RESPONSIBLE
Mariusz MACIEJEWSKI, Policy Department for Citizens' Rights and Constitutional Affairs, DG IPOL

EDITORIAL ASSISTANT
Fabienne VAN DER ELST

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in September 2022

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. POLITICAL AND INSTITUTIONAL SETTING IN POLAND

The Republic of Poland (*Rzeczpospolita Polska*) is a democratic state with a bicameral parliamentary system and a social market economy.

The Constitution ratified in 1997 defines its political structure and acts as the supreme organic law.

At a glance information on political forces in Poland

Law and Justice (PiS, ECR website: http://pis.org.pl/

Party leader: Jarosław Kaczyński

Leading figures: party Chairman, MP, former vice-PM and Chairman of the Committee on Security and Defence: Jarosław Kaczyński, PM Mateusz Morawiecki, Minister of National Defence Mariusz Błaszczak, Deputy Chairman Joachim Brudziński (MEP), Speaker of the Sejm (Lower Chamber)

Elżbieta Witek, Deputy Chairman of the party Adam Lipiński, Ryszard Terlecki (Head of PiS parliamentary caucus).

Party profile: national, right-wing, pro-social party. It combines a strongly catholic-oriented conservatism with a redistributive economic programme. The party was founded by the 'Kaczyński brothers' and is currently led by Jarosław Kaczyński.

Civic Platform (PO, EPP) website: http://www.platforma.org/

Party leader: Donald Tusk

Leading figures: party leader and MP Borys Budka, MP Małgorzata Kidawa-Błońska

(Deputy-Speaker of the Sejm and party's candidate for the next PM), Rafał Trzaskowski (Mayor of Warsaw and ex-EU Affairs Minister), MEP Ewa Kopacz (exPM, current Vice-President of the EP) and MP Rafał Grupiński (Head of PO parliamentary caucus).

Party profile: centrist party representing a moderate approach towards socioeconomic and moral issues; committed to the EU. The party was co-founded by Donald Tusk. Since autumn 2018 forms an electoral alliance with liberal (Modern), green (Greens) and social democrat (Polish Initiative) parties.

Left (S&D) website: Nowa Lewica

Party leader: it is a grouping composed of two parties, having altogether three leaders: Włodzimierz Czarzasty, Robert Biedroń (co-leaders of New Left) and Adrian Zandberg (Left Together)

Leading figures:, Krzysztof Gawkowski, Marcelina Zawisza, Krzysztof Śmiszek, Anna Maria Żukowska

Party profile: it is not formally a party but a coalition of: 1) socialdemocratic New Left, whose origin is, SLD, having a post-communist origin. It ruled Poland twice: 1993-1997 and 2001-2005. It has merits in steering the country towards the EU membership, 2) Progressive Part of New Left is also a former Spring party (*Wiosna*) established in spring 2019 by popular LGBT activist and mayor of Slupsk Robert Bierdoń (currently MEP), and 3) far-left Left Together (*Lewica Razem*) a small party grouping mainly left-wingers recruiting from young urban electorate.

The three parties established a coalition in mid-2019. In late 2019 SLD and Spring initiated a process of merging their parties. In the Sejm they all have 3 sit in a common caucus.

Polish People's Party (PSL, EPP) website: http://www.psl.org.pl/

- **Party leader:** Władysław Kosiniak-Kamysz (also Head of Polish People's Party parliamentary caucus)
- **Leading figures:** party leader and MP Władysław Kosiniak-Kamysz, Piotr Zgorzelski

(Deputy Speaker of the Sejm), MP Marek Sawicki (ex-Minister of Agriculture), Waldemar Pawlak (former PM – twice)

Party profile: an agrarian, conservative party, left-of-the centre in economy. Lost a considerable part of its electorate based on farming communities. Influent at local and regional level, was very close to an abyss in the last parliamentary elections (passed the Sejm's entry threshold by 0.13% only). The party's new, young leader Kosiniak-Kamysz is very critical of PiS, while his style is always to calm down the conflicts and seek compromises. That earned him a reputation of the most popular among the opposition party leaders. Since mid-2019 they form an electoral alliance called Polish Coalition with two tiny EPP-oriented groupings.

Confederation (*Konfederacja*, no EP affiliation) website: https://konfederacja.net/

- **Party leader:** as it is a federation of two groupings, there are two leaders: Janusz Korwin-Mikke and Robert Winnicki
- **Leading figures:** Grzegorz Braun (MP), Krzysztof Bosak (MP), Jacek Wilk (MP)

Party profile: a party established only in mid-2019 as a merger of two antisystemic and bitterly anti-EU far-right groupings. They were:

1) KORWiN part: libertarian in economics (almost no State), ultra-conservative in moral issues and pro-Russian. Its leader Janusz Korwin-Mikke (ex-MEP) is known for blatant discriminatory statements against Muslims, women, LGBT or handicapped people.
2) National Movement: nationalistic and ultra-conservative.

Konfederacja made over 5% entry threshold in October 2019 parliamentary election.

1.1. Legislative branch in Poland

1.1.1. Senate and Sejm

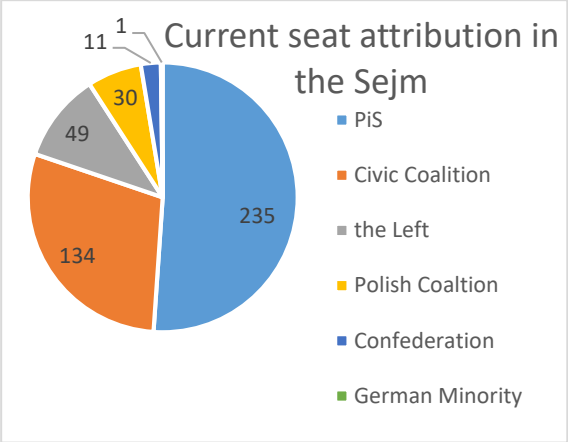
Poland has a bicameral legislature composed of the lower house (Sejm, 460 members) and the upper house (the Senate, 100 members). Both these chambers are directly elected through universal suffrage opened to all citizens for a term of 4 years. The Sejm is responsible for passing legislation and controlling the state administration. The Senate co-legislates with the Sejm.

The Sejm is elected through a proportional representation system that makes use of lists. To enter the parliament, there is a threshold of 5% for a political party and a threshold of 8% for a coalition of parties. National minorities' lists are exempted from the threshold requirements.

Law and Justice (PiS-ECR) is a dominant party in a coalition called United Right which has been running the country since 2015.

The last parliamentary elections in Poland were held in 2019, resulting in PiS obtaining 43.76% of vote, largely ahead of the main opposition party, Civic Coalition, which obtained 27.24% of the votes. The number of seats attributed are shown in the chart below.

Figure 1: Current seat attribution in the Sejm



Since 2019 elections, the PiS holds a majority in the lower House of the Parliament. This majority is not as strong as in 2015, opening paths for more diverse coalitions.

In the table below the result of parliamentary election 2019 is weighed against outcome of EP elections 2019, presidential (first round) 2020 and current support of respective in recent opinion polls.

Table 1: the result of parliamentary election 2019

Political party	EP group	General election Oct. 2019 (%)	Number of MPs in the Sejm[1]	EP election May 2019 (%)	Align-ment to a bigger block	Score of candidate in presiden-tial election June 2020 (%)	Average support in 2 opinion polls in July 2022 (%)
Law & Justice (PiS) + its allies	ECR	43.59	236	45.38	**United Right**	Andrzej Duda 43.5	33.8
Polish Peoples' Party (PSL)	EPP	8.55	24	38.47 (running as European Coalition)	**Polish Coalition**	Władysław Kosiniak-Kamysz 2.4	4.7
Modern (N)[2]	RE	27.40	126		**Civic Coalition**	Rafał Trzaskowski 30.5	24.6
Civic Platform (PO)/Civic Coalition	EPP						
Democratic Left Alliance (SLD)	S&D	12.56	44		**Left**	Robert Biedroń 2.2	8.6
Spring (Wiosna)	S&D			6.06			
Together (Razem)	None (leftist)			1.24			
Confederation (Konfederacja)	None (far right)	6.81	11	4.55	-	Krzysztof Bosak 6.8	6.3
Poland 2050 / Szymon Hołownia	Renew Europe	-	8	-	-	Szymon Hołownia 13.9	10.2

In August 2021, the least radical of the coalition parties (Agreement-ECR) left it. PiS overcame that crisis because out of 11MPs of the revolted party only 5 followed their leader, former Deputy Prime Minister Jarosław Gowin. After a few weeks PiS managed to rebuild the majority by attracting 7 MPs who previously had no affiliation or belonged to micro-groupings.

In the Senate the opposition parties and independent Senators have 52 seats, whereas the governing PiS has 48 seats.

Since the Sejm is controlled by the ruling PiS and the Senate by the opposition, two **Senate's prerogatives have grown in importance** invigorating democratic discourse in Poland:

[1] The total number of MPs in the Sejm is 460 MPs. The numbers in the column do not sum up to 460, because over 10 MPs have no affiliation or moved to new microscopic groupings during the term of office.

[2] Modern party has lost almost all of its support, it is now teamed up with Civic Platform, which has changed its brand to Civic Coalition.

- **reviewing and proposing legislation**: during the PiS's full control over Parliament in the years 2015-2019, it happened a few times that the politically urgent laws were pushed through all the three readings in the Sejm and Senate within one day. Since the upper chamber is controlled by the opposition it contributes to deepening reflection and discussion on legislation since the Senate has to take position on the Sejm's legislative proposals. An opposition driven Senate gives the opposition parties a greater visibility in internal and foreign policy. The Senate's ambition is an example of a rational legislative work, through i.a. inclusion of stakeholders through public hearings – a procedure which has been extremely rarely applied in PiS-dominated Sejm. It may also come with its own legislative initiatives, which may appeal to large segments of society and thus be difficult to reject for PiS for political reasons. However, the last say belongs to the Sejm and all Senate's proposals or amendments could be eventually voted down by the lower chamber.

- **decisions on certain important appointments**: it proved to be important when it came to nomination of the Ombudsman – the candidate is chosen by the Sejm and then needs to be approved by the Senate. That Senate also nominates its representatives to a few important collegial bodies.

The Senate's focus on **better law-making** is in line with **better regulation agenda** and **evidence-based policy making** being at the top of the agenda in the EU and subject to constant improvement as to the focus on delivering benefits to citizens, improved quality of policy criteria and improved use of information, including data and expertise in law-making.

On 18 November 2015, Sejm has set up a **Special Services Committee**.

The scope of the Committee's activities includes issuing opinions on legislative draft, regulations, orders and other normative acts relating to special services, including those regulating the activities of these services, expressing opinions on the directions of activities and considering annual reports of heads of special services, giving opinions on the draft budget with regard to special services, considering the annual report on its implementation and other financial information of special services, giving opinions on applications for the appointment and dismissal of individual people to the positions of heads of special services and their deputies, getting acquainted with information of special services about particularly important events in their activities, including suspected irregularities in their activities and suspected violations of the law by these services, through access to and inspection of information, documents and materials obtained as a result of the performance of statutory tasks, in accordance with the provisions of the Act on the protection of information and special services, and laws regulating the activities of special services; assessment of the cooperation of special services with other authorities, services and institutions authorized to perform operational and reconnaissance activities in the scope of activities undertaken by them for the protection of State's security, assessment of cooperation of special services with the Armed Forces, government administration bodies, law enforcement and other State institutions and units', local government bodies, competent authorities and special services of other countries, assessment of the protection of classified information and examination of complaints regarding the activities of special services, as well as consideration of periodic information, reports or reports on the activities of institutions and bodies of state authority, other than special services, containing information obtained in the course of performing operational and reconnaissance activities as well as preventive activities and activities (Annex to the Resolution of the Sejm of the Republic of Poland of 30 July 1992 - Regulations of the Sejm of the Republic of Poland, consolidated text: M.P. 2012 item 32, as amended)

On October 16th, 2019, the Committee held a closed meeting on inquiry concerning acquisition of spyware Pegasus by Central Anticorruption Bureau ("Wyjaśnienie sprawy potencjalnego zakupu oprogramowania szpiegowskiego Pegasus przez Centralne Biuro Antykorupcyjne). No materials are publicly available from this meeting.

On January 12th, 2022, Senate has constituted a **Special Committee to inquire on cases of illegal surveillance, their impact on election process in Poland and reform of special services** (Komisja Nadzwyczajna do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych) ")(further referred to as "Senate's Special Committee").

The following Senators are members of the Committee: Marcin Bosacki (Chair), Gabriela Morawska-Stanecka (vice-Chair), Sławomir Rybicki (vice-Chair), Jacek Bury, Michał Kamiński, Magdalena Kochan i Wadim Tyszkiewicz.

The competences of the Committee are the following:

1) inquiry on exposed cases of illegal surveillance with use of e.g. spyware Pegasus and on law infringements by special services during operational surveillance;

2) assessment of impact of exposed cases of illegal surveillance on election process in Poland;

3) preparation, tabling and participation for reading by Senate of legislative proposal reforming special services on the basis of, among others, guidelines presented by the Ombudsman and Ombudsman's Expert Group on September 23rd 2019.

Secretary: tel. +48 (22) 694 94 07

The Committee held numerous meetings publically available and documented on its website. The recordings and transcripts from the meeting constitute important evidence concerning Pegasus. While we include in this report selected translation of testimonies given before the Senate's Special Committee, we advise MEPs to request full translation of transcripts into English.

1.1.2. Issues

In its 2022 Rule of Law Report the European Commission indicated that legislation carrying out **significant** reforms continues to be frequently adopted while bypassing procedures that provide for adequate consultations. Recently proposed initiatives could adversely affect the civic space and there are concerns about measures limiting activities of civil society.

Importantly, already in 2016 the European Commission was concerned with the following issues: the appointment of judges to the Constitutional Tribunal and the implementation of the judgments of the Constitutional Tribunal of 3 and 9 December 2015 relating to these matters; the Law of 22 December 2015 amending the Law on the Constitutional Tribunal, the judgment of the Constitutional Tribunal of 9 March 2016 relating to this law, and the respect of the judgments rendered by the Constitutional Tribunal since 9 March 2016; the effectiveness of the Constitutional review of new legislation which has been adopted and enacted in 2016.[3] Further concerns in this area were formulated in 2017, 2018, 2019, 2020, and 2021. Proper functioning of the Constitutional Court would be essential for review of constitutionality of legislation.

Venice Commission has issued numerous opinions negatively assessing Polish legislation.

Civic Legislative Forum (Batory Foundation) noted the following with regard to Polish legislation since 2015:

[3] https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2015

- In the 2015-2019 term, a characteristic phenomenon was the multiple amendments to the same act.
- In the first year of the term of office, the pace of adopting laws was incomparably faster than in the previous years and there were more bills submitted by MPs from clubs forming the government's backing.
- Despite the slower pace of legislative work in the following years of the term of office, there were still acts that were passed very quickly. In the fourth year of the term of office, the Sejm worked on 56 bills for less than 15 days, which accounts for over 23% of all adopted acts. This means that when proceeding with almost 1/4 of the acts, the provisions of the Regulations of the Sejm of the Republic of Poland, which require that basic, non-urgent work should take over 15 days were ignored.
- The greatest concern is the limitation of the parliamentary debate and the importance of public and social consultations. As a result of frequent use of separate procedures and the resignation without justification from conducting public consultations in the last year of the term of office, which is inconsistent with the provisions of the Rules of Procedure of the Council of Ministers, the government consulted less than 2/3 of the bills on which it was working. The average consultation time was less than 12 days.
- In the third year of the term of office, we found 8, and in the fourth as many as 21 "hidden" bills. These are government laws, about the existence of which the public learned only after starting work in parliament.[4]

While Polish Constitution generally provides excellent catalogue of rights, since 2015 there has been an urgent overhaul of essential laws largely disregarding law-making standards (such as assessment of conformity with international obligations and constitutionality as well as assessment of impacts and public consultations, reasonable time for assessment of proposals and readings), disregarding benefits of democratic discussion with the opposition and without meaningful judicial control.[5]

1.2. Executive branch in Poland

1.2.1. The President, the Council of Ministers, special services and independent agencies.

According to art. 10 of Polish Constitution executive power shall be vested in the President of the Republic of Poland and the Council of Ministers

The President of the Republic of Poland (Prezydent Rzeczpospolitej Polskiej)

According to art. 126 of the Polish Constitution, the President of the Republic of Poland shall be the supreme representative of the Republic of Poland and the guarantor of the continuity of State authority. The President of the Republic shall ensure observance of the Constitution, safeguard the sovereignty and security of the State as well as the inviolability and integrity of its territory.

[4] https://www.batory.org.pl/informacje_prasowe/xiii-raport-obywatelskiego-forum-legislacji-przy-fundacji-batorego/

[5] https://publicystyka.ngo.pl/obywatelska-analiza-prawa-doswiadczenia-dla-systemu-stanowienia-prawa

The position of the President of the Republic of Poland is not as strong as for instance in France, but still much stronger than in countries like Germany. In the fields of the defence and security policy the President shares the powers with the Government. The President is also the Chief Commander of Polish Army. The President may propose new laws. The President may also veto parliamentary bills (the veto may be overridden by the Sejm only with a majority of 3/5 of votes).

Andrzej Duda is currently the President of the Republic of Poland.

The Council of Ministers, the Prime Ministers and selected Ministries

The Council of Ministers is led by the Prime Minister.

The current Prime Minister is Mateusz Morawiecki (PiS).[6] Beata Szydlo, currently Member of the European Parliament, was his predecessor from **November 2015 till December 2017**.

The current government consists of 18 ministries and a Chancellery of the Prime Minister constituting the main body of the Centre of Government. Ministries (as well as the Chancellery) are structured into departments (performing content-related tasks) and bureaus (providing coordinating and supporting services). Both types are further divided into units. At the top of every ministry there is a political minister together with deputy ministers and a political cabinet.

The most important civil servant (providing most HRM functions) is the Director General of a ministry. Department and bureaus also have their directors. Units are run by heads, constituting the lowest level of managerial posts. Ministries are generally large organisations, comprising up to 30 departments/bureaus and employing more than two thousand employees.

[6] https://www.politico.eu/article/polands-pis-wins-parliamentary-election/

Below table presents selected Ministers within the central government:

Table 2: selected Ministers within the central government

Title	Name	Party	Appointment
Prime Minister[7]	**Mateusz Morawiecki**	Law and Justice	15 November 2019
Deputy Prime Minister / Minister of Culture , National Heritage and Sport[8]	Piotr Gliński	Law and Justice	15 November 2019
Minister of Education and Science[9]	Przemysław Czarnek	Law and Justice	19 October 2020
Deputy Prime Minister, minister of state assets[10]	Jacek Sasin	Law and Justice	15 November 2019
Minister of Infrastructure[11]	Andrzej Adamczyk	Law and Justice	15 November 2019
Minister of Agriculture and Rural Development[12]	Grzegorz Puda	Law and Justice	6 October 2020
Minister of National Defence[13]	Mariusz Błaszczak	Law and Justice	15 November 2019
Minister of Foreign Affairs[14]	Zbigniew Rau	Law and Justice	26 August 2020
Minister of Finances[15]	Tadeusz Kościński	Independent	15 November 2019
Minister of Interior and Administration[16]	Mariusz Kamiński	Law and Justice	15 November 2019
Minister of Climate and Environment[17]	Michał Kurtyka	Independent	15 November 2019
Minister of Family, Labour and Social Policy[18]	Marlena Maląg	Law and Justice	15 November 2019
Minister of Health[19]	Adam Niedzielski	Independent	19 August 2020
Minister of European Affairs[20]	Konrad Szymański	Law and Justice	15 November 2019
Minister of Justice[21]	Zbigniew Ziobro	United Poland	15 November 2019

[7] https://www.gov.pl/web/premier/mateusz-morawiecki
[8] https://www.gov.pl/web/kultura/piotr-glinski
[9] https://czarnek.pl/
[10] https://www.gov.pl/web/primeminister/jacek-sasin-cm
[11] https://www.gov.pl/web/primeminister/andrzej-adamczyk-cm
[12] https://www.gov.pl/web/premier/grzegorz-puda
[13] https://www.gov.pl/web/obrona-narodowa/mariusz-blaszczak
[14] https://www.gov.pl/web/diplomacy/zbigniew-rau
[15] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjpupGxmbT4AhXXi_0HHS-AD1gQFnoECAgQAQ&url=https%3A%2F%2Fwww.ebrd.com%2Fcv-koscinski.pdf&usg=AOvVaw2aoWd9x-wYa5j31T0thy-N
[16] https://www.gov.pl/web/mswia/mariusz-kaminski2
[17] https://www.gov.pl/web/klimat/michalkurtyka-fr
[18] https://www.gov.pl/web/rodzina/marlena-malag
[19] https://www.gov.pl/web/zdrowie/adam-niedzielski
[20] https://www.gov.pl/web/premier/konrad-szymanski
[21] https://www.gov.pl/web/sprawiedliwosc/zbigniew-ziobro

Ministry of Finance (Ministerstwo Finansów)

Magdalena Rzeczkowska is currently the Minister of Finance. Previous ministers were:

- Paweł Szałamacha (16 XI 2015 - 28 IX 2016),

- Mateusz Morawiecki (**28 IX 2016- 9 I 2018**),

- Teresa Czerwińska (9 I 2018-4 VI 2019),

- Marian Banaś (4 VI 2019-30 VIII 2019),

- Jerzy Kwieciński (20 IX 2019-15 XI 2019),

- Tadeusz Kościński (15 XI 2019- 9 II 2022),

- Mateusz Morawiecki (10 II 2022-26 IV 2022)

Among main tasks of the Ministry of Finance is to **develop**, **execute** and **control** the implementation of the state budget. In addition, the Ministry deals with the system of financing local government, the budgetary sphere and state security, and manages the public debt.

The organisational structure of the Ministry in available under the following link:

https://www.gov.pl/web/finanse/kierownictwo

Committee of the Council of Ministers for National Security and Defence

Currently the Chairman of the Committee is Mariusz Błaszczak. His predecessor was Jarosław Kaczyński.

