BRIEFING NOTE

Requested by the PEGA Committee

European Parliament

Briefing for the PEGA Committee Mission to Spain

20 - 21 March 2023

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 752.602 - March 2023

EN

Briefing for the PEGA Committee Mission to Spain

20 - 21 March 2023

Abstract

This briefing contains background materials for PEGA Committee's mission to Spain.

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
Mariusz MACIEJEWSKI, Policy Department C
Martina SCHONARD, Policy Department C (Chapter 1)
Quentin LIGER, Asterisk Research and Analysis GmbH, Mirja GUTHEIL, Asterisk Research and Analysis GmbH (Chapter 2 and Annex)

ADMINISTRATOR RESPONSIBLE
Mariusz MACIEJEWSKI

EDITORIAL ASSISTANT
Ivona KLECAN

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 March 2023

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

CONTENTS

LIST OF ABBREVIATIONS

Charter	Charter of Fundamental Rights of the European Union
CIFAS	Centro de Inteligencia de las Fuerzas Armadas
CITCO	Centro de Inteligencia contra el Terrorismo y el Crimen Organizado
CJEU	Court of Justice of the European Union
CNI	Centro Nacional de Inteligencia
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EPD	E-Privacy Directive – Directive 2002/58/EC, as revised
EUR	Euro
GDPR	General Data Protection Regulation
EDPS	European Data Protection Supervisor
LED	Law Enforcement Directive –Directive (EU) 2016/680
NSO	Niv, Shalev and Omri
PEGA	Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware
UN	United Nations

1. INTRODUCTION: SPAIN - ITS LEGISLATIVE AND EXECUTIVE POWERS, JUDICIAL SYSTEM AND THE TERRITORIAL ORGANISATION

The political form of the Spanish State is that of a parliamentary monarchy. It is a decentralised unitary country. The Crown, in his capacity as head of State, symbolises the unity and presence of the State, exerts an arbitration and moderating function of the regular functioning of the institutions, and is the highest representative of Spain in international relations.

Legislative Power

The Cortes Generales

The exercise of the legislative power of the State falls to the Cortes Generales, representing the Spanish people and controlling the actions of the Government. **The Cortes generales comprise of two Houses: the Congress of Deputies and the Senate**. Although they share legislative power, the Congress holds the power to ultimately override any decision of the Senate by a sufficient majority (usually an absolute majority or three-fifths majority). The Cortes Generales are composed of 615 members: 350 Deputies and 265 Senators. Deputies and senators are elected for four years.

The Congress of Deputies

The Congress of Deputies (the lower House of the Cortes Generales) comprises of 350 members. All bills must be examined in the Congress of Deputies. The Senate has the right of veto or amendment of the text produced by the Congress, the latter being entitled to make the final decision after a new examination. The Congress executes the investiture of the President of the Government and, therefore, it is this House which may bring about their resignation, either by approving a motion of censure or refusing to concede the confidence required by the Government. After the 2019 general election in April, the number of female deputies was up to 168 representing 48% of all members, making Spain the European country with the highest percentage of women in parliament; surpassing Sweden and Finland. The XIV legislature of Spain started on 3 December 2019 when the Cortes Generales were constituted, once the 2019 general election was held.

The Senate

The composition of the Senate is established in Part III of the Spanish Constitution. The Senate is composed of senators, each of whom represents a province, an autonomous city or an autonomous community. Each mainland province, regardless of its population size, is equally represented by four senators; in the insular provinces, the big islands are represented by three senators and the minor islands are represented by a single senator. Likewise, the autonomous cities of Ceuta and Melilla elect two senators each. This direct election results in the election of 208 senators by the citizens. In addition, the regional legislatures also designate their own representatives, one senator for each autonomous community and another for every million residents, resulting in a total of 57 additional senators.

Spain is expected to hold parliamentary elections by December 10, 2023[1].

[1] https://www.electionguide.org/elections/id/4071/

Executive Power

The Government

The Government is responsible for the executive function of the legislative initiative, the possibility of governing by way of emergency legislation (the ratification of which is delegated to Congress) and the drawing up of the draft budget. The Government oversees domestic and foreign policy, civil and military administration and the defence of the State. In Spain the Government is formed in two phases. A first phase in which the presidential candidate submits their mandate of Government to the consideration of the Congress, and a second phase in which the president, once the confidence of the House has been conferred and once appointed by the King, proposes the appointment of ministers to the King.