The Committee is composed of:

- Chairman of the Committee - Deputy Prime Minister appointed by the Prime Minister;
- Minister of National Defence,
- Minister responsible for internal affairs,
- Minister of Justice,
- Minister responsible for coordinating the activities of secret services, if appointed by the Prime Minister,
- Minister responsible for foreign affairs.
- The Chairman of the Committee may invite other persons to participate in the work of the Committee, in an advisory capacity.

Pursuant to § 2 of the ordinance no.162 of the Chairman of the Council of Ministers of October 9, 2020 on the Committee of the Council of Ministers for National Security and Defense, the tasks of the Committee include the coordination of preparation, activities and efficient decision-making in matters of State security and defence and recommending the Council of Ministers or the President of the Council of Ministers of proposals in this regard, in particular conducting analyses in the field of home affairs, public order, defence and justice, including those concerning the rule of law in the decisions taken.

Ministry of National Defence (Ministerstwo Obrony Narodowej)

Mariusz Błaszczak Deputy Prime Minister, Minister of National Defense. In 2015-2018, the Minister of Internal Affairs and Administration in the governments of Beata Szydło and Mateusz Morawiecki, from

January 9, 2018, the Minister of National Defense in the government of Mateusz Morawiecki. On June 22, 2022, he was appointed the vice-President of the Council of Ministers and the head of the Committee for National Security and Defence.

The Minister of National Defence manages government administration of national defence and is the body through which the President of the Republic of Poland exercises, in times of peace, sovereignty over the Armed Forces of the Republic of Poland.

The organisational structure of the Ministry is available under the following link:

https://www.gov.pl/web/obrona-narodowa/biura-i-departamenty1

Ministry of Internal Affairs and Administration (Ministerstwo Spraw Wewnętrznych i Administracji)

Mariusz Kaminski is currently the Minister of Internal Affairs and Administration.

Mariusz Kamiński was a co-founder of the Central Anticorruption Bureau ("CBA"), and from August 2006 to October 2009, the head of the CBA. Since November 2011, he has been the vice-president of Law and Justice. In 2015, he became a minister-member of the Council of Ministers in the government of Prime Minister Beata Szydło, and then Prime Minister Mateusz Morawiecki. Under the Prime Minister's ordinance, he was granted powers to coordinate the activities of special services. On August 14, 2019, Mariusz Kamiński was appointed the Minister of Internal Affairs and Administration.

On January 26th, 2020, Mr Kaminski made a written statement in response to the Senate's Special Committee to inquire on cases of illegal surveillance, their impact on election process in Poland and reform of special services, refusing to cooperate with the Committee, in violation of the Act on the performance of the mandate of a deputy and senator of May 9, 1996, according to which representatives of competent state bodies are obliged to present information and explanations at the request of permanent and extraordinary senate committees on matters falling within their scope of activity. It is also a violation of art. 112, in connection with art. 124 of the Constitution, according to which the manner of performing the constitutional and statutory duties of state organs towards the Senate is specified in the Regulations of the Senate. And it is a violation of art. 60(3) of the Senate's rules of procedure obliging representatives of state bodies to cooperate with the committee, in particular to actively participate in committee meetings.

Maciej Wąsik is the Secretary of State in the Ministry.

The organisational structure of the Ministry is available under the following link: https://www.gov.pl/web/mswia/struktura-organizacyjna

Ministry of Justice (Ministerstwo Sprawiedliwosci)

The Ministry of Justice is an auxiliary office of the Minister of Justice, the supreme body of government administration responsible for the department of government administration: justice. By virtue of the Constitution, the Minister of Justice is a member of the National Council of the Judiciary.

The current Minister of Justice and General Prosecutor is Mr Zbigniew Ziobro.

The organisational structure of the Ministry is available under the following link:

https://www.gov.pl/web/sprawiedliwosc/struktura-organizacyjna

Special services

Special services are listed in art. 11 of the Act of May 24, 2002 on the Internal Security Agency and the Foreign Intelligence Agency: Internal Security Agency (ABW), Foreign Intelligence Agency (AW), Military Counterintelligence Service (SKW), Military Intelligence Service (SWW) and Central Anticorruption Bureau (CBA).

Competences to undertake intelligence and operational activities have been given also to police services such as police (policja), military police (Żandarmeria wojskowa) and border guards (straż graniczna), as well as treasury services such as tax intelligence (wywiad skarbowy) i customs services (Służbę Celną).

Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego)

Colonel Krzysztof Wacławek is currently the Chief of ABW.

The Internal Security Agency (ABW) has a statutory obligation to identify terrorist threats and prevent acts of terror. Acquiring and analyzing information allows to assess the sources and scale of the phenomenon, select groups of potential attackers, identify their plans and logistics.

Foreign Intelligence Agency (Agencja Wywiadu)

Current Head of the Agency is colonel Bartosz Jarmuszkiewicz.

Among competences of the AW are:

- obtaining, analyzing, processing and forwarding to competent authorities information that may be of significant importance for the security and international position of the Republic of Poland as well as its economic and defense potential;
- identifying and counteracting external threats to security, defence, independence and inviolability of the territory of the Republic of Poland;
- recognizing international terrorism, extremism and international organized crime groups;
- identification of international trade in weapons, ammunition and explosives, narcotic drugs and psychotropic substances as well as goods, technologies and services of strategic importance for state security, as well as recognition of international trade in weapons of mass destruction and threats related to the proliferation of these weapons and their means of delivery;
- identifying and analyzing threats in the areas of international tensions, conflicts and crises affecting the security of the state, and taking actions to eliminate these threats;
- identifying, counteracting and preventing terrorist events directed against citizens or property of the Republic of Poland outside the state, excluding events of a terrorist nature directed against the personnel or property of the Polish Armed Forces;
- conducting electronic interview;
- undertaking other activities specified in separate acts and international agreements.

Organisational structure of the Agency is available under the following link:

https://www.aw.gov.pl/pl/o-nas/struktura/101,Struktura.html

Central Anticorruption Bureau (Centralne Biuro Antykorupcyjne)

Andrzej Stróżny is currently the Head of the Central Anticorruption Bureau.

Previously the Bureau was run by:

- Mariusz Kamiński od 3 sierpnia 2006 r. do 13 października 2009 r.
- Paweł Wojtunik od 13 października 2009 r. do 1 grudnia 2015 r.
- Ernest Bejda od 1 grudnia 2015 r. do 20 lutego 2020 r.

The Central Anticorruption Bureau (CBA) is a special service established to combat corruption in public and economic life, in particular in state and local government institutions, as well as to combat activities detrimental to the economic interests of the state. It operates pursuant to the Act on the Central Anti-Corruption Office of June 9, 2006.

The activities of the CBA are financed from the state budget.

The tasks of the CBA within the scope of the Bureau's competence (combating corruption in public and economic life, in particular in state and local government institutions, as well as combating activities detrimental to the economic interests of the state) include, first and foremost, the identification, prevention and detection of crimes (listed in Article 2 sec. 1 point 1 of the CBA Act) and the prosecution of their perpetrators, but also:

• revealing and preventing cases of non-compliance with the provisions on limiting the conduct of business activity by persons performing public functions;

• documenting the grounds and initiating the implementation of provisions on the return of unjustly obtained benefits at the expense of the State Treasury or other state legal entities;

• disclosure of cases of non-compliance with the procedures for making and implementing decisions specified by law in the scope of: privatization and commercialization, financial support, awarding public contracts, disposing of property of public finance sector entities, entities receiving public funds, entrepreneurs with the participation of the State Treasury or local government units, granting concessions , permits, subjective and objective exemptions, discounts, preferences, quotas, plafonds, bank sureties and guarantees;

• control of the correctness and truthfulness of asset declarations or declarations on conducting business activity by persons performing public functions;

• conducting analytical activities regarding phenomena occurring in the area of the CBA's competence and presenting information in this respect to the Prime Minister, the President of the Republic of Poland, the Sejm and the Senate.

An important part of the functioning of the CBA is also preventive activity.

The head of the CBA is a central body of government administration, supervised by the Prime Minister. On May 20, 2020, Prime Minister Mateusz Morawiecki appointed the Head of the Central Anticorruption Bureau **Andrzej Stróżny**. His predecessor, **Ernest Bejda**, appointed by Beata Szydlo, stayed in that office since 2015. Both Mr Stróżny and Bejda refused to stand before Senate's Special Committee, in violation of the Act on the performance of the mandate of a deputy and senator of May 9, 1996, according to which representatives of competent state bodies are obliged to present information and explanations at the request of permanent and extraordinary senate committees on matters falling within their scope of activity. It is also a violation of art. 112, in connection with art. 124 of the Constitution, according to which the manner of performing the constitutional and statutory duties of state organs towards the Senate is specified in the Regulations of the Senate. And it is a violation of art.

60(3) of the Senate's rules of procedure obliging representatives of state bodies to cooperate with the committee, in particular to actively participate in committee meetings.

Former head of Central Anticorruption Bureau 2009–2015, Paweł Wojtunik, presented negative assessment of the use of "operational control" both from the point of view of its legality and effectiveness.[22]

Organisational structure of the Bureau is available under the following link: https://www.cba.gov.pl/pl/o-nas/struktura/351,struktura.html

International cooperation includes meetings with OLAF and participation in EUROPOL meetings.

Independent agencies

Personal Data Protection Office (Urząd Ochrony Danych Osobowych)

Jan Nowak fulfils the function of the President of the Personal Data Protection Office. On 4th of April, 2019, he was appointed for this post by the Sejm (lower chamber of the Polish Parliament). On 16th of May, 2019, Jan Nowak took the oath before the Sejm and that moment marked the beginning of his four-year term of office.

Mirosław Sanek fulfils the function of the Deputy President of the Personal Data Protection Office. Previously, he fulfilled the function of the Deputy Inspector General for Personal Data Protection. He was appointed for that position on 17 January 2018 by the Speaker of the Sejm (lower chamber of the Polish Parliament) upon a motion of the Inspector General for Personal Data Protection.

Edyta Bielak-Jomaa, Ph.D. in law, fulfilled the function of the President of the Personal Data Protection Office in the first term of office. Immediately before being appointed as the President of the PDPO, Edyta Bielak-Jomaa fulfilled the duties of the Inspector General for Personal Data Protection. On 9 April 2015 she was appointed for this post by the Sejm (lower chamber of the Polish Parliament), and on 16 April 2015 the Senate (upper chamber of the Polish Parliament) consented to her appointment.

Among the most important tasks of the Personal Data Protection Office are:

- monitoring and enforcing the application of provisions on the protection of personal data;
- advising (in accordance with national law) the national parliament, government and other institutions and bodies on legal acts and administrative measures to protect the rights and freedoms of natural persons in relation to processing;
- providing information to data subjects about their rights under the law and, when necessary, cooperating with supervisory authorities from other Member States;
- considering complaints submitted by data subjects or by other entities, organizations, associations;
- cooperating with other supervisory authorities, providing mutual assistance, exchanging information in order to enforce the EU GDPR regulation;
- conducting proceedings on the application of the provisions on the protection of personal data, also on the basis of information received from another supervisory authority or other public authority;

[22] https://www.senat.gov.pl/prace/komisje-senackie/przebieg,9555,1.html

- monitoring developments in relevant areas affecting the protection of personal data, in particular monitoring the development of information and communication technologies [...];
- keeping a list of the types of processing operations subject to the requirement for a Data Protection Impact Assessment (DPIA) and providing recommendations under a prior consultation procedure;
- encouraging the establishment of data protection certification mechanisms and data protection seals and marks, and the approval of certification criteria;
- keeping an internal register of infringements based on information provided by administrators;
- taking part in the work of the European Data Protection Board (EDPB) and cooperating with other supervisory authorities.

The organisational structure of the Office can be found under the following link: https://uodo.gov.pl/en/494. The office has a broad network of cooperation.

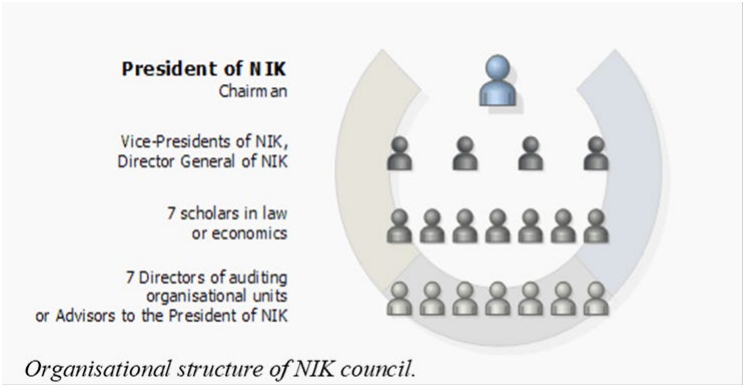
The Supreme Audit Office of Poland (Najwyższa Izba Kontroli)

The president of the Supreme Audit Office is appointed by the Sejm upon consent of the Senate, following a request of the Sejm speaker or a group of at least 35 members of the lower house.

The current Supreme Audit Office president is Mr. Marian Banaś, assisted by two vice-presidents: Mrs Malgorzata Motylow and Mr. Tadeusz Dziuba. The administration of the Supreme Audit Office is headed by a Director General, who is appointed by the Supreme Audit Office President, upon consent of the Speaker of the Sejm.

These presidents and the director general, alongside 14 other members make up the Council of the Supreme Audit Office. This body is in charge to ensure the collegiality principle for the audit body as set in the Polish Constitution and statutory provisions. This council is also in charge of approving all documents that the institution is obliged to transfer to the Sejm, under constitutional provisions.

Figure 2: Organisational structure of NIK Cuncil



Organisational structure of NIK council.
Source: https://www.nik.gov.pl/en/about-us/the-council-of-nik/the-council-of-nik.html

Beyond the Council of Supreme Audit Office, which steers the institution, the auditing organization is also comprised of 14 different audit departments, each with a specific field of auditing. Alongside these sub-units, there are also four administrative departments, backing the logistics and resources of the organization.

The Supreme Audit Office is the top auditing body of Poland. The independent institution has carried missions to safeguard public spending in Poland for over 100 years. The current form of the auditing authority is set out in the Polish Constitution, notably in the chapter 9, article 202, 203, 204, 205, 206 and 207. Its functioning is detailed through the 1994 Act on the Supreme Audit Office. In the first article of this act, alinea 2, it is clear that the Supreme Audit Office is subordinated to the Sejm, and therefore reports accordingly.

Every year, the financial consequences of irregularities in public-money spending reach up to PLN 10 billion (+/- EUR 2.13 billion). When these irregularities result of a legal gap or lack of clarity in the law, the Supreme Audit Office usually draws recommendations, the so-called *de lege ferenda* proposals. While the auditing institution does not have any law-making power, these recommendations used to have noticeable influence on the process of legislative design. Out of the 330 de lege ferenda suggested by the Supreme Audit Office for the period 2010-15, 161 were rejected and 104 implemented in full.[23]

The President of the Supreme Audit Office, Mr Marian Banas has sometimes been critical of the Polish government, notably in a report criticizing the government's decision to print ballots for an electoral election that had not been approved by parliament.

Supreme Audit Office's budgetary control played an important role in revealing that Pegasus has been acquired by Central Anticorruption Burea as well as in indicating that the acquisition has been made with violation of law, in particular with violation of budgetary provisions.

Ombudsman (Rzecznik Praw Obywatelskich) is the constitutional authority for legal control and protection. In his activities, the Ombudsman is integral and independent from other state authorities. The Ombudsman acts pursuant to the Constitution of the Republic of Poland and the Ombudsman Act of 15 July 1987. The Ombudsman is appointed by the Sejm and approved by the Senate for a 5 -year term of office.

The Ombudsman safeguards human and civic freedoms and rights specified in the Constitution and other legal acts. In order to fulfill this task the Ombudsman investigates whether actions undertaken or abandoned by the entities, organizations or institutions obliged to observe and implement human and citizen rights and freedoms have not led to infringement of the law or the principles of social coexistence and justice, and undertakes appropriate measures. The Ombudsman is assisted by the Office.

Currently, Prof. Marcin Wiącek is the Ombudsman. Prof. Marcin Wiącek was preceded in his function by Prof. Adam Bodnar.

When acting on the basis of a complaint, the Ombudsman checks the facts presented by a complainant, but may also request another supervisory body to investigate the case.

The Ombudsman may examine the case right away or request the case files or information about the status of the case to be delivered by any institution concerned;

Having examined the case and confirmed that human and citizen rights or freedoms have been infringed, the Ombudsman refers the request to the competent authority, organisation or institution

[23] Mazur, J. (2016). Contribution of the Supreme Audit Office of Poland to Legislation and Experiences of Some Other SAIs. Public Finance Quarterly, 61(3), 343

whose actions led to the infringement, or to a superior authority to ensure redress for the infringement, and monitors implementation of the recommended actions.

The Ombudsman may lodge a last resort appeal with the Supreme Court in a penal case. The last resort appeal must be based on a statement that the law has been seriously infringed by the court; last resort appeal in a penal case cannot be lodged solely due to disproportionate punishment.

The Ombudsman may participate in constitutional complaint proceedings before the Constitutional Tribunal.

The Ombudsman may also exercise other powers laid down in the Ombudsman Act.

The Ombudsman decides about selecting and implementing a particular legal measure solely on the basis on his own evaluation of the case. The Ombudsman is not bound by the Code of Administrative Procedure to meet the time limits of case examination. No measure of appeal is available, if the Ombudsman decides to reject a request.

Both Prof. Adam Bodnar and Prof. Marcin Wiącek took numerous initiatives aimed at obtaining clarifications concerning the use of Pegasus by Polish special services.

The clarifications have been provided on July 13, 2022 and are summarized on Ombudsman website.

1.2.2. Issues

In its 2022 Rule of Law Report the European Commission indicated that concerns exist over the broad scope of immunities for top executives who are also members of Parliament, and impunity clauses for public officials who commit the crime of abuse of office.[24] Risks remain as regards the effectiveness of the fight against high-level corruption, including the threat of selective application of the law and impunity caused by a disparity in the treatment of corruption cases for political purposes. The independence of main anti-corruption institutions remains an issue, considering in particular the subordination of the Central Anti-Corruption Bureau to the executive and the Minister of Justice also being the Prosecutor-General.

As stated by the European Commission the fact that the Minister of Justice continues to serve also as Prosecutor-General adds to the concerns over the independence of the Central Anti-Corruption Bureau from the executive power.[25] The increased supervisory powers of the Prosecutor-General, who can issue instructions in individual cases, including not to prosecute, and take over corruption cases of his subordinate prosecutors, provide avenues to influence anti-corruption prosecutions politically, which has also been the case on several occasions.[26] In this context, concerns exist about the risks of politically

[24] GRECO Fifth Evaluation Round – Compliance Report, paragraphs 54-63; and GRECO Fifth Evaluation Round – Evaluation Report, paragraphs 82-91, reiterating its recommendation that in respect of persons exercising top executive functions, an in-depth reform of the system of immunities be carried out with a view to facilitating the prosecution of corruption offences by excluding these from the scope of immunities and by ensuring that the procedure for the lifting of the immunity is transparent and based on objective and fair criteria used effectively in practice (see paragraph 87). See also 2021 Rule of Law Report, Country Chapter on the rule of law situation in Poland, p. 17.

[25] As reported in the 2020 and 2021 Rule of Law Reports, Country Chapters on the rule of law situation in Poland, p. 8 and 11 (for 2020) and 18 (for 2021) ; GRECO Fifth Evaluation Round – Evaluation Report, paragraph 78.

[26] Helsinki Foundation (2022), A state of accusation: Polish prosecution service 2015-2022, and information received from the Batory Foundation in the context of the country visit to Poland and as reported, with more details, in the 2020 Rule of Law

motivated investigations and wiretapping of public officials, prosecutors and defence lawyers by the Central Anti-Corruption Bureau's Pegasus surveillance spyware.[27]

The report pointed as well that **the Supreme Audit Office operates under adverse conditions**. As of 2021, the Marshal of the Sejm has been refusing to appoint Members of the Supreme Audit Office's College, thus hampering the effective functioning of the Office. The Prosecutor-General has made a request to deprive the President of the Supreme Audit Office of his immunity, which is currently under examination of the Sejm. Representatives of the Supreme Audit Office raised concerns about the lack of effective follow-up by the prosecution services to its requests made in the aftermath of audits. Furthermore, the chief office-holders in Poland refuse to cooperate with the Supreme Audit Office in the context of audit reports. Since 2021, the Supreme Audit Office has produced a number of audit reports raising concerns regarding possible instances of public funds' embezzlement and mismanagement by public authorities, notably by the Ministry of Justice and bodies responsible for implementing the State budget. While the Supreme Audit Office raised concerns about developments adversely affecting its own independence at the forum of the European Organisation of Supreme Audit Institutions, no steps have so far been taken by the state authorities to rectify the situation.

The newly appointed Ombudsman continues to play a key role as a rule of law safeguard, despite limited resources.

There are longstanding concerns regarding politicization of civil service in Poland.[28] In general, the existence of the civil service in Poland is based on the Constitution, which stipulates that its function is to ensure the professional, diligent, impartial and politically neutral implementation of state duties by the central administration (art. 153). The other main legal basis is the Civil Service Act passed in 2008 (with additional changes), which lists public bodies that are part of the civil service (these include in particular: the Chancellery of the Prime Minister, ministries and other central administration offices, regional voivodship offices and other regional and local offices of government administration, fiscal administration and civil employees of law enforcement agencies).

Originally, the relationships between high-ranking civil servants and their political superiors were based on the assumption of their distinct statuses and formal separation. This is reflected in the Constitution.

In the first decade of the 21st century, although there were legal requirements in place for filling higher posts through a competitive process, in practice these were bypassed and higher posts remained highly politicized. Some signs of improvement in this regard could however be seen up until 2005. Since 2006, the status of higher posts has been changed three times with the Law & Justice (PiS) party government twice formally politicizing them – the second time in 2016. Nowadays it seems that the

Report, Country Chapter on the rule of law situation in Poland, pp. 8 and 11. In this context, see also the concerns raised by the Venice Commission (opinion CDL-AD(2017)028).

[27] As also reported in Part IV below, p. 24. Contribution by the Supreme Audit Office for the 2022 Rule of Law Report, p. 1; contribution from the Marshal of the Senate of the Republic of Poland for the 2022 Rule of Law Report, p. 1. See in this context also Prosecutor Wrzosek under surveillance with Pegasus? The prosecutor's office refused to initiate proceedings (29 Dec. 2021). Reportedly, also opposition lawyer Roman Giertych was under surveillance by the Pegasus software, who used his phone also for professional conversations subject to the attorney's secrecy, see Roman Giertych under surveillance with Pegasus (21 Dec. 2021). The same software was used in the case of Senator Krzysztof Brejza, see Brejza – another victim of Pegasus: The KO Chief of Staff was surveilled during the election campaign (23 December 2021).

[28] Mazur S. et al., Public administration characteristics and performance in EU28: Poland, 2018.

politicization of these posts remains the biggest challenge for the long-term effectiveness of central public administration. [29]

In particular, **the 2015 amendment of the Civil Service Act repealed all provisions on open and competitive recruitment positions and provided for possibilities of a simple appointment within the meaning of the Labor Code (Article 53a of the new wording of the Civil Service Act) and provided a frame for one time removal from the service of higher ranking civil servants employed on the basis of a work contract on December 30th, 2015**. Art 6 (1) as amended provided that "employment relationships with persons occupying higher positions on the date of entry into force of this act in the civil service and managerial positions in the foreign service, which are senior positions in the civil service, **shall expire 30 days from the date of entry into force of this Act**, if before the expiry of this period they are not offered new working or pay conditions for a further period or in the event of refusing to accept new working conditions or pay"[30] Batory Foundation presented an opinion on these amendments (and a report summarizing these practices in 2018) while Ombudsman filed a motion against these provisions with Constitutional Court.

The 2021 Rule of Law Report, points to several risks regarding the effectiveness of the fight against high-level corruption, including a risk of undue influence on corruption prosecutions for political purposes. Specifically, the report mentions concerns over the independence of the main anti-corruption bodies, with, for instance, the subordination of the Central Anti-Corruption Bureau to the executive.

1.3. Judicial authorities

1.3.1. Structure of judicial authorities

In Poland, Polish Supreme Court heads the judicial branch in matters regarding the activity of subsequent common courts. Constitutional Tribunal heads the judicial activities regarding constitutional matters in international agreement, political parties' activities and adjudicates tensions between governing authorities and constitutional watchdogs. The Supreme Administrative Court heads all matters regarding public administration.

Tribunal of State (Trybunal Stanu)

The Tribunal of State is a judicial authority which enforces the responsibility of the highest organs and state officials for violations of the Constitution or statute, in connection with their position or covered by the scope of their office.

The following may be brought before the Tribunal of State:

a) the President - for violation of the Constitution or statute, and for fiscal crimes and offenses (the President may be punished only by the Tribunal of State);

[29] Mazur S. et al., Public administration characteristics and performance in EU28: Poland, 2018.

[30] Own translation.

b) the Prime Minister and members of the Council of Ministers - for violation of the Constitution or the Act, and for offenses or fiscal offenses related to their function;

c) the President of the National Bank of Poland, the President of the Supreme Audit Office, members of the National Broadcasting Council, persons entrusted with the management of the ministry by the Prime Minister, the Supreme Commander of the Armed Forces - for violation of the Constitution or law;

d) deputies and senators - in the event of breaking the ban on economic activity and deriving benefits from the property of the State Treasury.

The decision on bringing the State before the Tribunal is made by: the National Assembly, the Sejm, and the Senate.

The Tribunal of State consists of 16 members elected by the Sejm for the duration of its term of office, 2 vice-chairmen, also elected by the Sejm, and the Chairman, who is the First President of the Supreme Court. Both the Vice-President and at least 1/2 of the members of the Tribunal must have judicial qualifications.

Polish Supreme Court (Sąd Najwyzszy)

According to art. 183 of Polish Constitution the Supreme Court exercises supervision over common and military courts regarding judgments and performs other activities specified in the Constitution and statutes.

The First President of the Supreme Court is appointed by the President of the Republic for a 6-year term of office from amongst candidates proposed by the General Assembly of the Judges of the Supreme Court.

Prof. Dr Małgorzata Manowska is currently the First President of the Supreme Court

Organisational structure of the Court is available under the following link: http://www.sn.pl/en/about/SitePages/OrganizationIOZ.aspx

Constitutional Tribunal (Trybunal Konstytucyjny)

The Constitutional Tribunal's jurisdiction includes four areas:

- the control of norms (abstract and concrete; a posteriori and a priori - Article 188 points 1-3, Article 122 (3) and (4), and Article 133 (2) of the Constitution); a special procedure for reviewing norms is the examination of constitutional complaints (Article 79 and Article 188 (5) of the Constitution);
- resolving disputes over powers between central constitutional state organs (Article 189 of the Constitution);
- adjudication if the aims or activities of political parties are consistent with the Constitution (Article 188 (4) of the Constitution);
- recognition of the temporary inability to hold office by the President of the Republic (Article 131 (1) of the Constitution).

The Polish system of control of norms gives priority to a posteriori control, i.e. subsequent control, i.e. it may only apply to normative acts that have already been established or have already become binding, or are still in the vacatio legis period. Exceptionally, the control of norms can take a preventive character - a priori (prior), and the only entity authorized to initiate it is the President of the Republic of Poland.

On December 21, 2016, Julia Przyłębska was appointed President of the Constitutional Tribunal by the President of the Republic of Poland.

Supreme Administrative Court (Naczelny Sąd Administracyjny)

Supreme Administrative Court is a judicial body that controls the functioning of local and regional public administration in terms of compliance with the Constitution of the Republic of Poland, EU law and other laws. This control covers local and professional self-government bodies, local government administration bodies and other entities performing public administration functions.

The Supreme Administrative Court, among other competences,:

- hears appeals against judgments of voivodeship administrative courts, pursuant to the provisions of the Act;
- adopts resolutions aimed at clarifying legal provisions, the application of which has caused discrepancies in the jurisprudence of administrative courts;
- adopts resolutions resolving legal issues raising serious doubts in a specific administrative court case.

Jacek Chlebny is the President of the Supreme Administrative Court.

Organisational structure of the Constitutional Court is available under the following link:

https://www.nsa.gov.pl/struktura-organizacyjna.php

Prosecutor's office (Prokuratura)

The public prosecutor's office consists of the Public Prosecutor General, the National Public Prosecutor, other deputies of the Public Prosecutor General and public prosecutors of common organizational units of the public prosecutor's office and public prosecutors of the Institute of National Remembrance - Commission for the Prosecution of Crimes against the Polish Nation.

The Public Prosecutor General is the supreme organ of the public prosecutor's office. The Office of the Public Prosecutor General is exercised by the Minister Justice.

The public prosecutor's office performs tasks in the area of prosecuting crimes and upholds the rule of law.

The duties mentioned above are performed by the Public Prosecutor General, the National Public Prosecutor and other deputies of the Public Prosecutor General and their **subordinate** public prosecutors by, among other:

- conducting or supervising preparatory proceedings in criminal cases and performing functions a public prosecutor before the courts;
- conducting research in the field of crime, as well as combating and preventing it, and cooperating with research units in the field of research on crime issues and combating it and prevention and control;
- collecting, processing and analyzing data, including personal data, in IT systems from the proceedings conducted or supervised pursuant to the Act and from participation in the court and administrative proceedings, in cases of offenses or other proceedings provided for by the law, transferring data and analysis results to competent authorities, including authorities of other countries, if provided for in a statute or in an international agreement ratified by the Republic of Poland;

- cooperation with State authorities, State organizational units and social organizations in the prevention of crime and other violations of the law;
- cooperation and participation in activities undertaken by international or supranational organizations, and international teams operating on the basis of international agreements, including those constituting international organizations, ratified by the Republic of Poland;
- issuing opinions on draft normative acts;
- cooperation with organizations associating public prosecutors or public prosecutor's office employees, including co-financing joint research or training projects.

Polish law states that the public prosecutor is independent when performing his activities. However, a public prosecutor is **obliged to carry out instructions, guidelines and orders of a superior public prosecutor**. If the public prosecutor does not agree with the instruction concerning the content of a procedural act, he may request a change of the instruction or exclude him from performing the act or from participating in the case. The exclusion is finally decided by the **prosecutor who is directly superior to the prosecutor who issued the order**.

Zbigniew Ziobro is currently Presecutor General.

The organisational structure if prosecutors' office is available under the following link: https://www.gov.pl/web/prokuratura-krajowa/organizacja-jednostki10

1.3.2. Issues

In its 2022 Rule of Law Report the European Commission indicated that serious concerns persist related to the independence of the Polish judiciary. Since July 2021, the Court of Justice and the European Court of Human Rights have delivered rulings, confirming a series of concerns identified by the Commission in the context of the procedure under Article 7(1) TEU and previous Rule of Law reports.

Similarly, the 2022 country report on Poland indicates at a deterioration of the rule of law in Poland. Judicial independence remains a serious concern, as follows from several rulings of the Court of Justice of the European Union and the European Court of Human Rights. In particular, the Court of Justice of the EU has challenged the functioning of the disciplinary regime applicable to Polish judges and this ruling remains to be implemented. An order for interim measures of July 2021 of the Court of Justice of the EU to protect judicial independence has still not been implemented. In addition, the Commission launched an infringement procedure against Poland following the Polish Constitutional Tribunal ruling, which, according to the Commission, challenged notably the primacy of EU law. These developments contribute to a perceived lack of adequate judicial protection and judicial independence.

In its Recovery and Resilience Plan (RRP), Poland committed to undertake reforms of the disciplinary regime regarding judges, to dismantle the Disciplinary Chamber of the Supreme Court, and to create review proceedings for judges affected by decisions of that Chamber aimed at strengthening certain aspects of the independence of the judiciary.

Recent study commissioned by LIBE Committee indicates that with the appointment of Julia Przyłębska as the President of the Constitutional Tribunal (December 2016) the functioning of the Tribunal has changed in a dramatic way. The judges elected by the old parliament were practically prevented from deciding in the cases important for the government, the unconstitutionally elected judges were admitted to the adjudicating panels. The president of the Tribunal started frivolously changing the

assignment to the cases.[31] At the current moment all judges in the Tribunal are the nominees of the ruling majority in parliament, some of them were directly before the appointment the activists of the ruling majority, known for the extreme positions, also in relation to the European Union. The Constitutional Tribunal lost its position as neutral arbitrator in the matters of constitutionality of law.[32]

The Constitutional Court played an important role in reviewing constitutionality of surveillance legislation reframing abusive provisions according to principles of Polish law. This role has been lost after 2016.

Further concerns regarding the functioning of the prosecution service persist.

1.4. Media in Poland (the fourth power)

General framework

Journalists' protection in Poland is based on constitutional principles and specified in sectorial legislation. The Broadcasting Act and the Press Law provide, respectively, a legal framework for the media regulator - the National Broadcasting Council (KRRiT) and safeguards for journalistic independence. However, the competences of the National Broadcasting Council are quite limited and independence of its members is being questioned.

Issues

European Parliament's resolution of 16 September 2021 on media freedom and further deterioration of the rule of law in Poland (2021/2880(RSP)) indicated that Poland, along with some other Member States, has not yet implemented all the requirements of the Audiovisual Media Services Directive (Directive (EU) 2018/1808), and in particular those regarding independence of the national media market regulator.

European Parliament pointed out as well that the European Audiovisual Observatory of the Council of Europe concluded in 2019 that the independence of the Polish media regulatory authorities was raising concerns regarding the implementation of the appointment procedures and accountability to the National Broadcasting Council (KRRiT); and the National Media Council (RMN) had 'no adequate safeguards for the functional independence from political parties and the government'

Reporters Without Borders' World Press Freedom Index 2021 ranks Poland in 64th place, its lowest-ever ranking, dropping from 18th place in 2015.

The 2020 Rule of law report indicated that there is a lack of regulatory safeguards limiting political control over media outlets in Poland. Such safeguards concern rules on conflicts of interest between owners of media and the ruling parties, partisan groups or politicians. The CBOS survey from 2019 shows that the perception of political bias in the media is widespread. The 2021 Rule of law report listed numerous further concerns in this area.

[31] As an example see: Ł. Strarzewski, „Bezprawna manipulacja składem TK ws. kadencji RPO. Wniosek Rzecznika o wyłączenie Julii Przyłębskiej. EDIT: TK oddalił wcześniejszy taki wniosek", from 12.04.2021, https://bip.brpo.gov.pl/pl/content/manipulacja-skladem-tk-kadencja-rpo-wylaczenie-juli-przylebskiej .

[32] About the political character of current Tribunal, see, e.g., D. Mnich, „Polityczny kontekst orzecznictwa Trybunał u Konstytucyjnego", Przegląd Prawa Publicznego (2017), No. 7-8, p. 11. Similarly, A. Sulikowski, "Trybunał Konstytucyjny a polityczność. O konsekwencjach upadku pewnego mitu", Państwo i Prawo (2016),No. 4, p. 14, who, however also sees the possibilities to upkeep such political status with also far-reaching social benefits upon restoration of the legitimacy of the Tribunal.

The 2022 Rule for law report indicates that controversies around the extension of the broadcasting licences for both **TVN24** and TVN7 channels show risks in relation to the operation of independent media actors. In the case of TVN24, KRRiT decided to extend its licence but only after 18 months and the TVN7 licence was extended after more than 12 months from the extension request being made. While both licences were ultimately extended for the period of 10 years, the administrative proceedings by the KRRiT were considered as particularly long, although the Broadcasting Law provides for a simplified examination procedure in the case of a request for license renewal.

The report points that there are concerns regarding the independence of Polish public service media. Following the 2016 reform, the competences related to public service media are distributed between the National Media Council (RMN) and National Broadcasting Council (KRRiT). Under the current legal framework, the RMN is competent for the appointment and removal of the management and supervisory boards of the Polish Television (TVP), the Polish Radio and the Polish Press Agency. The 2022 Media Pluralism Monitor reports high risks in relation to independence of public service media governance and funding, referring to the support of the public service media management towards growing political partisanship as well as points the issues related to the justification and opaqueness of the public service media funding.

In the light of these considerations and with regard to Pegasus, the former Head of Military Counter-Intelligence Service (2014–2015) general Piotr Pytel (hearing of Senate's Special Committee 23-02-2022 (transcript) made the following observations on **a connection between the Central Anticorruption Bureau and State's television**:

"I see it, of course, in a certain sequence, which I can show here, i.e. the cooperation of the Central Anticorruption Bureau and certainly the broadly understood State television, because there it is also possible to broadcast programs by various television stations located under this cover of State television, as well as such a broad resonance in the press, which is somehow controlled by the authorities. In the period from August 2019 to, say, 2022, we had about 600 programs on the television itself, which were targeted ... which disavowed, humiliated, but also shaped a very negative image in the society, among the audience, of Mr. Krzysztof Brejza. Until January 10, 2022, there were exactly 672 such programs. This shows the scale, but also, I would say, a very consistent implementation of this plan."[33]

[33] Own translation.

2. ECONOMIC SITUATION IN POLAND

The basic economic data for Poland are the following:

Growth[34] (Quarter 1/2022): 1.0% (compared with Quarter 4/2021).

Unemployment [35] (April 2022): 2.7%; youth unemployment: 8.8%.

Spring 2022 economic forecast[36]: Real GDP grew by 1.0 % quarter-on-quarter in Q1, with the easing of COVID-related restrictions, leading to increased spending opportunities.

Poland is the largest economy of central Europe. It also is the sixth largest economy within the European Union and twentieth worldwide.

The most important sectors of the Polish economy are wholesale and retail trade, transport, accommodation and food services (24.9%), industry (24.2%) and public administration, defence, education, human health and social work activities (15.3%).[37]

Poland mostly exports to its EU partners (74%) and mostly imports from them as well (67%).

The OECD report points that the economy expanded strongly in the first quarter of 2022 with industrial production and retail sales growing at a solid pace, accompanied by robust wage growth and low unemployment.

However, high energy and food price growth and supply chain disruptions occurred in 2022, exacerbated by the war in Ukraine. Higher uncertainty, trade disruptions, inflationary pressures and monetary policy are set to curb GDP growth, which is expected to decelerate to 3.7% in 2022 and 3.0% in 2023.

Inflation was 15.6% in June 2022[38], highest since last 25 years and is predicted to grow further in the course of 2022 due to various factors, including rising energy prices, supply chain disruptions and increased input costs for businesses, which have been passed down to consumers. That prompted the central bank of Poland to introduce a series of rate hikes since October 2021 (currently 6.0%) significantly raising credit costs in Poland.

[34] Spring 2022 economic forecast published on 16 May 2022

[35] May figures published on 30 June 2022: Euro area: 6.6%; EU: 6.1%.

[36] Spring 2022 economic forecast published on 16 May 2022

[37] https://european-union.europa.eu/principles-countries-history/country-profiles/poland_en

[38] According to National Statistical Office, PL methodology, last available result according to HICP methodology is 12.8% in May.

Table 3: Economic forecast for Poland – 16 May 2022

Economic forecast for Poland – 16 May 2022				
Indicators	**2020**	**2021**	**2022**	**2023**
Gross Domestic Product growth (%, year-on-year)*	-2.2	5.9	3.7	3.0
Inflation (%, year-on-year)*	3.7	5.2	11.6	7.3
Unemployment (%)	3.2	3.4	4.1	3.9
Public budget balance (% of GDP)	-6.9	-1.9	-4.0	-4.4
Gross public debt (% of GDP)	57.1	53.8	50.8	49.8
Current account balance (% of GDP)	3.3	1.6	-0.5	-0.2

The war in Ukraine will significantly affect the Polish economy. Inflation has been pushed up by a surge in energy and food prices and the zloty's depreciation. Returning Ukrainian men have exacerbated skill shortages in construction and transport. Meanwhile, more than three million Ukrainian refugees, mostly women and children, have entered Poland. Having been granted access to the labour market and social benefits, the projections assume an additional 350 000 workers will join the labour force, alleviating skills shortages in some sectors.

Direct trade with Russia, Belarus and Ukraine, which represents 3-5% of GDP and 6-8% of total trade, will fall as exports drop while energy imports are diverted as planned, minimising the impact of the recent end to Russian natural gas imports.

Higher uncertainty and lower consumer and business confidence should also damp consumption and investment growth. Nonetheless, refugee spending in Poland should bolster consumption growth. Expansionary fiscal policy will be accompanied by tighter monetary policy.

Fiscal spending will rise to shield the economy against the impact of the war. The Polish New Deal, introduced in January, has been expanded. The government has also set aside an 11 billion zloty special fund for Ukrainian refugees. The Anti-Inflation Shield, introduced at the turn of the year and originally set to expire in mid-2022, is assumed to be extended until the end of 2022 to cushion households against high energy and food prices. Moreover, national defense spending is set to increase from 2.2% of GDP in 2022 to 3% by 2023. Given rising headline inflation, growing domestic inflationary pressures and an expansionary fiscal policy, the National Bank of Poland has continued raising key short-term interest rates.

The economy is expected to slow amid high inflation and uncertainty. Economic growth is set to slow considerably over the next two years. In 2022, inflation is expected to remain high but is likely to peak by the end of the year. Weaker real incomes and high uncertainty should lead to significantly slower consumption growth with investment and trade growth also dampened. A rise in fiscal spending will partly offset these shocks over 2022, with real GDP set to expand by 4.4%. In 2023, the effects of higher uncertainty should dissipate and, while the announced EU embargo on Russian oil will exert additional upward pressure on energy prices, headline inflation should slow as monetary policy tightens further.

Core inflation should also ease but is likely to remain elevated. Fiscal policy will support activity, boosted by spending from the EU Recovery and Resilience Facility funds, but monetary policy tightening will reduce growth. Overall, real GDP is expected to slow to 1.8% in 2023.

There is considerable uncertainty around this outlook and the balance of risks lies to the downside. Further escalation of the war would increase uncertainty, exacerbate inflation, and strain public finances. Additional disruptions to energy supplies would hit growth. A persistently tight labour market and continued consumption growth could further push up inflation. On the upside, a quick resolution of the war would increase GDP growth and reduce inflation.

On 24 June 2022, the Council endorsed the following **country-specific recommendations for Poland**:

In 2023, ensure that the growth of nationally-financed current expenditure is in line with an overall neutral policy stance, taking into account continued temporary and targeted support to households and firms most vulnerable to energy price hikes and to people fleeing Ukraine. Stand ready to adjust current spending to the evolving situation. Expand public investment for the green and digital transition and for energy security, including by making use of the RRF, RePowerEU and other EU funds. For the period beyond 2023, pursue a fiscal policy aimed at achieving prudent medium-term fiscal positions. Improve the efficiency of public spending, including by continuing the reform of the budget process. Ensure the adequacy of future pension benefits and the sustainability of the pension system by taking measures to increase the effective retirement age and by reforming the preferential pension schemes.

Swiftly finalise the negotiations with the Commission of the 2021-2027 cohesion policy programming documents with a view to starting their implementation.

Increase labour market participation, including by improving access to childcare and long-term care, and remove remaining obstacles to more permanent types of employment. Foster quality education and skills relevant to the labour market, especially through adult learning and improving digital skills. Better target social benefits and ensure access to those in need.

Improve the resilience, accessibility and effectiveness of the health system, including by providing sufficient resources to reverse the pyramid of care and accelerating the deployment of e-health services. Strengthen the innovative capacity of the economy, including by supporting research institutions and their closer collaboration with business. Enhance further digitalisation of businesses and public administration, including through development of infrastructure.

Enhance the investment climate, in particular by safeguarding judicial independence. Ensure effective public consultations and involvement of social partners in the policy-making process.

Reduce overall reliance on fossil fuels by removing regulatory, administrative and infrastructural barriers to accelerate permitting and deployment of renewable energy sources. Reform building renovation policies and support schemes to incentivise deeper energy efficiency, promote energy savings and faster phase-out of fossil fuels in heating and accelerated deployment of heat pumps. Accelerate modal shift towards public transport and active mobility and promote faster uptake of electric vehicles with incentives and investment in charging infrastructure. Improve long- and medium-term strategic planning of the green transition by updating national energy policies in line with the European Green Deal objectives and the REPowerEU Communication to provide certainty to the business community and use funding effectively with a view to accelerating clean energy investments.

Recovery and resilience plan

The Polish recovery and resilience plan (RRP) was submitted on 3 May 2021. There were delays in endorsing it due to the rule of law situation. On 17 June 2022, the Council approved the Commission's positive assessment of the RRP issued on 1 June 2022. The Commission stated that before any disbursement under the RRF can be made, Poland must demonstrate that milestones on the

independence of the judiciary are fulfilled. The law which aimed at addressing this problem was signed by the President on 13 June 2022 and will come into force on 13 July 2022.

The minor coalition party of PiS (ECR) - SP - challenges other obligations under Poland's RRP such as registration fee and ownership tax for non-emissions-free vehicles or increase of effective retirement age.

Demographics

The demographic situation in Poland in 2020 was influenced by the pandemic. Poland's total population, according to official statistics is 38.2 million people on 31 December 2020, which was about 118 thousand less than at the end of 2019. The situation in 2020 was most influenced by the highest number of deaths over many decades. Their number exceeded by over 100,000 the average annual value from the last 50 years (477 thousand to 364 thousand). Last year, 355 thousand of live births were registered (a decrease of almost 20 thousand yearly). 60% of Poland's population lives in urban areas and 40% in rural. The average life expectancy is 77.7 years and it is considerably higher for women (81.6) than for men (73.8).

To tackle the demographic challenge, in April 2016 the government introduced the child benefits programme 500+ offering around EUR 115 (PLN 500) per every second and subsequent children and for each child in low income families (for more see: Politics). 4 million children are now covered by 500+ programme which is almost 58% of children under 18 years old. It is a flagship social policy scheme to reverse Poland's negative demographic trends and the fulfilment of an election promise from the 2015 campaign. During the PiS convention held at the end of February 2019 to start its campaign before the European elections, the party presented a very generous modification of its social programme. The most important part was to extend the 500+ child allowance programme to include every child irrespective of the family income level, beginning from mid-2019. The yearly cost of the new package is around PLN 20 bn (EUR 4.6 bn).

2022 country report for Poland is available under the following link:
https://ec.europa.eu/info/system/files/2022-european-semester-country-report-poland_en.pdf

3. SURVEILLANCE AND USE OF SPYWARE IN POLAND

3.1. Use of Pegasus in Poland

3.1.1. Unfolding of evidence on the acquisition and the use of Pegasus in Poland

Pegasus is a hacking tool developed and marketed around the world by the Israeli company NSO Group and allegedly only sold to governments. This spyware tool is designed to secretly turn mobile phones - both with Android operating system and iOS - into 24-hour surveillance devices, as it grants complete and unrestricted access to all sensors and information of the targeted device.[39]

Forbidden Stories, a Paris based journalist nonprofit organisation, and Amnesty International, a human rights group, shared with 17 news organizations a list of more than **50,000 phone numbers** for people believed to be of interest to NSO customers. **Citizen lab**, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, indicated that the spyware was used to infect a **broad range of civilian targets, including government officials, journalists, human rights activists and dissidents**.

The use of Pegasus unfolded in Poland in a specific pace. Importantly, the sources of information about the acquisition and the use varied and at first it was the Supreme Audit Office, NGOs and press that pointed at this acquisition and use, while official confirmation of the fact that Pegasus was acquired came later on while any official information on its use is largely missing.

In a report published in June 2018, the **Supreme Audit Office** clearly indicated that on September 29th, 2017, an agreement was concluded by the Central Anticorruption Bureau for the amount of PLN 25 million (the contract is classified as confidential), as part of the implementation of statutory tasks by public finance sector entities related to the protection of the interests of victims and witnesses, as well as to the detection and prevention of crime. In the opinion of the Supreme Audit Office, the Ministry of Justice broke the law by transferring these funds to the CBA. As a result of these activities, millions of zlotys intended for crime victims were allocated to the purchase of special technology resources for the CBA, which may use them in violation of the regulations and rules in force in a democratic state ruled by law.[40]

On September 18th, 2018, Citizen's Lab published a report[41], in which it revealed that between August 2016 and August 2018, it scanned the Internet for servers associated with NSO Group's Pegasus spyware.[42] Citizen's Lab found 1,091 IP addresses that matched the fingerprint and 1,014 domain names that pointed to them. Citizen Lab developed and used Athena, a novel technique to cluster some of its matches into 36 distinct Pegasus systems, each one which appears to be run by a separate operator. Citizen's Lab designed and conducted a global DNS Cache Probing study on the matching domain names in order to identify in which countries each operator was spying. Its technique identified

---

[39] Pegasus and surveillance spyware, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, 2022, https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf

[40] https://bip.brpo.gov.pl/pl/content/rpo-ma-watpliwosci-dotyczace-zakupu-przez-cba-systemu-pegasus (own translation).

[41] Marczak B. et al., HIDE AND SEEK, Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries

[42] A previous report of Citizen's Lab from 2014 referred as well to Poland in the context of Milan based Hacking Team and their RCS spyware, see: https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/.

a total of 45 countries where Pegasus operators may be conducting surveillance operations. At least 10 Pegasus operators appear to be actively engaged in cross-border surveillance.

Citizen's Lab found suspected NSO Pegasus infections associated with 33 of the 36 Pegasus operators it identified in 45 countries, Poland, among others.

Citizen's Lab identified five operators that they believed are focusing on Europe. In case of Poland the name of the operator was ORZELBIALY, it started operating on November 2017 with focus on Poland.

Suspected infections were executed exploiting telecommunication networks of provides such as Polkomtel Sp. z o.o., T-mobile Polska S.A., Orange Polska S.A., Netia S.A., PROSAT s.c., Vectra S.A., FIBERLINK Sp. z o.o..

On August 28th, 2019, the tvn24.pl station in the magazine "Black on the White" informed about the results of a journalistic investigation, which showed that the Central Anticorruption Bureau has for two years been using a system called Pegasus, made available by the Israeli company NSO Group in Poland authorities through one of the Polish companies selling IT systems.[43]

In September 2019, Polish Ombudsman with a number of independent experts, including from foundation Panoptykon, published a highly critical report: "How to saddle Pegasus: observance of civil rights in the activities of secret services -assumptions of the reform."

In June 2021, foundation Panoptykon filed with the Sejm and the Senat, Polish President and Polish Prime Minister, a petition, signed by numerous other NGOs, for a reform on surveillance framework in Poland.

On 21 December 2021, media reported[44] that a Polish barrister had been targeted by Pegasus software,[45] compromising the lawyer's secrecy. Prosecution services declined to conduct an investigation into these matters.[46] Stakeholders expressed serious concerns in that respect, pointing at the likelihood that more lawyers were targeted in this specific way.[47]

Amongst the alleged targets there was reportedly also a prosecutor and two members of opposition parties and a business representative.[48] Reportedly, the Pegasus surveillance software was purchased

[43] https://tvn24.pl/polska/czarno-na-bialym-czy-cba-kupilo-system-pegasus-ra964707-2310942

[44] The initial statement on this development was published by the Associated Press (2021), AP Exclusive: Polish opposition due hacked with NSO spyware.

[45] The barrister concerned specialises in representing interests of politicians, including of a former President of the European Council, before Polish courts. See also the 2021 Rule of Law Report, Country Chapter on the rule of law situation in Poland, p. 12, footnote 90.

[46] On 29 December 2021, the public prosecutor's office informed the prosecutor reportedly affected by Pegasus attacks that her allegations are based on the information received from her phone's manufacturer. The prosecutor declined the request to submit her phone device for further examination by the prosecution services. See: RadioZet of 29 December 2021 where a statement of the prosecutor concerned is reproduced together with press statement of the public prosecutor's office.

[47] Including by pointing at the likelihood that more lawyers were targeted in this specific way. See Statement of 1 February 2022 of the Council of Bars and Law Societies of Europe. See also the Council of Bars and Law Societies of Europe contribution submitted in the context of the Rule of Law Report preparation

[48] The prosecutor concerned is a member of the association of prosecutors 'Lex Super Omnia' who initiated a criminal investigation in the case concerning the organization of the presidential elections in 2020 via post (see the 2021 Rule of Law Report, Country Chapter on the rule of law situation in Poland, p. 26, footnote 217). As confirmed in the Senate, one of the members of the opposition concerned, at the time of the alleged Pegasus-based surveillance, was the main person responsible for the parliamentary electoral campaign in 2019. The business representative allegedly targeted was the President of the association 'Employers of the Republic of Poland'; see Onet.pl of 19 April 2022, Citizen Lab: another

for the Central Anti-Corruption Bureau, which raised further concerns regarding the use of corruption investigations for political purposes.

The Minister of National Security and Defence Matters confirmed that the Pegasus software had been acquired.[49]

The Ombudsman submitted that judicial control in that respect is insufficient and courts do not know what type of surveillance would eventually be imposed by the State bodies.

The Senate set up an extraordinary committee to conduct an inquiry into these developments.

On January 18th, 2022, former Chairman of Supreme Audit Office (2013-2019) explained before the Senate's Special Committee that financial resources for the acquisitions of Pegasus spyware have been appropriated and committed. Further, that the appropriation and commitment were done in violation of budgetary law and in a way misleading as to the purpose of the acquisition. He has also presented invoices from the acquisition of the Pegasus software. Video recording from this session is available under link 1 and 2:

„Performing our statutory duties, we conducted an audit of the state budget implementation in part No. 37 for 2017. This audit was carried out at the beginning of 2018. And let me start with what is most important - what every citizen should in this room hear.

In the conclusion of this audit, we stated that the funds from the Justice Fund could not be transferred to the Central Anticorruption Bureau, because according to the Act on the Central Anticorruption Bureau, the activities of the CBA are financed exclusively from the State budget, and the resources of the State earmarked fund are not such funds. And it is not the basis, it is not an effective trick - because such a trick has been taken, an attempt to do so - changing the provisions of the Penal Code or changing the provisions of the Justice Fund Act, because the amendment to the Justice Fund Act did not change the Act on Secret Services, the Act on the Central Anti-Corruption Bureau and the Act on public finances, and it is in these acts that the financing of special services is limited only to funds from the State budget. And in the case when the legislator provided for the co-financing of a budgetary unit with funds from other sources - because there are such exceptions in other acts, e.g. on the Police.

If we have such a possibility, I would like to clarify, without any doubt, finally and definitively, whether the transfer of these funds, as well as the formal evaluation, has taken place. If we have the opportunity, I would like to show you a copy from the account of the National Bank of Poland, which will certify - I will provide all these documents to you in the form of evidence applications - that there has been a transfer of funds from the Ministry of Justice to the account of the Central Anti-Corruption Bureau with a description, that it was the implementation of an agreement concluded between the Justice Fund and the Central Anticorruption Bureau. The description of this invoice - because it is crucial and leaves

Pegasus victim in Poland.

[49] Wpolityce.pl of 7 January 2022, containing an interview in which the admission was made. On 14 January 2022, the Supreme Audit Office disclosed to the media two invoices which were assigned to the Central Anti-Corruption Bureau from the 'Justice Fund' – operated by the Ministry of Justice – to acquire 'means of special technique'. On 7 February 2022, the Supreme Audit Office organized a press conference where it informed the public that over 7000 'possibly dangerous' attacks had been conducted on electronic devices in possession of the Office's staff, including the President of the Supreme Audit Office. The Office has not confirmed that any of these alleged attacks had been carried out by means of the Pegasus software. According to the Office, financial means from the 'Justice Fund' could not be used for any such purchase in accordance with law. See minutes of the Senate's special Committee session of 18 January 2022.

no doubt - states that the invoice is a realization, confirmation of the purchase of special technology measures for crime detection and prevention. It is also important that the decision was not made at a low, official level. On this copy of the bill we have the signatures of people who certify - I will quote from the description of this copy - that: "We hereby make a statement that the information contained in the report on the implementation of this application" ... Here you have the original slide, it is the decision to remove the confidentiality obligation from me as a controller. Please go to the next slide. Another slide please. This is the copy I told you about of the transfer order from the account office of the Ministry of Justice to the account of the Central Anticorruption Bureau. On the next slide you have what is the essence of such an account: a description of what the funds were transferred to - that is, for the purchase of means of special technology used to detect and prevent crime. You may ask yourself why the name "Pegasus" is not explicitly mentioned here. As no one was using this name, attempts were made to hide it consciously in my opinion. This name was also unknown to us, not only to citizens, but also - and at this point I would like to thank them - the controllers of the Supreme Audit Office, who showed great professionalism in uncovering the arrangements for this purchase.

And, Ladies and Gentlemen, slide No. 4. Every decision, including the one that violates the law, is made by someone. Here you have the description on the next slide: we, the undersigned, declare that the information contained in these financial statements, which I show you on these copies, has been raised in accordance with the rules resulting from the relevant national legislation. Who signed this statement? Daniel Art, director of the Finance Office of the Central Anticorruption Bureau, and Mr. Ernest Bejda, head of the Central Anticorruption Bureau, were signed.

I would also like to point out here that all the documents that I use are not classified according to State regulations on legally protected secrets. I will also tell you later in my speech, if there is such an opportunity, that there are also documents classified by State clause. But the documents that I can show you today are the effect of removing the control secrecy so today I can use these documents in this mode.

Ladies and Gentlemen, I would just like to say that this invoice that you saw was launched in the sense - as you can see on the next slide - that these funds were used ... Here you have another slide - please - the so-called quarterly information on the use of funds received from the Victims' Aid Fund. And this document confirms the receipt of funds allocated to the task, in accordance with the concluded contract. Of course, we are talking about an agreement on the basis of which there was a purchase of means of special technology for the detection and prevention of crime, and in practice: the surveillance of citizens. "

Chairman Marcin Bosacki:

Do we see correctly that it is the sum of PLN 25 million? Yes?

President of the Supreme Audit Office in 2013–2019 Krzysztof Kwiatkowski:

This is the sum of PLN 25 million. Based on public documents, I can tell you that it was not the entire cost of purchasing this system. But here we have that sum included. Why? The fact that the Supreme Audit Office's auditors managed to capture this purchase is the result of the fact that the beneficiary, i.e. the Central Anticorruption Bureau, provided confirmation, informed about the use and implementation of the contract with the Justice Fund. The Supreme Audit Office was able to identify this document and, as a consequence, Polish citizens can find out about it today, because it is in public

documents from the control of the Justice Fund, which, as I read to you, we assessed negatively - and this negative assessment is also included in the official document analysis of the implementation of the state budget for 2017, which I presented to the Sejm.

And on the last, next slide you have directly written: "The invoice concerns the purchase" ... This is the invoice of the company that delivered this product, and the next slide is the description of this invoice, where we can read: "The invoice concerns the purchase of a system co-financed by the Aid Fund. The aggrieved party "- that is, the so-called Fund of Justice - and "The invoice has been settled in full". This is the first tranche, directly from the special fund.

And Ladies and Gentlemen, at the end of my introductory speech, I would like to make you aware of one more thing. Those who made these decisions, and those who carried them out, are, in my opinion, at least aware that they violated the law or acted on its border. The Supreme Audit Office's assessment is that it was a violation of the law. Why? I am going to show you an exceptionally important document - this is the next slide - on which slide you can ... Please, another slide. You can read ... This is a letter of February 15, signed by Minister Michał Woś, Undersecretary of State in the Ministry of Justice, addressed to Mr. Jarosław Wyżgowski, director of the Administration and Finance Office. And what can we read in this letter? I quote: "I would like to inform you that the earmarked subsidy from the funds received from the Justice Fund in connection with the contract concluded with the Central Investigatory Office has been settled in full". I would like to draw your attention to the phrase "I would like to inform you that a targeted subsidy". Why? There is a mistake - which is also shown by the professionalism of those who wrote it - because it says not "with the Central Anti-Corruption Bureau", but there is another unit entered. But you have another letter on the same matter, already signed here by a person who also has an extremely important role in this matter, by director Mikołaj Pawlak, then director of the Department of Family and Juvenile Affairs, who informs - 3 days later, [...] - that, and I quote: "I inform you that the transfer of funds from the Justice Fund - attention! - it was not a targeted subsidy ". That is, in the Ministry of Justice, within 3 days, various versions of the formal and legal nature of these measures were developed. I have no doubts that it was related to the commenced and already ongoing inspection of the Supreme Audit Office, which assessed from the formal point of view - also in terms of the Public Finance Act - the correctness of the decision taken.

[...]

I have already talked about the representatives of the services, but please note the next slide. This is a letter from the head of the Central Anticorruption Bureau, Mr. Ernest Bejda, to the Minister of Justice, Mr. Zbigniew Ziobro. In this letter of September 15th, 2017 - please, if technically possible, show it - we read that "Referring to previous arrangements" ... This is what the head of the Central Anticorruption Bureau writes to the Minister of Justice Zbigniew Ziobro: I'm asking for "… Please… This is not the slide, please see another one. He writes: "I am applying for the transfer of the agreed amount in order to carry out the task consisting in the purchase of means of special technology for the detection and prevention of crime." This letter is a letter sent by the head of the CBA, Ernest Bejda, to the Minister of Justice Zbigniew Ziobro. And at the bottom we read that this letter is for the attention of Mariusz Kamiński, minister, member of the Council of Ministers, coordinator for special services. This shows that the most important public officials at the level of the Ministry of Justice and at the supervisory level over special services were informed about this transaction by means of official letters. Of course, I also attach this letter as evidence to the work of the commission.

[...]

Ladies and Gentlemen, I am holding in my hands a copy of the application to Mr. Maciej Strójwąsa, the commissioner for public finance discipline, competent in cases adjudicated by the committee formed at the Prime Minister's Office. This application was made on July 18th, 2018, i.e. when I was in charge of the work of the Supreme Audit Office. And what do we read in this application? "Notification of breach of public finance discipline. Supreme Audit Office, Department of Order and Internal Security, acting on the basis of the Act on Supreme Audit Office and the responsibility for violation of public finance discipline - here the relevant act - informs that in the course of the performance audit carried out in the period from January 5 to April 4, 2018 at the Ministry of Justice concerning the State's budget for year 2017, in part 37 "Justice" - and here the most important fragment - ascertained circumstances indicating violation of public finance discipline, as defined in Art. 11 of the Act on liability for violation of public finance discipline, consisting in the fact that in the period from September 14th, 2017 to September 29th, Undersecretary of State Michał Woś, acting under the authority of the Minister of Justice as the administrator of the Justice Fund, contrary to the authorization granted by the Minister of Finance and the opinion of the Parliamentary Public Finance Committee, in connection with the change in the fund's financial plan, made a decision resulting in the transfer of funds in the amount of 25 million to the budgetary unit, i.e. the CBA, for tasks other than those resulting from this authorization, despite the fact that this unit may be financed only from the State budget, which was in breach of Art. 11 of the Public Finance Act and Art. 4 of the Act on the Central Anticorruption Bureau ". Here we have the audit evidence listed in detail in this application and of course a description of the whole situation.

And now you can ask what happened with the notification of the constitutional body of State control, which is the Supreme Audit Office. This notification - I would like to remind you that I am discussing it in the part concerning the Justice Fund, because here I was able to tell you about the notification, and in the part concerning the Central Anti-Corruption Bureau - it is closed - it was refused even to initiate an investigation. This is the decision of the public finance discipline commissioner by the Chancellery of the Prime Minister. We… If we can, we can show these decisions. This is the original decision, the July 13th notice to the finance discipline commissioner, and this is the decision to refuse to initiate. This decision was signed by the public finance discipline commissioner by the Chancellery of the Prime Minister.

[...]

On November 29th, 2018, we filed a complaint against the decision of the public finance discipline commissioner. In accordance with the applicable procedure, we submitted this complaint to the appeal body, i.e. to the chief commissioner for public finance discipline, Mr. Leszek Skiba, the current deputy minister of finance. And in this complaint we raised the same arguments that we raised in the application. And, ladies and gentlemen, the key thing. This is the last slide in this regard. The decision in this regard was made - it is hard to believe, knowing the deadlines resulting from administrative procedures - almost 2 years later. The decision was finally made only in September 2020.

And here I can even tell you about two decisions, because just as the complaint was declared clasified, the decision is fortunately public. Here I have a decision that refuses to initiate an investigation for infringement of regulations - attention! - at the Central Anticorruption Bureau. This is the decision of September 2020. But there is a very important passage here: "I am changing the contested decision of the first instance." Why is this such an important passage? I will read to you only one sentence from this decision signed by Piotr Patkowski, i.e. the deputy minister of finance, and which in this respect changed the previous provisions. And why is she so important? Ladies and Gentlemen, in this letter we

can read that the discipline commissioner considered the correct conduct of the CBA related to the use of the commissioned sum structure and, consequently, assessed the lack of changes to the financial plan as correct, but the complainant - i.e. the Supreme Audit Office - did not share this argument and raised it. And here are two important fragments of this provision: “It cannot be effectively concluded, in the opinion of the complainant, that the provisions of the ministerial decree relating to the type of bank accounts could modify the basic statutory principles defining the method of financing State budgetary units. In this respect, it is difficult to disagree with the complainant. " In his decision, the deputy finance minister says: The Supreme Audit Office is right. In this regard, as for the method of assessing this operation in the accounting and financial dimension, performed by the Supreme Audit Office - let me repeat - it is difficult to disagree with the assessment of the Supreme Audit Office.

Later in the same decision we read: "Taking into account the above circumstances, it should be concluded that the conclusion of the public finance discipline commissioner of the first instance that the act indicated in the notification does not constitute a violation of public finance discipline is unfounded." Ladies and Gentlemen, the motion of the public finance discipline commissioner of the first instance, who refused to initiate proceedings in this case, is, in the opinion of the second instance commissioner, unfounded. With this statement, Deputy Minister Piotr Patkowski confirmed the violation of the law.

And the last sentence that I would like to recall to you from this decision: "The circumstances of the allegation made by the notifying party, the complainant - that is the Supreme Audit Office - make it necessary to consider whether there are grounds for refusing to initiate the investigation in the case due to the negligible harmfulness of the act to public finances." For Minister Patkowski, several tens of millions of zlotys are negligible harm to public finances. For a citizen it is a signal that wiretapping a citizen is a negligible act. Of course, I do not agree with this justification, but I do agree with that part when the public finance discipline commissioner stated that there was a breach of the regulations. In my opinion, this violation was not of a minor harmful nature.

[...]

The Justice Fund… This is not its name at all, it is the name after the changes. This fund was called "Crime Victims and Post-penitentiary Aid Fund" - I say this as the former Minister of Justice who created this fund. This money, in return, previously went to social organizations that helped women subject to violence, children with suicidal thoughts, and they could be used to finance emergency calls, so that such children would not take their lives. Nobody ever thought - and I am saying this as a person who was in the preparation of this law - that this fund would finance special services. That's not the title. The State may finance secret services, including purchases from the operational fund, but in a different way - in accordance with the Public Finance Act and the Service Act, so that citizens have supervision, at least on a general level, over the services, through the services budget, and not by secretly transferred money from the Justice Fund, that is, the fund to help victims, to serve quite different purposes, social goals, of which there is indeed a lot. And based on this legal analysis, the most important fragment, the Supreme Audit Office College dismissed the reservations made by the secretary of state in the Ministry of Justice in this respect and upheld ...

[...]

The role of the children's Ombudsman, i.e. the then director of the Department of Family and Juvenile Affairs, was crucial in terms of handling the entire operation. I have a letter of September 13th, 2017

before me. It is a letter addressed to Jan Paziewski, director of the Budget and Financial Efficiency Department at the Ministry of Justice. And signed by whom? By the director of the Department of Family and Juveniles, Mr. Mikołaj Pawlak. What do we read in this letter? "I would like to kindly ask you to change the financial plan for the Victims' Assistance Fund and Post-penitentiary Assistance in accordance with the attached project. Justification: On August 12, an amendment to Art. 43 of the Executive Penal Code relating to the Fund. The legislator envisaged extending the forms of assistance that may be financed from the Fund's resources and expanding the catalog of entities that can provide such assistance. It is important that funds from the Fund may also be transferred to public finance sector entities. The legislator also changed the statutory authorization for the Minister of Justice to issue executive regulations. The current financial plan concerned only the implementation of the fund's tasks in the field of assistance to victims provided through units not included in the financial sector ". And here the key point: "The accumulated funds of the Justice Fund allow for the financing of the tasks entrusted by the legislator - new tasks - while the proposed change fully corresponds to the classification of tasks provided for by the act, taking into account planning requirements at the same time." And here is the most important fragment of this letter: "The administrator presents the change of planned funds in the plan for 2017". And here we read: "other - 25 million".

The Supreme Audit Office auditors followed this lead - what is "other" in the amount of PLN 25 million? Thanks to this, we revealed the transfer of these funds to the CBA.

[...]

During the period under control, during these operations related to changes to the Justice Fund, with the transfer of funds, also - as you have read - during the issuance of certain approvals from the Ministry of Finance, e.g. to change the plan, during this period, specifically, from September 28th, 2016 to January 9th, 2018, Mateusz Morawiecki was the Minister of Finance, and at the time of the inspection activities, from January 9th, 2018 to June 4th, 2019, Teresa Czerwińska was the Minister of Finance. Of course, the audit concerned decisions that were made in 2017."[50]

Regarding Pegasus, **current president of the Supreme Audit Office, Maria Banaś** reconfirmed:

"Tools of special technique Pegasus. As a result of the control of the implementation of the State budget for 2017 by the CBA and the Ministry of Interior and Administration, the Supreme Audit Office established the fact of illegal co-financing of the CBA's activities by the Justice Fund in the amount of PLN 25 million, which was used for the purchase, as stated in the financial documentation, of operational technique funds. During the inspection, however, Supreme Audit Office did not obtain information on what type of software was purchased, because of the secrecy related to the forms, means and principles of operational and reconnaissance activities. On September 15th, 2017, the then head of the Central Anticorruption Bureau, Mr. Ernest Bejda, referring to previous arrangements, pursuant to Art. 43 §8 point 1c of the Act - Executive Penal Code applied directly to the Minister of Justice, Zbigniew Ziobro, to transfer the agreed amount to the CBA in order to perform the task consisting in the purchase of means of special technology for the detection and prevention of crime. According to the above letter, the application addressed to the Minister of Justice was also

[50] Own translation.

communicated to Mariusz Kamiński, the coordinator of the special services. Then, the head of the CBA, Ernest Bejda, with a request submitted on October 3, 2017, asked the Minister of Justice - the Prosecutor General, that the first tranche of funds in the amount of PLN 13 million 360 thousand was paid on the basis of the previously concluded CBA agreement. As a result of the submitted application, the Undersecretary of State in the Ministry of Justice, Mr. Michał Woś, in a letter of October 6, 2017, requested the director of the Administration and Finance Office of the Ministry of Justice that, in connection with the implementation of the classified agreement of September 29th, 2017, concluded with the Central Anticorruption Bureau for the amount of PLN 25 million, paid the first tranche of funds in the amount of PLN 13 million 360 thousand from the account of the Victims Assistance Fund and the Post-penitentiary Assistance Fund - by October 9th, 2017. The letter was also sent for information to the director of the Department of Budget and Financial Efficiency of the Ministry of Justice. The head of the CBA sent another request to the Minister of Justice on November 10, 2017, in which he requested the payment of the second tranche of funds in the amount of PLN 11 million 640 thousand. As a result of the submitted application, the Undersecretary of State in the Ministry of Justice, Mr. Michał Woś, also in a letter of November 15th, 2017, asked the director of the Administration and Finance Office of the Ministry of Justice, that in connection with the implementation of the classified agreement of September 29th, 2017, concluded with the Central Anticorruption Bureau for the amount of PLN 25 million, paid the first tranche of funds in the amount of PLN 11 million PLN 640 from the account of the Victims Assistance Fund - Justice Fund by November 20th, 2017. This letter was also communicated to the director Department of Budget and Financial Efficiency. It is also worth emphasizing that the director of the Department of Family and Juvenile Affairs, in a letter of February 18, 2018, addressed to the director of the Administration and Finance Office, informed that the transfer of funds from the Justice Fund - Victims Assistance Fund and Post-penitentiary Assistance under the contract concluded with the Central Anticorruption Office on September 29, 2017 was not a special-purpose subsidy. Finally, it should be noted that the CBA received 2 advance invoices from Matic Sp. z o.o. The first invoice was issued on October 3, 2017, the invoice documents the purchase by the CBA dated October 3, 2017 and indicates the first installment - an advance payment - indicated in art. 9 point 2.1 for the performance of the agreement of September 29, 2017 for the amount of PLN 13 million 360 thousand. The second advance invoice was issued by Matic Sp. z o.o. on November 9, 2017. This invoice documents the purchase by the Central Anti-Corruption Bureau dated November 9, 2017 and also indicates the second installment, on the basis of the acceptance protocol of November 7, for the amount of PLN 11 million 640 thousand. The above circumstances were established as a result of the audit of the State budget implementation for 2017 at the CBA and the Ministry of Interior and Administration. In this respect, it is worth recalling that despite the notifications submitted by the Supreme Audit Office about the possibility of violating the public finance discipline referred to in Art. 11 of the Act on Violation of Public Finance Discipline, i.e. the allegation of spending public funds without authorization or exceeding it by the head of the CBA Ernest Bejda and Michał Woś, the main commissioner for public finance discipline Piotr Patkowski, current deputy minister of finance, by the decisions of September 14, 2020 [proceeded with the procedure] - despite it being clearly stated that the acts alleged by the Supreme Audit Office fulfill the criteria of violation of public finance discipline"[51]

[51] Own transaltion.

During subsequent five months Senate's Special Committee heard numerous victims to understand the nature of abusive surveillance and experts in order to understand legal qualification of the abusive surveillance.

3.1.2. Lists of victims

A study prepared for the European Parliament's PEGA Committee by Policy Department C indicates that Pegasus had been used against the following Polish personalities:

- **Roman Giertych**, lawyer working for Donald Tusk, leader of Civic Platform (18 intrusions)(expertise prepared for Mr Giertych concerning his phone in English version)(transcript of testimony to Senate's Special Committee),

- prosecutor **Ewa Wrzosek,**[52] (transcript of testimony to Senate's Special Committee)

- Civic Platform Senator **Krzysztof Brejza**, coordinating his party's election campaign (33 intrusions)(testimony before Senate's Special Committee and videorecording),

- agrarian social movement leader **Michal Kolodziejczak,** (transcript and videorecording from Senate's Special Committee meeting,

- author and former collaborator of the Polish secret services **Tomasz Szwejgiert,**

- the **Supreme Audit Office** affirmed that its employees have been put under surveillance,[53]

- **Adam Hofman**, former PiS spokesman,

- **Dawid Jackiewicz**, former PiS Treasury Minister in the Cabinet of Beata Szydło

- **Mariusz Antoni Kamiński**, former PiS MP, (transcript and videorecording from the meeting of April 29, 2022, of Senate's Special Committee)

- **Bartłomiej Misiewicz**, former head of the PiS cabinet and former spokesman of the Ministry of National Defence,

- **Katarzyna Kaczmarek**, wife of Tomasz Kaczmarek [pl] (referred to as "agent Tomek"), former policeman and former CBA officer, later a PiS MP. [54]

A study prepared by DG EPRS of the European Parliament indicated that first used in Poland in 2017 to surveil former spokesman of the Ministry of National Defence Bartłomiej Misiewicz and former PiS MP Mariusz Antoni K., now accused of influence peddling and exposing the Polish Armaments Group to a loss of 1.2 million złotys. Other potential Pegasus targets formerly associated with the ruling party PiS include Adam Hofman and Dawid Jackiewicz, who were involved in the 'Wrocław Collusion' corruption affair. According to sources, Katarzyna Kaczmarek, the wife of former CBA agent and former PiS MP Tomasz Kaczmarek ('agent Tomek'), was surveilled with Pegasus due to her knowledge of potentially

[52] See https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e

[53] See https://notesfrompoland.com/2022/02/07/polish-state-auditor-claims-7300-cyberattacks-made-against-it-including-suspected-use-of-pegasus/

[54] See https://wyborcza.pl/7,75398,28009790,40-licencji-na-pegasusa-ujawniamy-kogo-jeszcze-inwigilowaly.html?disableRedirects=true

damaging information about the internal affairs of Mariusz Kamiński, Minister of the Interior and Administration and Coordinator of Special Services.

Most prominently, targets include opposition figures and their associates, such as: lawyer (and former politician) Roman Giertych, representing opposition leaders including Donald Tusk, who, according to his lawyer, was the real target; prosecutor Ewa Wrzosek, who launched an investigation into the organisation of the (eventually called-off) May 2020 presidential elections by postal voting; opposition Senator Krzysztof Brejza, as well as his father and former assistant; founder of the 'Agrounia'farmers'movement Michał Kołodziejczak; journalist Tomasz Szwejgiert, co-author of a book about Kamiński's activities as CBA chief; and possibly former (under the Civic Platform government) head of the Central Anti-Corruption Bureau Paweł Wojtunik, as well as former Minister of Transport Sławomir Nowak, who was arrested three days before the second round of the presidential election on suspicion of corruption, management of an organised criminal group, and money laundering. 85 Concerning the latter, Mariusz Kamiński formally rejected allegations that Sławomir Nowak was under surveillance in the run-up to elections. Roman Giertych assumes that messages obtained through Pegasus were modified and disseminated as part of smear campaigns to discredit him. Recently, it was revealed that the President of Employers of Poland, Andrzej Malinowski, had been surveilled with Pegasus. He suspects that this could have been related to, among other things, his activities in the Social Dialogue Council, his contacts in Poland and abroad, and his columns critical of PiS, published in Rzeczpospolita.

Additionally, relatives of potential and confirmed Pegasus targets have fallen victim to spoofing attacks.

Victims heard by Senate's Special Committee included also Magdalena Łośko - (MP)(a list of sms messages sent to infect her phone)(transcript of her testimony) and Pawel Tamborski[55].

3.2. Legal framework concerning data protection and surveillance in Poland

3.2.1. European law

The European Data Protecton Supervisor in his Preliminary Remarks on Modern Spyware (annex I to this briefing note) clarified that when it is used for law enforcement purposes, targeted surveillance has to comply with applicable Union primary and secondary law.

The legal conditions and safeguards for the use of digital surveillance and communication interception have been subject to extensive analysis and interpretation of the Curt of Justice of the European Union. In particular, in the judgement on Joined Cases C-511/18 and C512/18 (La Quadrature du Net and Others) the CJEU clarified the applicability of EU law to certain measures adopted on national security grounds.

CJEU acknowledged that a serious threat to national security, genuine and present or foreseeable could justify serious interference with fundamental rights, subject to strict conditions and safeguards. **Necessity** implies in this case the need for a combined, fact-based assessment of the effectiveness of

[55] https://wyborcza.pl/7,75398,28700262,czego-cba-szukalo-u-bylego-wiceministra-skarbu-inwigilowani.html

the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal.

Concerning extreme level of intrusiveness of Pegasus (interfering with every aspect of life of person subject to surveillance and people in her surroundings) according to testimonies given to Polish Senate's Special Committee, there are other tools that could serve the same purpose with less intrusiveness, thus being more **proportionate** for the purpose.

EDPS indicates that Pegasus could potentially pass the necessity and proportionality test solely in cases of **imminent terrorist attack or such cases as abduction where physical threat is eminent**. In fact, Pegasus is unfit as a tool for evidence collection since its use **could actually encroach on the right to fair trial**.

Polish Ombudsman repeatedly mentioned in his interventions the standard of admissibility of interference by State authorities in the content of communication. Both the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) do not allow the possibility of surveillance of citizens without providing the necessary legal guarantees, pointing to the obligation to establish a clear and distinct basis legal, which categories of persons could be subject to surveillance and their possible link to the terrorist threat; necessity justifying the need for access to information by the services; the need for precise definition of the maximum period during which supervision may be carried out, and - in particular - to ensure effective means of control on the activities of the services[56]

The European Data Protection Supervisor pointed that the use of digital surveillance tools by EU Member States authorities for national security purposes, even when it falls outside the scope of Union law on the basis of art. 4(2) TEU, is nevertheless subject to national constitutional law as well as the relevant legal framework of the Council of Europe, in particular the European Convention on Human Rights.[57]

It is important to add that the exemption foreseen in art. 4(2) of the Treaty on the European Union applies to measures having as their purpose national security. However, in the case of Pegasus use in Poland various testimonies indicate that **the purpose was politically motivated and served surveillance of the opposition**.

PEGA Committee has been provided with an Opinion of Legal Service of the European Parliament that explains in detail this issue.

In the context of necessity test it is important to note the statement of the Head of Couter-Military Intelligence Service Szef Służby (2014–2015) general Piotr Pytel (Senate's Special Committee heariing of 23-02-2022 (transcript):

„On the other hand, what the Central Anticorruption Bureau can draw from the application of operational control measures is, first of all, the recording of evidence for the purposes of criminal proceedings. I don't see a Pegasus application here. The existing measures, classic for the anti-corruption bureau, from before the Pegasus type devices and systems, and they are also often advanced technologies, are completely sufficient. So I would rather opt for a version of the events - of

[56] Examples include the older Weber and Saravia cases, case no. 54934/00; Rotaru v. Romania, application no. 28341/95; Uzun v. Germany, application no. 35623/05. Recently, the ECtHR has dealt with this issue, for examplein the cases of Szabó and Vissy v. Hungary, application 37138/14, Zakharov v. Russia, application no. 47413/06 or Big Brother Watch and others v. Great Britain, applications 58170/13, 62322/14 and 24960/15. On the other hand, in the case of the CJEU, see the judgment of the CJEU of 8 April 2014 in joined cases C-293/12 Digital Rights Ireland and C-594/12 Kärtner Landesregierungi in or the judgment of 21 December 2016 in joined cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis.

[57] CJEU judgment on Joined Cases C-511/18 and D-512/18, La Quadrature du Net and Others, para 103.

course I can elaborate on it later - regarding the use of this Pegasus in the area we define, what we call the operation of special services in the field of politics. Obviously, it is illegal, illegal and contrary to the ethos of the services. In my opinion, this evidence obtained by Pegasus, via Pegasus in the activities of the Central Anti-Corruption Bureau, of course, in a very simple way, i.e. in a way that, I would say, quite obvious from the point of view of the characteristics of this system, should be rejected by the court, should not be accepted."[58]

Authors of this report would like to add that among European provisions violated by the acquisition and the use of Pegasus spyware are in particular provisions of the art. 2 of the Treaty on the European Union, the rights enshrined in the Charter of Fundamental Rights of the European Union, in particular under art 7, article 8, art. 17, art. 21, art. 41, art. 42, art. 47, art. 48, Data Protection Regulation, the e-Privacy Directive and the Law Enforcement Directive.

Final remark concerns the right to property guaranteed under art 17(1) of the Charter of Fundamental Rights of the European Union which provides that "[e]veryone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest".

Unlike classical surveillance tools which utilise tools and materials that belong to surveillance agencies, Pegasus makes use of a mobile phone and of the internet connectivity of the victim. The mobile phone, including its camera, microphone and memory, is the property of the victim while internet connectivity is paid for by the victim, while surveillance data transfers potentially trigger financial costs on the part of the victim. This constitutes clear interference with the right to property as protected by aforementioned art. 17.

3.2.2. International law

The requirement of effective oversight of special services results from i.e. article 13 of the European Convention of Human Rights, which states that everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity. This provision – as well as case-law of the ECtHR – requires to establish a national authority, which is competent to hear the claim based on Article 13 ECHR and which is independent from the executive power. The analysis of the binding law leads to a conclusion that the access to such effective remedy – in case rights are being violated by covert actions conducted by the special services – is not available e.g. in the Polish law.[59]

The amendment introduced by the Act of 15 January 2016 amending the Polish Police Act, [...] has already been subjected to the analysis of compliance with the European privacy standard by the Venice Commission in June 2016. Moreover, another basic challenges in ensuring effective oversight of special services results from the international intelligence cooperation. These challenges were expressed i.e.

[58] Own translation.

[59] https://depotuw.ceon.pl/handle/item/2143

in two judgements of the ECtHR issued in 2014 concerning the Polish involvement in so called extraordinary rendition programme (Al Nasiri v. Poland and Abu Zubaydah v. Poland). Additionally, the Court expressed a concern whether a democratic oversight of intelligence services in Poland is effective enough in order to guarantee protection of rights and freedoms. The analysis shows the need to introduce changes into existing law dealing with tasks and competences of special services in Poland. Lack of precision in defining the statutory tasks of special services is not supplemented with the adequate procedural safeguards (e.g. there is still lack of follow-up assessment of the legality and necessity of collected data). Legislative amendments should be introduced in order to implement the recommendations of the Venice Commission, concerning establishment of an independent expert body responsible for conducting everyday oversight of the use of the cover powers by the special services. This authority should also be equipped with the competence to hear the individual complaints concerning covert actions carried out by special services, in particular to verify the legality of interference with rights and freedoms.[60]

On 29 September 2017 and 12 February 2018 applications were lodged with the European Court of Human Rights by Mr Mikołaj Pietrzak (dean of Warsaw Bar), Ms Dominika Bychawska-Siniarska and Ms Barbara Grabowska-Moroz, (members and employees of the Helsinki Foundation for Human Rights); Mr Wojciech Klicki and Ms Katarzyna Szymielewicz (members of the Panoptykon Foundation), Polish nationals (Pietrzak v. Poland and Bychawska-Siniarska and Others v. Poland (nos. 72038/17 and 25237/18). Relying on Article 8 (right to respect for private and family life) of the Convention, the applicants complain that the secret systems for monitoring communications (telecommunications, postal and digital communications) and gathering metadata, introduced in application of the Law of 15 January 2016 amending the Police Act and certain other laws, and the Anti-Terrorism Act (Law of 16 June 2016), interfere with their right to respect for their private life. Relying on Article 8 taken together with Article 13 (right to an effective remedy), the applicants allege that they had no effective remedy which would have enabled them to establish whether they themselves had been subjected to secret surveillance and, if necessary, to have the lawfulness of that surveillance reviewed by a court.

A hearing is forthcoming in this case on 27 September 2022.

3.2.3. Polish law

The acquisition and the use of Pegasus spyware violated a number of provision of Polish Constitution, including:

"Art. 2 The Republic of Poland shall be a **democratic state ruled by law** and implementing the principles of social justice.

Art. 5 The Republic of Poland shall [...] ensure the **freedoms and rights of persons and citizens** [...]

Art. 7 The organs of public authority shall function on the **basis of, and within the limits of, the law**.

[60] https://depotuw.ceon.pl/handle/item/2143

Art. 9 The Republic of Poland shall **respect international law** binding upon it.

Art. 10 The system of government of the Republic of Poland shall be based on the **separation of and balance between the legislative, executive and judicial powers**.

Art. 21 The Republic of Poland shall **protect ownership** [...].

Art. 30 The inherent and inalienable dignity of the person shall constitute a source of freedoms and rights of persons and citizens. **It shall be inviolable**. The respect and protection thereof shall be the obligation of public authorities.

Art. 31

1. Freedom of the person shall receive **legal protection**.

[...]

3. Any limitation upon the exercise of constitutional freedoms and rights may be imposed only by statute, and only when **necessary in a democratic state for the protection of its security or public order**, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations shall not violate the essence of freedoms and rights.

Art. 41 **Personal inviolability and security** shall be ensured to everyone. Any deprivation or limitation of liberty may be imposed only in accordance with principles and under procedures specified by statute.

Art. 45 Everyone shall have the right to a **fair and public hearing of his case**, without undue delay, before a competent, impartial and independent court.

Exceptions to the public nature of hearings may be made for **reasons** of morality, State security, public order or protection of the private life of a party, or other important private interest. Judgments shall be announced publicly.

Art. 47 Everyone shall have **the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life**.

Art. 49 **The freedom and privacy of communication shall be ensured**. Any limitations thereon may be imposed only in cases and in a manner specified by statute.

Art. 50 The **inviolability of the home shall be ensured**. Any search of a home, premises or vehicles may be made only in cases and in a manner specified by statute.

Art. 51

1. **No one may be obliged, except on the basis of statute, to disclose information concerning his person**.

2. **Public authorities shall not acquire, collect nor make accessible information on citizens** other than that which is **necessary** in a democratic state ruled by law.

3. **Everyone shall have a right of access to official documents and data collections concerning himself**. Limitations upon such rights may be established by statute.

4. Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or **information acquired by means contrary to statute**.

5. Principles and procedures for collection of and access to information shall be specified by statute."[61]

In the context of the Pegasus system and its purchase and use by Polish State services, the principle of legality referred to in Art. 7 of the Polish Constitution was violated. No legal provision allows any State authority to break security and intercept and use, in this way, the content of communication messages and gain access to any information and data from a mobile device. Also, the legal provisions regulating the principles of applying operational control do not allow it. This is not allowed even by the provisions of the Act of June 10, 2019 on anti-terrorist activities or any other provisions regulating the activities of individual services, including in particular the provisions of the Act of June 9, 2006 on the Central Anticorruption Bureau.

The tasks of the CBA do not include activities for which the Pegasus system could be useful in the context of combating terrorism (cf. Articles 1 and 2 of the Act on the Central Anti-Corruption Bureau).

A report on acceptance of the acquisition and use under operational control of a specific type of computer programs (casus Pegasus) prepared by the Jagiellonian University[62] contains the following conclusions:

1. The use of ICT systems, the integral part of which are computer programs that allow recording, without the user's knowledge and consent, telephone conversations and downloading SMS / MMS messages and messages from communicators used by the person subjected to operational control, including messages sent and received before the date of commencement of operational control, is in accordance with the provisions of Polish law, provided that the computer program used for this purpose has been **accredited** by the Internal Security Agency or the Military Counterintelligence Service and are used to **ensure the security of classified information**, the functionalities of which do not allow **interference with the content of data** stored in the device or making these **data available to third parties** , unauthorized to access classified information.

2. The use of computer programs that allow recording the content of conversations and the image in rooms where there is a telephone / tablet / other device, after taking control of the device and activating the microphone or camera by the services, is **contrary to the provisions of Polish law**, which do not provide for the competence of the services to **actively** use the functionality of an IT system or terminal device in order to aggregate data that is not in the controlled IT system as a result of the activity of user's of this system or as a result of its individual configuration.

[61] https://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm Emphasis added.

[62] Barczak-Oplustil A. et al., Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (casus Pegasusa), 2022, https://kipk.pl/ekspertyzy/casus-pegasusa/

3. The use of computer programs that download from the phone / tablet / other device of a person under operational control, access data (passwords / keys) enabling logging in to servers with e-mail, banking, and social networks is in accordance with the provisions of Polish law; however, **viewing and downloading data collected in these IT systems after separate logging** into them by the services using the downloaded access data (passwords / keys) it **is contrary to the provisions of Polish law**.

4. The use of computer programs downloading from the phone / tablet / other device of the person subject to operational control all its content stored in the device during and before the commencement of the operational control raises doubts as to the compliance with the provisions of Polish law in the context of meeting ***in concreto* the constitutional principle of proportionality, and is contrary to the provisions of Polish law**, when computer programs not accredited by the Internal Security Agency or the Military Counterintelligence Service are used for this purpose, which do not ensure the security of classified information, or whose functionalities allow interference with the content of data stored on the device, or the use of which involves the provision of these data to third parties unauthorized to access classified information.

5. The use of computer programs as part of the operational control allowing access to all or part of the IT system on the phone / tablet / other device of the person subjected to operational control and **making changes to their content** (including adding, editing or deleting files) **is contrary to the provisions Polish law**.

6. The acquisition and use of computer programs, the use of which as part of operational control involves **the transfer of obtained data to third parties**, not authorized to access classified information, in particular administrators or intelligence services of foreign countries, **is contrary to the provisions of Polish law**.

7. The application for operational control submitted to the court should define the purposes, scope and method of control, including the computer programs used, along **with an indication of their functionality in the context of the type, sources and quantity of information** obtained, as well as the time scope of data collection.

8. In the light of the constitutional standard, a person subject to control should have the right to be notified about the completion of operational inspection and to submit a complaint to an independent inspection body about operational activities undertaken against him.[63]

According to the Head of Couter-Military Intelligence Service Szef Służby (2014–2015) general Piotr Pytel (Senate's Special Committee hearing of 23 February 2022 (transcript):

"The use of a private telephone of the person subject to control, the so-called terminal device for collecting image and sound from the environment is unacceptable from the point of view of Polish law. There is no such possibility, there are no such regulations. These are not the actions of that person consisting in the use of this device or changing its properties, i.e. they are not products of his activities in the form of a conversation, in the form of saving some files, to which, under the current law, after changing the provisions of the acts of individual services regarding operational control ... in point 4 it was developed that you can actually suck this type of data. Well, it is not a device that is controlled by the service as a material harvesting device under operational control, and it cannot be, because the authorized service has no control over this device. This is not a device that belongs to the service. If

[63] Own translation.

viewing is used or recording is used in a place, in a specific room - in fact, it should be specified in the application for operational control, where this place or room is located - then the services use their own devices. So this is unacceptable.

Finally, very generally, the use of the Pegasus system is illegal because the system cannot be certified. I talked to specialists who certified systems in terms of ICT security in the services, I have many friends with whom I worked. This system cannot be certified. This results in a very high probability of disclosing to unauthorized persons classified information protected with the following clause: top secret. Why the clause: top secret? Because operational control is not really an autonomous procedure from a service point of view. It results from the procedure carried out, which is documented in the form of materials in a specific set, limited to this procedure, and these materials are protected to the level of the highest clause: top secret. So here we have disclosure of the interests concerning the people subject to the control. We also have the possibility, first of all, maybe not primarily, of obtaining information by a foreign service that may compromise the Polish government, if the services under the supervision of ministers Kamiński and Wąsik carry out illegal activities. Recent press reports related to the Pegasus hacking on the phone of Mr. Ryszard Brejza indicate that most likely we were dealing with an activity that took place outside of operational control. I can somehow relate to it later."[64]

General Pytel's remark that Pegasus makes use of a mobile phone of the victim, unlike classical surveillance tools that depend on the equipment of surveillance authorities triggers also a conclusion that using private property (the mobile phone, including its camera, microphone and memory - the property of the victim as well as the internet connectivity which is paid for by the victim, while surveillance data transfers potentially trigger financial costs on the part of the victim) for the purposes of surveillance executed by means of Pegasus meets the prerequisites of chapter XXXV of Polish Criminal Code, including art. 278 on theft, and art. 285 on triggering phone impulses and art. 287 on computer fraud.

Prof. Andrzej Zoll during Senate's Special Committee hearing of February 23, 2022 (transcript) clarified that Pegasus is illegal in Poland due to its missing certification, possible leakages and potential manipulation of data:

„Now: what is data protection all about? It is about making the tools with which we obtain this data absolutely tight, that this data does not go outside, that it cannot be picked up by third parties who do not have the authority to access this data. This is the first task of data protection: that there is no leakage from the operational control process. The second problem, which is no less important, is that in the process of making the data set, i.e. during the operational control period, it is impossible to manipulate the data, i.e. the information collected on the tool used by the person under surveillance. Here, in particular, it is about such manipulations that consist of changing the content of the received data, changing the image, changing e.g. the address or sender, addressee or sender - here the number of these various manipulations can be very large.

And now it must be said right away that all these tools that are used in a democratic country require certification and accreditation by specific authorities. In Poland, such accreditation is issued by the Internal Security Agency or the Military Counterintelligence Service.

[64] Own translation.

As for Pegasus, Pegasus is not secured against data leakage, there is no way to secure it, e.g. because the information collected by Polish offices - well, it is especially about the Central Anticorruption Bureau ... They are not the only recipient of the information. Before this information reaches the Central Anticorruption Bureau, it passes through other servers, including servers outside Poland. Therefore, these data, due to the very nature, the very structure of the Pegasus system, are not secured against access to third parties who do not have the competence to access these data under Polish law. And also here it can be said at once that such a leak is not only a violation of the functioning of the entire operational control system itself, the procedure that is applied here, but it is a matter of State security, because if this information reaches some foreign institutions - e.g. to the manufacturer, which is certain, the manufacturer of the Pegasus system - they certainly also reach the secret services. In connection with this, it may involve informing, providing data to special services, intelligence services of a foreign country. Well, this means that this leakage of the Pegasus used in Poland may also lead to the implementation of the offense specified in Art. 130 § 2 of the Criminal Code, i.e. espionage.

The second problem with security is that Pegasus allows for possibility, it accepts the ability to manipulate this collected data. On this device which has been infected, you can change the content that is e.g. created by the user - most often it will be - that is, by the user of a given device. You can make such manipulations that you enter ... the operator of the surveillance device may introduce completely different content, not created by the user of the surveillance device. This is extremely dangerous. In addition, when it comes to procedural issues, what is the purpose of using Pegasus? The data we obtain with this system can in no way be evidence in criminal proceedings, because there is no guarantee that this is content that has not been changed in some way, or whether such content was not present at all in the surveillance device prior to the inspection that led to the obtaining of this data. This makes the use of Pegasus in the Polish system unacceptable.

The second issue is, in my opinion, some experience with electoral law. Here, I must say that it is so often believed that elections are the very act of voting. Elections, the election process begins with the announcement of the date of elections by the Marshal of the Sejm - and from the time it begins ... then the election campaign will be launched. All regulations concerning the rights of people participating in the campaign and candidates - it is also about election offices, including those who run an election campaign ... The whole election campaign is an element of the election. Therefore, the principles must be observed here, and above all the principle of equality of all candidates, equal rights of all candidates taking part in it. The possibility of using such an operational control device, and above all just such a leaky device, capable of manipulating the obtained data, as is the case with Pegasus, well, introduces an absolute inequality of candidates running in the elections, because those candidates who have political support or political service of the office which has Pegasus at its disposal ... Well, it gives a much better chance to the candidate who can use such a service.

The chairman asked if we can discuss the validity here. It is today, from our perspective, when it comes to the 2019 elections, you can also say here presidential - it is not known whether there was also such a procedure, operational control by ... from the Pegasus user ... If we were at the time when the process of affirmation, validation or invalidity would take place in the Supreme Court, the establishment of such a practice would obviously lead to the annulment of the election. Today we do not have such a possibility. There is a ruling of the Supreme Court chamber and this ruling is not subject to review, there is no way to challenge such a ruling. Therefore, we can only strive to make the use of such unfair methods impossible in future election campaigns.

And here I want to conclude right away that the purchase of the Pegasus system, the use of the system, is a violation of the Polish order, it is a violation of the Constitution, it is absolutely unacceptable, regardless of whether the use of this measure - apart from these two elements, that is, leakage or

tampering, apart from these elements - could be useful in the fight against crime. This condition for the accreditation of such a system must be met. Also, all systems that are used in the election campaign must also be recognized by the National Electoral Commission as meeting the requirements of equality in running in elections and the requirements of electoral rights or the principles of conducting the electoral law in general."

[...]

I am sorry to say that the rule of law in Poland is at a very low level. After all, on the example of Pegasus, we are actually dealing with a process that goes towards a police state, which goes towards a state that properly uses measures that do not protect the interest of the State, but only serve to secure the political position of a given formation that exercises power and wants keep this power."[65]

Finally, Polish Ombudsman expressed fundamental reservations as to the compliance of Art. 168a of the Act of June 6, 1997 - Procedural Penal Code with the provisions of the Constitution. By the Act of March 11, 2016 amending Procedural Penal Code and some other acts (Journal of Laws, item 437) the wording of art. 168a was changed and now indicates that "The evidence cannot be considered inadmissible solely on the basis that it was obtained in breach of the provisions of the procedure or by means of a prohibited act referred to in art. 1 § 1 of the Penal Code, unless the evidence was obtained in connection with the performance by a public official's official duties as a result of: murder, willful damage of health or imprisonment". Serious objections of the Ombudsman, expressed in an application to the Constitutional Tribunal of May 6th, 2016, have not been settled in connection with the situation in the Constitutional Tribunal, and the need to withdraw the application from the Constitutional Tribunal for reasons referred to in the Ombudsman's letter of April 9th, 2018. However, this does not mean that the matter is settled, and that the provisions are in line with the Constitution. On the contrary, the Ombudsman maintains his reservations, and their the importance and essence is even more pronounced in a situation where State authorities use systems that allow to obtain information that may constitute evidence in proceedings in violation of applicable regulations.

[65] Own translation.

4. THE U.S. CONTEXT:

4.1. The U.S. position on Pegasus software and other existing spywares

After revelations published in New York Times in 2022, the **FBI** has confirmed that it obtained NSO Group's powerful Pegasus spyware in 2019, during Trump administration, suggesting that it bought access to the Israeli surveillance tool to "stay abreast of emerging technologies and tradecraft". It claimed it had never used Pegasus in support of any FBI investigation. However, FBI admitted it was testing the spyware for its possible use in domestic criminal investigations.

Guardian indicated that according to its source the Pegasus licence was acquired by the FBI using a financial "vehicle" that was not easily identified as being linked to the bureau.

In 2019, **WhatsApp** brought a lawsuit under the Computer Fraud and Abuse Act and California state law, alleging that NSO, the privately owned and operated Israeli corporation producing the Pegasus spyware, sent malware through WhatsApp's server system to approximately 1,400 mobile devices. The company has said about 100 of the individuals who were targeted were members of civil society, including journalists and activists. WhatsApp has also alleged in court filings that a U.S. phone number was targeted by Pegasus on 9 May 2019. Without providing evidence or sourcing, the New York Times reported that the alleged intrusion on a U.S. number, as described in WhatsApp's legal case, was in fact a demonstration of NSO's technology to the FBI.

Similarly, on November 23rd 2021, **Apple** filed a lawsuit against NSO Group and its parent company to hold it accountable for the surveillance and targeting of Apple users. The complaint provides new information on how NSO Group infected victims' devices with its Pegasus spyware. To prevent further abuse and harm to its users, Apple is also seeking a permanent injunction to ban NSO Group from using any Apple software, services, or devices.[66]

On November 4th, 2021, the Commerce Department's Bureau of Industry and Security (BIS) has released a final rule adding NSO Group and Candiru (Israel) to the **Entity List for engaging in activities that are contrary to the national security or foreign policy interests of the United States**. These were added to the Entity List based on evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. These tools have also enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such

[66] According to Apple, by utilizing an exploit in iOS software called "FORCEDENTRY," NSO Group created fake Apple IDs to target individual phones, then used those accounts to send spyware through the iMessage service, disabling logging on a user's phone and used this opening to deliver the larger Pegasus file to the target phones. Meanwhile, this large file was also stored in an encrypted and unreadable format on Apple servers in the United States and abroad. This activity was first detected by Apple in September 2021. The company engaged its Security Engineering and Architecture (SEAR) team to identify and patch the vulnerability. This resulted in the release of iOS 14.8. Subsequently, Apple released iOS 15 which also contains a security feature called BlastDoor. Apple does not believe NSO Group has found a way to circumvent BlastDoor on iOS 15, however, they acknowledge that the company has found ways around earlier versions of this feature.

practices threaten the rules-based international order. Furthermore, it appeared that at least 9 U.S. State Department employees in Uganda had been targeted with Pegasus.[67]

U.S. Secretary of Commerce Gina M. Raimondo released the following statement: "The United States is committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organizations here and abroad."

A study prepared for LIBE Committee, in 2013, directly after the global surveillance estate has been unveiled by Edward Snowden, concluded that the analysis of various surveillance programmes (Echelon, PRISM) and US national security legislation (FISA, PATRIOT and FAA) clearly indicated that surveillance activities by the US authorities were **conducted without taking into account the rights of non-US citizens and residents**. In particular, the scope of FAA created a power of mass-surveillance specifically targeted at the data of non-US persons located outside the US, including data processed by 'Cloud computing', which eluded EU Data Protection regulation.

Strikingly, conclusions of this publically available study prepared for the European Parliament, have only been fully taken into account after they were repeated by the CJEU in its Schrems II judgment.

While spyware - defined by NIST as a software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code - evolved since nineties into a booming multimillion industry, big jurisdictions, such as the U.S., do not need to depend on commercially developed spyware since they have sufficient resources to develop spyware internally.

For example, the U.S. National Security Agency had developed an advanced cyber-espionage weapon called Eternal Blue, which was subsequently leaked by the hacker collective Shadow Brokers and later used in 2017 Wannacry ransomware attack, which targeted the NHS and hundreds of other organisations, as well as in the 2017 NotPetya cyberattack.

4.2. Watergate - a problem and solution.

The U.S. has a longstanding concern with using surveillance technologies against opposition and journalists in internal context. **Watergate scandal**, which led to resignation of President Nixon in 1974, came to encompass an array of clandestine and illegal activities undertaken by members of the Nixon administration, including bugging the offices of political opponents and people of whom Nixon or his officials were suspicious; ordering investigations of activist groups and political figures; and using the Federal Bureau of Investigation, the Central Intelligence Agency, and the Internal Revenue Service as political weapons.

There are important parallels between Watergate and Pegasus scandal concerning how government administration felt exonerated from law when using surveillance against political opponents and rivals, journalist and activists.

67 https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/

There are also important lessons to be drawn from Watergate scandal for any parliamentary, investigatory committee that would like to understand how U.S. Congress managed to resolve the issue:

- neither President Nixon nor his administration didn't think that discovering their illegal surveillance activities was a serious problem; on numerous occasions they refused access to documents and recordings invoking privileges;
- the Congress consequently pushed its investigation establishing an investigatory committee and pursuing its work;
- the right of subpoena (mandatory and sanctioned obligation on witnesses to stand before Congressional committee and provide evidence) was granted by U.S. courts for the first time to Congress during this investigation.

We present, for Members convenience, a description of the Watergate hearings as provided on the website of Levin Center for Oversight and Democracy:

"On May 28 and June 17, 1972, seven operatives from President Richard Nixon's campaign, the Committee to Re-elect the President (CREEP) – E. Howard Hunt, G. Gordon Liddy, James McCord, Jr., Bernard Barker, Virgilio Gonzalez, Eugenio Martinez, and Frank Sturgis – broke into the headquarters of the Democratic National Committee, located in the Watergate complex in Washington, D.C. During the second of the two visits, five of the burglars were arrested while attempting to wiretap telephones and steal sensitive documents. The police had been alerted by security guard Frank Wills.

Over the next year, Carl Bernstein and Bob Woodward of the *Washington Post*, working with a secret source called "Deep Throat" (identified years later as former FBI official Mark Felt), discovered and disclosed financial connections between the burglars, CREEP, and the White House. Though all seven initially pleaded not guilty, Mr. Hunt, Mr. Barker, Mr. Gonzalez, Mr. Martinez, and Mr. Sturgis changed their pleas at a January 7, 1973, appearance before federal D.C. District Court Judge John Sirica. Mr. Liddy and Mr. McCord were later found guilty at trial.

On February 7, 1973, the Senate responded to growing concerns about the break-in by voting 77 to 0 to establish the Senate Select Committee on Presidential Campaign Activities, known as the Watergate Committee. Members were selected with extreme care by both parties to avoid partisanship, choosing liberal and conservative members of both parties and taking presidential ambitions into account. Democratic Senator Sam Ervin of North Carolina was named chair of the committee and was joined by Democrats Herman Talmadge of Georgia, Joseph Montoya of New Mexico, and Daniel Inouye of Hawaii. Republican Senator Howard Baker of Tennessee was the vice chair, serving alongside Republicans Edward Gurney of Florida and Lowell Weicker of Connecticut. The committee was charged with investigating "illegal, improper or unethical activities" occurring in connection with the 1972 presidential campaign and determining the need for new legislation to safeguard U.S. elections.

Samuel Dash was hired as chief counsel and Fred Thompson as minority counsel. The committee eventually employed over 120 staffers, including 22 who electronically organized a massive collection of records.

As the committee commenced its investigation, revelations about the break-in and subsequent cover-up continued to emerge. Mr. McCord alleged that during the burglary trial, people had committed perjury at the behest of the White House, and it was uncovered that Mr. Hunt and Mr. Liddy had also broken into the psychiatrist's office of Daniel Ellsberg, the man responsible for leaking the Pentagon Papers. In addition, evidence emerged that CREEP had engaged in activities focused on undermining

the presidential campaign of Democratic frontrunner Edmund Muskie, using "dirty tricks" to prevent him from winning his party's nomination to run against President Nixon in the 1972 election. Tactics included advertising fake campaign events, sending offensive mailers on doctored stationery, and paying Mr. Muskie's driver to gain access to Muskie files being delivered to a new location. CREEP was successful in sinking his campaign, and Senator George McGovern, who ultimately secured the Democratic nomination, lost the election in a landslide to President Nixon.

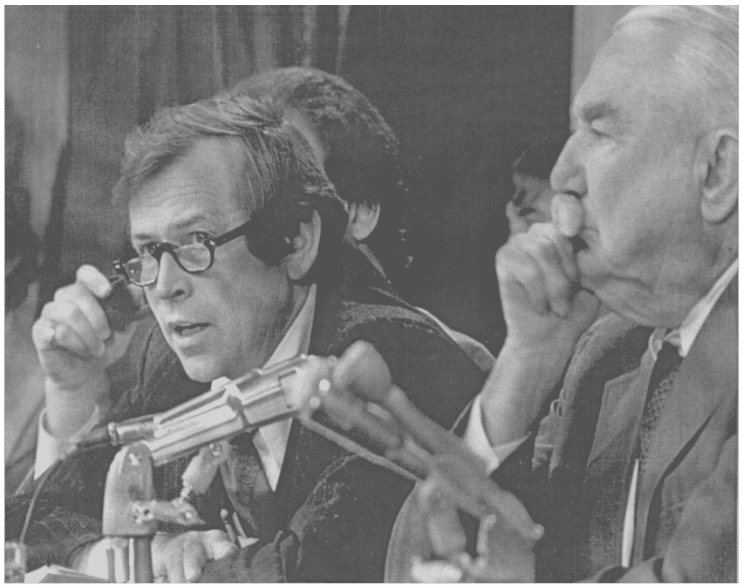
On April 30, 1973, President Nixon announced the resignations of Chief of Staff H.R. Haldeman, Domestic Affairs Advisor John Ehrlichman, and Attorney General Richard Kleindienst from his administration and the firing of John Dean, White House legal counsel. On May 1, Republican Senator Charles Percy of Illinois introduced a resolution that requested appointment of a special prosecutor to investigate the Watergate break-in. Cosponsored by ten Republicans and seven Democrats, the resolution was adopted the same day.

Congressional hearings began on May 17, 1973, and were organized into three phases: "Watergate Investigations," "Campaign Practices," and "Campaign Financing." In his opening statement, Senator Baker stated, "[V]irtually every action taken by this committee since its inception has been taken with complete unanimity of purpose and procedure …. This is not in any way a partisan undertaking, but rather it is a bipartisan search for the unvarnished truth."

Although **President Nixon had initially said that White House aides would not be permitted to testify due to executive privilege**, the committee pushed back. Senator Ervin responded, "That is not executive privilege, it's executive poppycock." The ensuing hearings lasted 51 days and were televised across the country, capturing 237 hours of witness testimony including by President Nixon's top aides, directors at CREEP, and the Watergate burglars. Many testified to destroying sensitive or stolen documents, sabotaging Mr. Muskie's campaign, paying bribes, and feeling pressured by the White House to commit perjury.

John Dean began his week-long testimony on June 24, 1973, with a 245-page statement that took him six hours to read. He admitted to obstructing justice while serving as White House counsel, encouraging perjured testimony, laundering money, and committing other misconduct. He famously reported that he had told President Nixon "there was a cancer growing on the presidency" that needed to be removed. He outlined six conversations with President Nixon indicating that the president was aware of, or even involved in, the Watergate cover-up; he was the first witness to make that allegation. He also submitted about 50 documents as supporting evidence.

Figure 3: Senators Howard Baker and Sam Ervin at the Watergate hearings



Source: Senate Historical Office

The Watergate Committee had granted Mr. Dean limited immunity in exchange for his cooperation and testimony. Special Prosecutor Archibald Cox refused his request for immunity, so Mr. Dean had not spoken to Mr. Cox or his team. They learned what he knew of the Watergate scandal on television at the same time as the 80 million Americans watching his testimony.

At several points during the Watergate hearings, Senator Baker asked Mr. Dean what has since become a famous question in the annals of congressional oversight: **"What did the president know and when did he know it?"** While his question was perceived at the time to be a factual inquiry, later disclosures revealed that it was not as simple as it sounded. Senator Baker had been an ardent supporter of President Richard Nixon and had met frequently with White House staff during the early stages of the Watergate investigation. His question, rather than an attempt to establish President Nixon's role in the scandal, was later described as part of a strategy concocted with White House aides "Bob" Haldeman and John Ehrlichman to try to get Mr. Dean to confuse dates, names, and times, possibly perjuring himself and discrediting his testimony.

When Mr. Dean instead provided coherent testimony backed up by documents and other witnesses corroborated some of the facts, Senator Baker apparently began to reconsider President Nixon's innocence. Republican Senator Weicker, who served with him on the Watergate Committee, reflected in a 1994 interview, "As soon as Howard Baker realized that much of what was being said about Nixon was true and based in fact, he immediately backed off and became probably the most prominent questioner of witnesses."

At the conclusion of Mr. Dean's testimony, the committee decided to request copies of certain documents he'd identified. **President Nixon claimed, however, that constitutional separation of powers prevented him from releasing those documents**. In response, the committee sent him a letter on July 12, 1973, that stated in part:

"The Committee feels that your position as stated in the [July 6] letter, measured against the Committee's responsibility to ascertain the facts related to the matters set out in Senate Resolution 60, present the very grave possibility of a fundamental constitutional confrontation between the Congress and the Presidency. We wish to avoid that, if possible."

Four days later, on July 16, Alexander Butterfield, former presidential appointments secretary and aide to Mr. Haldeman, told the committee in testimony that shocked both Congress and the public that President Nixon had recording devices installed in the Oval Office and his office in the Executive Office Building in the spring of 1971. The newly revealed tape recordings offered an unexpected, contemporaneous, and potent source of information about what the president knew and said about the Watergate burglary and other activities pertaining to his reelection campaign.

The White House eventually admitted the tapes existed, but **President Nixon claimed they were protected by executive privilege and refused to provide copies**. After Senators Ervin and Baker publicly called upon the president to release the tapes to the committee, President Nixon sent a July 23, 1973, letter explaining that, although he had listened to the tapes and they confirmed what he had told them, he would not release them to the committee for fear that "they contain comments that persons with different perspectives and motivations would inevitably interpret in different ways." In response, the committee voted unanimously to issue one subpoena for the tapes and another for related presidential records. On July 26, Special Prosecutor Cox also subpoenaed the tapes, asserting that executive privilege could not override a criminal investigation.

President Nixon continued to defy the subpoenas throughout the summer and fall, despite widespread public opinion in favor of their release. On August 29, 1973, in a case brought by the special prosecutor, **Judge John Sirica ruled that the White House must surrender relevant tapes to the court for a private review to determine whether they should be given to the grand jury**. On October 12, the **D.C. Circuit Court of Appeals upheld his ruling, finding that the federal court had jurisdiction to resolve the dispute, that presidents are not absolutely immune to grand jury subpoenas**, and that courts may rule on matters related to executive privilege.

In the meantime, Mr. Ehrlichman and Mr. Haldeman had testified before the committee, defending themselves and President Nixon while attempting to paint Mr. Dean as the mastermind of the cover-up. In September 1973, Mr. Ehrlichman and Mr. Liddy, along with two accomplices, were indicted for the separate break-in at the office of Mr. Ellsberg's psychiatrist. On October 10, 1973, bribery allegations unrelated to Watergate against Vice President Spiro Agnew led to his resignation.

A few days later, in light of the court order to produce the tapes, President Nixon offered to transcribe them and allow Senator John Stennis of Mississippi, Senate Armed Service Committee chair and Nixon loyalist, to listen to the tapes to verify the transcripts' accuracy. Special Prosecutor Cox held a press conference explaining why he could not accept the "Stennis Compromise," noting in part that the transcripts would not be admissible at trial under federal rules of evidence.

In response, President Nixon ordered Attorney General Elliot Richardson to fire Mr. Cox. The Attorney General refused and resigned immediately. When President Nixon gave the same order to Deputy Attorney General William Ruckelshaus, he also refused and resigned. President Nixon issued the order a third time to Solicitor General Robert Bork who complied by firing Mr. Cox and abolishing the office of the special prosecutor. The press dubbed the events, which took place on Saturday, October 20, 1973, the "Saturday Night Massacre." The impropriety of a president firing a sitting federal prosecutor conducting a criminal investigation still resonates to this day.

President Nixon greatly underestimated the repercussions of his actions. An NBC News poll showed that 75% of the public disapproved of his actions. The House began receiving 30,000 telegrams per day[1] supporting impeachment, and Western Union and the Capital switchboard had to hire more staff to handle all the calls and telegrams flooding Congress.

Representatives responded to the public outcry. Democrat Jerome Waldie of California, a member of the House Judiciary Committee, stated, "The President is gambling. Gambling that the Congress

doesn't have the courage to impeach. I think the President will lose that gamble, because I think the people, in their anger and outrage, will insist upon impeachment." Another committee member, Representative Pete McCloskey of California, who was the first Republican to call for impeachment, declared, "The public is going to demand that we impeach. Congress, in this kind of a case, is representative of the American people. We will react to the American people's demands." Majority Leader Thomas "Tip" O'Neill of Massachusetts announced on October 23, "In their anger and exasperation, the people have turned to the House of Representatives. The case must be referred to the Judiciary Committee for speedy and expeditious consideration." House members overwhelmingly agreed, voting 410 to 4 to authorize the Judiciary Committee to open an impeachment inquiry.

The House Judiciary Committee was chaired by Democrat Peter Rodino of New Jersey and was composed of 21 Democrats and 17 Republicans. The gravity of the task before the committee led members to proceed in a bipartisan way. Democratic Representative Elizabeth Holtzman of New York, the newest and youngest member of the committee, recounted in a 1994 interview:

"Peter Rodino was brilliant and wise. I think he understood the stakes. Peter Rodino knew that impeachment would never work if it was seen to be partisan. So, Rodino looked very hard and far and wide to find a Republican to be Chief of Staff of the House Judiciary Committee's impeachment inquiry. And he found a Republican, John Doar. That was the first signal of how serious this was."

The Judiciary committee members each received a black book with statements of fact and supporting evidence, including information supplied by the Senate Watergate Committee, and attended closed sessions to review the materials. The statements of fact were read aloud by committee lawyers, who were specifically told by Representative Rodino to read in a flat, monotone voice so that members would not be influenced by any emotions in the reading of the texts.

The White House continued to maintain that it was not required to turn over any evidence to Congress, but the new Special Prosecutor Leon Jaworski, appointed on November 1, 1973, after Mr. Cox's dismissal, took the stance that, because impeachment was the sole responsibility of the House, the Judiciary Committee should have access to the few tapes they had been able to obtain. **Judge Sirica granted him permission to turn over the tapes as well as grand jury reports showing evidence of criminal acts**. The most important tape recording concerned a conversation on March 21, 1973, between President Nixon and John Dean, in which they discussed paying off the Watergate burglars, and Mr. Dean told the president that some of his aides, himself included, could go to jail for obstruction of justice.

In February 1974, in an opinion later affirmed by the D.C. Circuit, Judge Sirica finally ruled on the Watergate Committee's request for copies of the tapes. The court determined that the committee had not made a sufficient showing of need for the tapes, since tape transcripts had already been produced, the House Judiciary Committee already had copies of some tapes, and the committee did not show how the tapes were essential to drafting legislation related to presidential elections.

On March 1, 1974, Special Prosecutor Jaworski indicted seven Nixon aides, including Messrs. Haldeman, Ehrlichman and Mitchell, for obstruction of justice, conspiracy, and other crimes. President Nixon was named as an unindicted coconspirator. To conduct the upcoming trial, **the special prosecutor subpoenaed additional tapes and materials from the president who, again, refused to provide them**. **The special prosecutor sued, and on July 23, 1974, the Supreme Court ruled 8 to 0 that President Nixon must turn over 64 tapes, rejecting his claim of executive privilege**. Archibald Cox, when asked about the ruling, tied it to the still unfulfilled subpoena issued by the Judiciary Committee, "I think the decision goes a long way to vindicate the subpoena issued by the

House Judiciary Committee and to establish the proposition that non-compliance with the House subpoena was itself a cause for impeachment."

In a press conference on the day of the Supreme Court decision, House Judiciary Committee member Republican Lawrence Hogan of Maryland offered this analysis:

"After having read and reread and sifted and tested this mass of information which came before us, I've come to the conclusion that ***Richard M. Nixon has, beyond a reasonable doubt, committed impeachable offenses, which in my judgment, are of such sufficient magnitude that he should be removed from office****. The evidence convinces me that my president has lied repeatedly, deceiving public officials and the American People.* ***He has withheld information necessary for our system of justice to work*** *…* ***he concealed and covered up evidence and coached witnesses*** *…. He tried to use the CIA to impede the investigation of Watergate by the FBI. He approved the payment of what he knew to be blackmail to buy the silence of an important Watergate witness. He praised and rewarded those whom he knew had committed perjury. He personally helped to orchestrate a scenario of events, facts, and testimony to coverup wrongdoing in the Watergate scandal and to throw investigators and prosecutors off the track.* ***He actively participated in an extended and extensive conspiracy to obstruct justice****."*

The next day, debate on impeachment began in the House committee. It was the first congressional impeachment debate to be televised live. Judiciary Chair Rodino stressed the following in his opening remarks:

"Make no mistake about it: This is a turning point, whatever we decide. Our judgment is not concerned with an individual, but with a system of constitutional government …. This committee must now decide a question of the highest constitutional importance. For more than two years, there have been serious allegations by people of good faith and sound intelligence that the president, Richard M. Nixon, has committed grave and systematic violations of the Constitution …. We have taken care to preserve the integrity of the process in which we are now engaged. We have deliberated, we have been patient, we have been fair. Now, the American people, the House of Representatives, the Constitution, and the whole history of our republic demand that we make up our minds."

Democrat Barbara Jordan of Texas gained national attention for her passionate opening remarks:

"I am not going to sit here and be an idle spectator to the diminution, the subversion, the destruction of the Constitution …. The Constitution charges the president with the task of taking care that the laws be faithfully executed, and yet the president has counseled his aides to commit perjury, willfully disregard the secrecy of grand jury proceedings, conceal surreptitious entry, attempt to compromise a federal judge, all while publicly displaying his cooperation with the processes of criminal justice. A president is impeachable if he attempts to subvert the Constitution."

[...]

While some Republican members of the committee defended President Nixon, others spoke out against his actions. Republican Representative Robert McClory of Illinois noted, "The only materials which we have received have come from the grand jury and from the special prosecutor. It seems to me the President's failure to comply threatens the integrity of our impeachment process itself. His action is a direct challenge to the Congress, and the exercise of its solemn constitutional duty." Republican Representative Caldwell Butler of Virginia said, "A power appears to have corrupted. It is a sad chapter in American history, but I cannot condone what I have heard. I cannot excuse it, and I cannot, and will not, stand still for it."

Following debate, the committee voted on five articles of impeachment:

- Article I, relating to obstruction of justice, was adopted by a vote of 27 to 11;
- Article II, relating to abuse of presidential power, was adopted by a vote of 28 to 10;
- Article III, relating to contempt of Congress, was adopted by a vote of 21 to 17;
- Article IV, relating to concealing facts from Congress about bombing operations in Cambodia, was rejected by a vote of 12 to 26; and
- Article V, relating to emoluments and tax fraud, was rejected by a vote of 12 to 26.

Despite the committee votes in July 1974, the Articles of Impeachment never received a vote by the full House membership. On Thursday, August 7, Senate Minority Leader Hugh Scott of Pennsylvania, Senator Barry Goldwater of Arizona, and House Minority Leader John Rhodes of Arizona visited President Nixon at the White House to inform him that, were he to stand before the Senate for an impeachment trial, he would be convicted and removed from office. At 9:01 pm on August 8, 1974, President Nixon addressed the nation live on television from the Oval Office and announced his resignation, effective at noon the next day. Representative Gerald Ford, who had been sworn in as Vice President on December 6, 1973, following the resignation of Spiro Agnew, took the Presidential Oath of Office and became the 38th President of the United States.

One month later, on September 8, 1974, President Ford issued Richard Nixon a pardon and gave the former president control of the White House tapes recorded during his tenure. The decision was unpopular with the public and outraged many in Congress after their long battle to obtain access to the tapes. President Ford was called before the House Judiciary Committee, and asked by Representative Holtzman:

"I know that the people want to understand how you can explain having pardoned Richard Nixon without specifying any of the crimes for which he was pardoned. And how can you explain having pardoned Richard Nixon without obtaining any acknowledgement of guilt from him? How can this extraordinary haste in which the pardon was decided on, and the secrecy with which it was carried out, be explained? And how can you explain the fact that the pardon of Richard Nixon was accompanied by an agreement with respect to the tapes, which in essence, in the public mind, hampered the special prosecutor's access to these materials?"

To stop the turnover of the tapes to former President Nixon, Congress overwhelmingly passed the Presidential Recordings and Materials Preservation Act of 1974, giving control of the tapes and other materials relating to Watergate and abuse of power to the National Archives. Although that law pertained only to Nixon-era materials, Congress subsequently passed the Presidential Records Act of 1978, to preserve all presidential, vice presidential, and White House records from successive administrations.

The Watergate investigation led Congress to take other steps as well to prevent presidential and government abuses. Key legislation included the following.

- Federal Election Campaign Act (FECA) amendments: FECA was amended in 1974, to create the Federal Elections Commission, as recommended by the Watergate Committee in its final report. FECA also set contribution limits to political campaigns and required candidates to disclose all funds raised and spent.
- Freedom of Information Act amendments: In 1974, Supreme Court Justice Earl Warren wrote: "If anything is to be learned from our present difficulties, compendiously known as Watergate, it is that we must open our public affairs to public scrutiny on every level of government." As part of the Watergate reforms, Congress enacted several laws to increase government transparency, including a bill strengthening the Freedom of Information Act (FOIA). The Nixon administration had often failed to grant FOIA requests, claiming that documents were "classified" by the executive branch, although they were not actually deemed "classified" materials. Congress amended the 1967 law in 1974, so that only officially "classified"

documents addressing national security concerns could be withheld and gave judges the authority to evaluate specific documents. The law also imposed time limits on agency responses to FOIA requests and required an annual report on overall FOIA requests and denials.

- Privacy Act of 1974: In response to President Nixon's abuses of tax information held by the IRS and illegal surveillance of Americans by the FBI, Congress enacted legislation establishing a Code of Fair Information Practice that federal agencies must follow when collecting and using certain personally identifiable information. It requires the public to be notified of systems containing these records, and forbids agencies from disclosing certain types of personal information without written consent from the individual.
- Tax Reform Act of 1976: Responding to actions taken by President Nixon to obtain copies from the IRS of tax returns filed by certain individuals, request IRS audits of persons on an "enemies" list, and enable multiple agencies to request tax returns from the IRS, Congress enacted Section 1202 of the Tax Reform Act of 1976, imposing strict limits on the IRS' ability to disclose tax information to the President, government agencies, and Congress itself. For the first time, the law required federal tax returns to be treated as "confidential" rather than "public" documents.
- Ethics in Government Act of 1978: This law created the federal Office of Government Ethics and required certain government officials to submit financial disclosure forms, including the president, vice president, members of Congress, officers of the executive branch, and others. It also restricted lobbying by former members of Congress and set limits on outside earned income and employment by individuals working for the government. In addition, it established a process for appointing "independent counsel" to investigate government misconduct, a provision later allowed to lapse. An early version of this bill was named the "Watergate Reorganization and Reform Act."

In addition to legislative reforms, information uncovered about President Nixon's use of the intelligence community for unlawful purposes helped spur creation of the Church Committee, which led to the Foreign Intelligence Surveillance Act and other important changes.

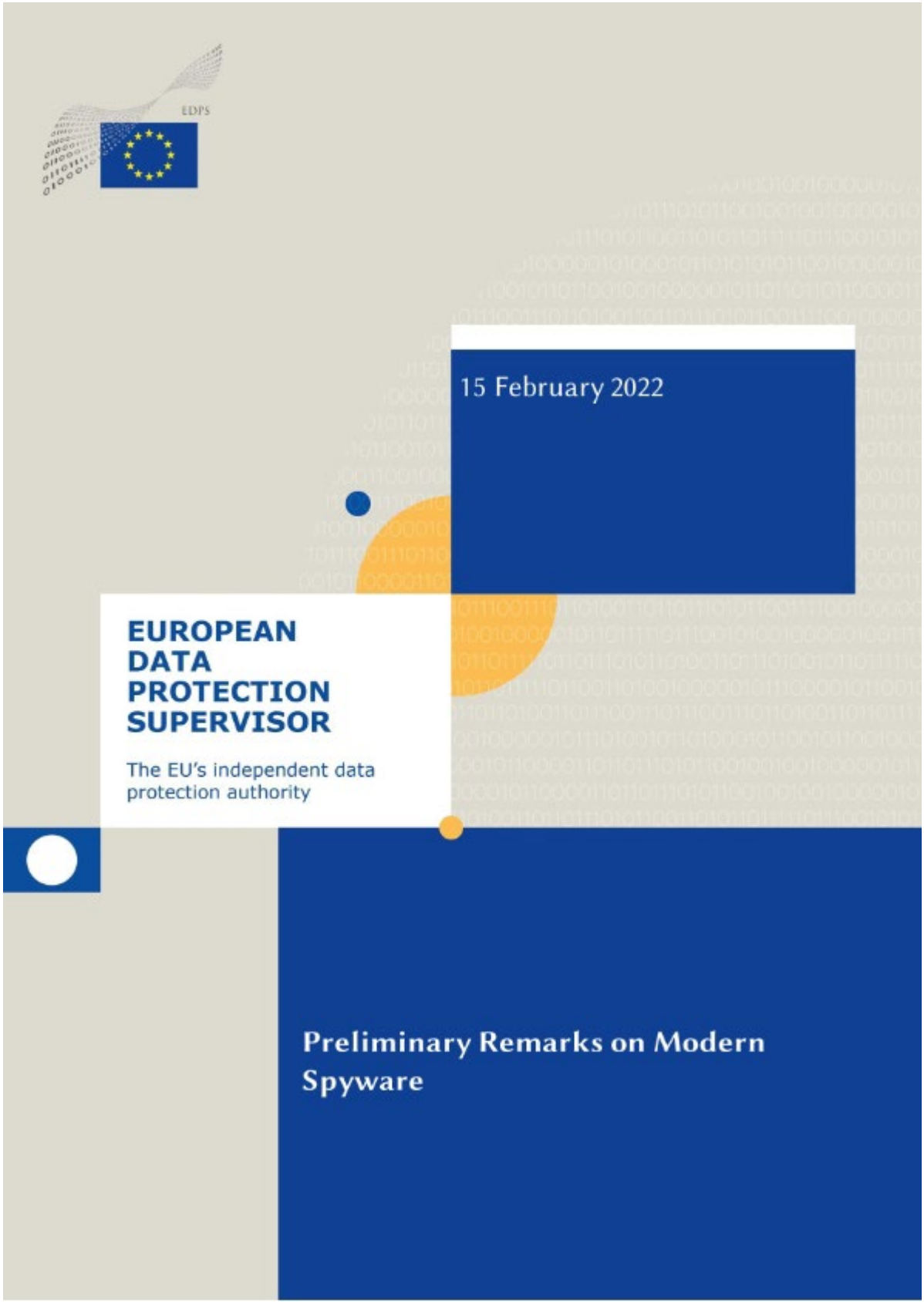
The Senate Select Committee on Presidential Campaign Activities issued its final report on June 27, 1974. It ran 1,250 pages, with an additional 907-page volume of supporting exhibits.

Ultimately, 48 people were convicted of crimes related to the Watergate scandal including for **conspiracy, obstruction of justice, perjury, burglary, wiretapping, and distributing illegal campaign literature**. Twenty corporations pled guilty to making illegal campaign contributions. Federal courts issued key precedents establishing that presidents are subject to grand jury subpoenas and limiting the scope of executive privilege."[68]

We advise PEGA Committee to request a workshop in order to benefit from experience of experts from **Levin Center for Oversight and Democracy** both regarding extensive experience on investigatory techniques that Congress acquired over extensive period of time and regarding legal and procedural reforms required for the U.S. legislator to become an efficient oversight body.

[68] https://www.levin-center.org/the-watergate-hearings/

ANNEX: EUROPEAN DATA PROTECTION SUPERVISOR: PRELIMINARY REMARKS ON MODERN SPYWARE


EDPS
15 February 2022
EUROPEAN DATA PROTECTION SUPERVISOR
The EU's independent data protection authority
Preliminary Remarks on Modern Spyware

Contents

EDPS Preliminary Remarks on Modern Spyware

1. Introduction

The revelations made about the Pegasus spyware raised very serious questions about the possible impact of modern spyware tools on fundamental rights, and particularly on the rights to privacy and data protection. This paper aims to contribute to the ongoing assessment in the EU and globally of the **unprecedented risks** posed by this type of surveillance technology. It comes from the EDPS' conviction that the use of Pegasus might lead to an **unprecedented level of intrusiveness**, which threatens the **essence of the right to privacy**, as the spyware is able to interfere with the most intimate aspects of our daily lives.

The distribution and use of spyware tools has been a long-standing serious concern for the EDPS, on which he issued Opinion 8/2015 on the dissemination and use of intrusive surveillance technologies. He underlined that "*[t]he use and dissemination (including inside the EU) of surveillance and interception tools, and related services, should be subject to appropriate regulation, taking into account the potential risk for the violation of fundamental rights, in particular the rights of privacy and data protection*".

As the specific technical characteristics of spyware tools like Pegasus make the control over their use very difficult, we have to **rethink the entire existing system of safeguards** established to protect our fundamental rights and freedoms, which are endangered by these tools.

2. What is Pegasus and how does it work?

According to media reports[1], Pegasus is **probably the most powerful hacking tool** – or spyware – to date. It was developed and marketed around the world by the Israeli company NSO Group. Pegasus is designed to successfully attack almost any smartphone running either iOS or Android operating systems, based on specific information of the target such as the mobile phone number. It can secretly turn a mobile phone into a 24-hour surveillance device, as it gains complete access to all sensors and information of the phone. It can read, send or receive messages that are supposed to be end-to-end encrypted, download stored photos, and hear and record voice/video calls. It has full access to the phone's camera, meaning that it might secretly use it to film you or your environment, or activate the microphone to record real world conversations (for instance, those of people next to you). It also has full access to the geolocation module of the phone, which means it knows where a phone is now and it might also record the timeline of its location.

Pegasus belongs to a new category of spyware tools that differ from "traditional" interception tools used by law enforcement authorities, in a number of ways:

First, it grants **complete, unrestricted access** to the targeted device. According to the research conducted by Amnesty International's Security Lab, this spyware allows the attacker to obtain so-called root privileges, or administrative privileges, on the device: "Pegasus can do more than what the owner of the device can do"[2]. In light of these unprecedented capabilities, one cannot exclude the possibility of using Pegasus beyond mere interception of communications. For instance, it might allow the attacker to gain access to digital credentials or digital identity apps[3], which could be used to **impersonate the victim** and gain access to digital and physical assets, or other similar activities[4].

Second, Pegasus is able to carry out a successful **"zero-click" attack**: a hacking attack that does not require any action by the user to be triggered, so that even a cyber-security-savvy user can do nothing in order to prevent it from happening. Moreover, even the biggest device vendors such as

---

[1] D. Pegg & S.Cutler, *What is Pegasus spyware and how does it hack phones*, The Guardian, 2021. Accessed 14 February 2022. https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

[2] Amnesty International, *Forensic Methodology Report: How to catch NSO Group's Pegasus*, 2021. Accessed 14 February 2022. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[3] See e.g. *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity* (SEC(2021) 228 final) - (SWD(2021) 124 final) - (SWD(2021) 125 final).

[4] Although not yet the case, one can even imagine a next generation of spyware, based on the full and unrestricted control over the target's device, where the attacker moves from 'passive' to 'active' attack, e.g. by 'planting' evidence of crime.

Apple and Google might not be able to entirely protect individuals from state-of-the-art malware such as Pegasus, despite their constant efforts to enhance the security of their software. Private hacking companies such as NSO Group may have the financial power to contract highly capable software engineers with the sole task of seeking ever-existing vulnerabilities and developing powerful exploits, on par with nation-state capabilities[5].

In addition, Pegasus software is **very difficult to detect** and the intrusions are very hard to prove unless the operating system is powered by secure system logging mechanisms[6]. Security researchers suspect that recent versions of Pegasus inhabit only the phone's temporary memory, rather than its hard drive, meaning that once the phone is powered down virtually, all trace of the software vanishes[7]. Furthermore, the uptake of cloud computing has enabled private companies selling malware and spyware to install their attack infrastructure in the cloud, using highly sophisticated network architectures and application software. Thus, they can provide a hacking service without the need for the customer to install a specific tool, e.g. through offering access to the victim's device via a website. This means that the actual hacking software is always protected[8] and can be always kept up to date and improved for all users, while offering the provider the opportunity to keep control of the tool and of customers.

Pegasus as a "game changer" for digital surveillance

Pegasus should not be equated to "traditional" law enforcement interception tools; instead, it appears to be more similar to "government Trojan" or "online searches" solutions[9] that had in the past raised serious legal concerns, often at constitutional level[10].

Spyware tools like Pegasus are actually hacking tools, and not just means for (lawful) interception of communication. They are based on breaching security mechanisms and exploiting unpatched

---

[5] *L.H. Newman. Google Warns That NSO Hacking Is On Par With Elite Nation-State Spies. The Wired. 2021. Accessed 14 February 2022.* https://www.wired.com/story/nso-group-forcedentry-pegasus-spyware-analysis/

[6] *This is why the security researchers were able to prove the infection of iPhones, as they had sufficient logging mechanisms, which was not the case for Android phones. However a next version of Pegasus might improve in that regard, taking them 'lessons learnt'.*

[7] *D. Pegg & S.Cutler. What is Pegasus spyware and how does it hack phones. The Guardian. 2021. Accessed 14 February 2022.* https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

[8] *Amnesty International. Forensic Methodology Report. How to catch NSO Group's Pegasus. 2021. Accessed 14 February 2022.* https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[9] *For more information see* https://www.techtarget.com/searchsecurity/definition/government-Trojan

[10] *E.g. CCC Challenge to use of government spyware (Germany). Privacy International. 2021. Accessed 14 February 2022* https://privacyinternational.org/legal-action/ccc-challenge-use-government-spyware-germany

vulnerabilities and, in this sense, allowing their use even under strict conditions would create a permanent and strong risk of massive security breaches for all users, comparable in a way with encryption backdoors[11].

Due to its unique features, the Pegasus spyware constitutes a "game-changer", combining a level of intrusiveness that is incomparable with what we have seen before, with features capable to render many of the existing legal and technical safeguards ineffective and meaningless. At the same time, it should be borne in mind that Pegasus is not the only spyware tool of this type currently available and the digital market offers a plethora of spyware tools that are often promoted as "law enforcement tools"[12].

3. How can spyware like Pegasus be abused?

NSO Group claims that their technologies "have helped prevent terror attacks, gun violence, car explosions and suicide bombings. The technologies are also being used every day to break up paedophilia, sex- and drug-trafficking rings, locate missing and kidnapped children" as part of the company's "life-saving mission"[13].

However, the worldwide media investigations indicate another, much **darker side of the software.** There is a growing body of evidence that some of the "vetted customers" applied Pegasus to hack mobile phones and spy on journalists, lawyers, opposition leaders and human rights activists[14].

It has been reported that the **Pegasus spyware had been used in the EU against EU citizens, including opposition politicians, journalists and lawyers.** Some EU governments admitted to

[11] In this regard, the CJEU ruled in DRI case that the risk of unlawful access to [telecommunications] data was, in the light of Articles 7, 8 and 52(1) of the Charter, one of the grounds for invalidating Directive 2006/24 (Data Retention Directive). Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Others, paragraphs 54 and 55.

[12] See for example: https://www.softwaresuggest.com/ws-pegasus-alternatives .

[13] The Pegasus Project. Response from NSO and governments. The Guardian. 2021. Accessed 14 February 2022. https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments. See also: A. Keshet Tal. Phonespy surveillance software mimics Pegasus and was spotted stealing data from thousands of South Korean Android users. Notebookcheck.net. 2021. https://www.notebookcheck.net/Phonespy-surveillance-software-mimics-Pegasus-and-was-spotted-stealing-data-from-thousands-of-South-Korean-Android-users.578637.0.html.

[14] Examples include: an alleged use of Pegasus to prepare the assassination of the Saudi journalist Jamal Khashoggi by agents of the Saudi state. See: P. Rueckert. Pegasus. The new global weapon for silencing journalists. Forbidden Stories. 2021. Accessed 14 February 2022. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

having bought Pegasus from the NSO Group[15]. The list of potential customers in the EU may prove even bigger, as it appears that a number of other Members States have at least initiated negotiations with NSO Group for the licencing of the product[16].

Applicable legal framework

Targeted surveillance, including intercepting communications, is regulated in the national legislation of virtually all EU Member States[17]. When it is used for law enforcement purposes, targeted surveillance has to comply with applicable Union primary and secondary law, in particular the Charter of Fundamental Rights[18], the ePrivacy Directive[19] and the Law Enforcement Directive[20].

The legal conditions and safeguards for the use digital surveillance and communication interception have been subject to extensive analysis and interpretation by both the **Court of Justice of the European Union**[21] and the European Court on Human Rights[22]. In particular, in the judgment in Joined Cases C-511/18 and C512/18 (La Quadrature du Net and Others) the CJEU clarified the applicability of EU law to certain measures adopted on national security grounds, namely where obligations are imposed on service providers.

It is important to emphasise that the use of digital surveillance tools by EU Member State authorities for national security purposes, even when it falls outside the scope of Union law[23], is nevertheless subject to national constitutional law as well as the **relevant legal framework of the Council of Europe, in particular the European Convention on Human Rights[24].** In addition, the Convention for the Protection of Individuals with regard to Automatic Processing of

---

[15] *Hungary admits to using NSO Group's Pegasus spyware. Deutsche Welle, 2021. Accessed 14 February 2022.* https://www.dw.com/en/hungary-admits-to-using-nso-groups-pegasus-spyware/a-59726217 *and Z. Wiosat. Poland's Watergate: Ruling party leader admits country has Pegasus hacking software. Politico. 2021. Accessed 14 February 2022.* https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/

[16] *D. Leloup & M. Untersinger. Malgré les approches de NSO Group, la France a choisi à la fin de 2020 de ne pas acheter le logiciel espion Pegasus. Le Monde. 2021. Accessed 14 February 2022.* https://www.lemonde.fr/pixels/article/2021/11/26/malgre-les-approches-de-nso-group-la-france-a-choisi-a-la-fin-de-2020-de-ne-pas-acheter-le-logiciel-espion-pegasus_6101783_4408996.html

[17] *See Fundamental Rights Agency (FRA) report "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU", 2017.*

[18] *OJ C 326, 26.10.2012, p. 391–407.*

[19] *OJ L 201, 31.7.2002, p. 37–47.*

[20] *OJ L 119, 4.5.2016, p. 89–131.*

[21] *See for example CJEU judgments in joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, case C-623/17, Privacy International, cit.*

[22] *See e.g. ECtHR judgments in cases Zakharov v. Russia, Big Brother Watch and Others v. the United Kingdom, Ekimdzhiev and Others v. Bulgaria.*

[23] *Pursuant to Article 4(2) TEU "national security remains the sole responsibility of each Member State".*

[24] *See CJEU judgment in Joined Cases C-511/18 and C-512/18, La Quadrature du Net and Others, para. 103.*

Personal Data (**Convention 108**), recently modernised as Convention 108+, applies to processing of personal data for State (national) security purposes, including defence[25].

4. Can Pegasus be used legally within the scope of EU law?

Pegasus and similar technologies are often advertised as "law enforcement tools". In this regard, it is important to analyse whether it is legally possible to use Pegasus or similar tools in the EU to pursue objectives of general interest recognised by the Union, such as combating terrorism and serious crime.

Terrorism and organised crime pose serious threats within the European Union and globally, and their detection, prevention and prosecution represent important objectives of general interest which may justify limitations on the exercise of the fundamental rights and freedoms of the individual, in accordance **with Article 52(1) of the EU Charter of Fundamental Rights**, to the extent that they are proportionate and necessary. Such limitations must in any event be provided for by law and respect the essence of the fundamental rights and freedoms recognised by the Charter.

The CJEU acknowledged in its recent case law[26] that a serious threat to national security that is genuine and present or foreseeable could justify very serious interferences with fundamental rights, subject to strict conditions and safeguards.

Necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal[27]. Given the scarcity of publicly available verifiable information about the functionalities of Pegasus, it is difficult to ascertain to what extent its use could not be replaced by the use of other, more "traditional" and potentially less intrusive means.

---

[25] Article 9 of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) Article 11 of Convention 108+.
[26] E.g. Judgment in Joined Cases C-511/18 and C-512/18, La Quadrature du Net and Others.
[27] See also the EDPS Necessity Toolkit, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf

Furthermore, today we all rely on smartphones to perform most of our activities in the digital world. Our smartphones know everything about us: they know our data, they can hear us, they can see us, and they know where we are and who we talk with. It is therefore highly unlikely that spyware such as Pegasus, which de facto grants full unlimited access to personal data, including sensitive data, **could meet the requirements of proportionality**[28].

The level of **interference with the right to privacy is so severe that the individual is in fact deprived of it**. In other words, the essence of the right is affected. Therefore, its use cannot be considered proportionate – irrespective of whether the measure can be deemed necessary to achieve the legitimate objectives of a democratic state[29]. Moreover, it is not just the target of the surveillance whose right to privacy is manifestly infringed, but also everybody in contact with him or her or even those around them (e.g. people sitting a restaurant close to the target could also be recorded). Furthermore, Pegasus and similar spyware deprive the affected individuals of additional forms of protection, such as **confidentiality of communication** with a lawyer.

At the same time, the EDPS takes note of the media reports alleging that certain features of Pegasus might be switched off, in order to limit the intrusiveness of the tool, which might have an impact on the result of the proportionality and necessity assessment. Therefore, one cannot exclude the possibility that the application of certain features of Pegasus may pass the necessity and proportionality test in specific situations of very serious threat, such as **imminent terrorist attack**.

However, the EDPS considers that such cases would be of exceptional nature and cannot justify a wider or systematic deployment of such highly intrusive technology. Consequently, regular deployment of Pegasus or similar highly intrusive spyware technology would not be compatible **with the EU legal order.**

In addition, the capability of spyware tools such as Pegasus to provide full and unrestricted control by the attacker of the target's phone, coupled with the fact that they leave very little, if any, digital traces, raises the question of to what extent the information gathered with their help could be used as evidence in a criminal procedure – from the point of view of both admissibility and verification.

---

[28] *"For a measure to respect the principle of proportionality, enshrined in Article 52(1) of the Charter, the advantages resulting from the measure should not be outweighed by the disadvantages the measure causes with respect to the exercise of fundamental rights", see EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019, available at https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf*

[29] *See CJEU judgment in case C-362/14 Maximillian Schrems v Data Protection Commissioner, para. 93-94.*

In this regard, many of the forensic experts may not have the necessary knowledge to identify and examine such highly advanced technology, especially when developed by private companies.

Consequently, one may argue that the use of such advanced hacking tools to collect evidence in a criminal investigation could actually **encroach on the right to fair trial**, provided for in Article 47 of the Charter, which is one of the of the cornerstones of European legal systems.

5. What could and should the EU do?

The recast of the **EU Dual Use Regulation**[30] introduced new export controls for "cyber-surveillance items". Still, the overall protection needs to be strengthened in order to guarantee that cyber-surveillance items will never be exported to countries that do not ensure the respect of fundamental rights, including the right to privacy. Moreover, such controls should also cover import of such dual-use technologies, as much as export. In this context, it should borne in mind that blacklisting of spyware vendors alone is not enough for ensuring the effective application of the Regulation.

The mounting evidence shows that highly advanced military-grade spyware like Pegasus has the potential to cause **unprecedented risks and damages** not only to the fundamental rights and freedoms of the individuals but also to **democracy and the rule of law**. Pegasus constitutes a paradigm shift in terms of access to private communications and devices, which is able to affect the **very essence of our fundamental rights, in particular the right to privacy**. This fact makes its use incompatible with our democratic values.

Therefore, the EDPS believes a **ban on the development and the deployment of spyware with the capability of Pegasus** in the EU would be the most effective option to protect our fundamental rights and freedoms. In any event, if such tools are nevertheless applied in exceptional situations, e.g. to prevent a very serious imminent threat, the EDPS proposes the following non-exhaustive list of **steps and measures as a guarantee against unlawful use**:

[30] OJ L 206, 11.6.2021, p. 1–461.

1. **Strengthening of democratic oversight over surveillance measures**. EU Member States should ensure effective oversight over the use of such surveillance measures. The role of data protection authorities, judicial control (ex ante and ex post), and democratic forms of scrutiny are absolutely necessary.[31] Any form of evaluations and monitoring must be meaningful and effective. While there is no 'one-size-fits-all' solution, there is a need for a broad spectrum of actions in a modern checks and balances system. The Commission's annual Rule of Law report should take into account the standards of national legislation in this field.

2. **The strict implementation of the EU legal framework on data protection**, especially the Law Enforcement Directive, is a critical prerequisite. Equally important is the full implementation of the relevant CJEU judgements (e.g. on data retention), which is still lacking in several Member States. In this regard, the Commission as the "guardian of the EU Treaties" pursuant to Article 17 of Treaty on the European Union (TEU)[32], has a central role for enforcing EU law and ensuring its uniform application throughout the Union.

3. **Judicial review, both ex-ante and ex-post, should be real; it cannot be a mere formality.** When reviewing an application for a surveillance order, the judicial authority should always be aware of what kind of surveillance would be carried out (e.g. when highly intrusive monitoring of an individual's activity is foreseen), in order to allow the court to decide whether the surveillance remains within what is strictly necessary.

4. **Strengthening of the protections offered by the criminal procedure.** Criminal procedural laws should outlaw the use of highly intrusive hacking tools like Pegasus. Based on Article 82 of the Treaty on the Functioning of the European Union (TFEU)[33], the EU has the competence to adopt minimal standards on the rights of individuals in criminal procedures. This includes restricting the admissibility of evidence collected with the help of highly intrusive hacking tools like Pegasus or even outlawing it[34]. The EU could also, based on Article 83 TFEU, define criminal offences such us illegal use of spyware technologies.

5. **Reducing the risk that data originating from such undemocratic and abusive surveillance practices reaches the databases of the Union** (e.g. Europol) and Member States law enforcement agencies, e.g. through "import" of criminal intelligence and other data from third countries, circumventing the legal limitations in the Union.

6. **Stop (ab)using national security purposes for legitimising politically motivated surveillance.** "National security" cannot be used as an excuse to an extensive use of such technologies nor as an argument against the involvement of the European Union. Both the jurisprudence of the CJEU and the relevant binding international legal framework, in particular the ECHR and Convention 108 of the Council of Europe, show clear limitations

---

[31] See Fundamental Rights Agency (FRA) report "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU", Volume 3, Chapter 2 "Oversight of intelligence services", 2017.
[32] OJ C 326, 26.10.2012, p. 47–390
[33] OJ C 326, 26.10.2012, p. 47–390
[34] Under the so-called 'fruit of the poisonous tree' doctrine.

that need to be strictly observed by state authorities[35]. The EDPS draws attention to the role the ePrivacy Directive might play in the safeguarding against the level of intrusions which modern spyware creates.

7. **Addressing the rule of law problems**. Deficiencies in the rule of law and democratic backsliding, such as encroaching on judicial independence or media freedom, create fertile ground for abuse of secret surveillance, with tools like Pegasus. Therefore, such issues within the EU should be addressed and enforced as a matter of priority.

8. **Empowering civil society to bring awareness and public debate forward**. Only with strong civil society, can democratic control can be exercised over the use of surveillance measures by the State. Abuse of such tools against politicians, journalists and activists has many times been discovered thanks to civil society. It is our duty to support it.

With this document, the EDPS would like to contribute to the discussion on whether spyware tools like Pegasus should have any place in a democratic society. At the centre of any such discussion, should not only be the use of the technology itself, but the importance we attribute, as a society, to the right to privacy as a core element of human dignity.

[35] See the EDPB response to MEP István Ujhelyi on the alleged use of the Pegasus spyware, available at https://edpb.europa.eu/system/files/2021-12/edpb_letter_out_2021-00160_mep_ujhelyi.pdf, and also https://hungarytoday.hu/pegasus-hungary-spyware-data-authority-naih-peterfalvi/

This briefing contains background materials for PEGA Committee mission to Poland.

Materials collected in the briefing indicate at a large scale legislative overhaul, deep politicisation of executive branch and undermining of judicial independence that led to a paralysis in resolving flagrant violations of law due to illegal acquisition and use of Pegasus spyware in Poland.

The briefing has been prepared by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the PEGA Committee.

PE 752.603

Print ISBN 978-92-848-0938-7 | doi:10.2861/484767 | QA-04-23-767-EN-C
PDF ISBN 978-92-848-0937-0 | doi:10.2861/367 | QA-04-23-767-EN-N