The collegiate body of the executive is the Council of Ministers (*Consejo de Ministros*), formed by the president, the vice-president(s) and the ministers.

The current prime minister is Pedro Sánchez, the leader of the Socialist Workers' Party.

Justice system

The Spanish judicial system is composed of courts of general jurisdiction and specialised courts[2], and is structured in accordance with the territorial organisation of the country. The Supreme Court is the highest judicial body in all areas of law. The General Council for the Judiciary, established by the Spanish Constitution, is the body of judicial self-governance, and ensures the independence of courts and judges. As such, it does not itself form part of the judiciary. It exercises disciplinary action and is competent to appoint, transfer and promote judges, as well as being responsible for the training and recruitment of judges.

The Constitutional Court (Articles 159-165 of the Constitution), is the supreme institution regarding the interpretation of the spanish Constitution with important union and powers such as unconstitutionality and question acts, conflict of powers, the Amparo or Conflicts in defense of local autonomy.

The public prosecution service is integrated in the judiciary with functional autonomy, and pursues the mission of promoting justice in defence of the law, the rights of the citizens and the general interest. The Prosecutor General[3] is appointed by the Head of State, upon proposal of the Government, consultating the General Council for the Judiciary, as stipulated for by the Article 122 of the Constitution.

The Solicitor General of the State is a senior official of the Ministry of Justice in charge of directing the Legal Service of the Government and its relationship with national and foreign organisms, entities and bodies. The Local Bars are public law organisations of professionals, independent from the public administration and do not depend on the budgets of the public authorities, nor are their assets public.

---

[2] Spain is the only EU country, where specialised courts dealing with violence against women, exist.

[3] The Public Prosecutor's Office has issued several instructions for the prosecution of violence against women since 1998. The most important among these are Instruction 7/2005 of the Public Prosecutor against violence against women. Instruction of the Public Prosecutor against violence against women and for the specialised anti-violence units of public prosecution offices (Instrucción 7/2005, sobre el Fiscal contra la Violencia sobre la Mujer y las Secciones contra la violencia de las Fiscalías), 23 June 2005, https://www.boe.es/buscar/doc.php?id=FIS-I-2005-00007.

They have competences for the organisation of the profession and professional deontology, and approve their own code of ethics. Within the so called the " *Indirizzo politico* " powers in Spain there are the Tribunal de Cuentas espanol - **Spanish Court of Auditors,** article 136 of the Constitution and the defendent of public rights -the Ombudsman- article 54 of the Constitution.

The territorial organisation of the State

The Autonomous Communities, towns and cities with a Statute of regional autonomy

The Constitution guarantees the right to autonomy of the nationalities and regions forming part of the Spanish nation and the solidarity between them (Article 2 of the Constitution). This has been brought about through the creation of 17 Autonomous Communities and 2 Autonomous Cities of Ceuta and Melilla, with the consequent redistribution of political and administrative powers according to the Articles 137, 140, 148 and 149 of the Constitution.

Each Autonomous Community has its Statute of Regional and Political Autonomy**.** It is important to mention that the Constitutional Tribunal has stressed since its first resolutions that "autonomy refers to limited power. Autonomy is not sovereignty - and even this power has its limits - and since each territorial organization endowed with autonomy is a part of the whole, in no case can the principle of autonomy be opposed to that of unity, but it is precisely within this that it reaches its true meaning, as expressed in Article 2 of the Constitution. (STC 4/1981). The Constitutional Tribunal has also declared that "the Autonomous Communities enjoy a qualitatively superior autonomy to the administrative one that corresponds to the local entities, since legislative and governmental powers are added that configure it as autonomy of a political nature" (SSTC 4/1981 and 25/1981).

2. THE USE OF PEGASUS AND SIMILAR SPYWARE IN SPAIN

2.1. General developments

In July 2020, a joint investigation by El País and the Guardian revealed that Roger Torrent, the speaker of the Catalan parliament and at least two other pro-independence leaders were targeted by spyware in the 2019.[4]

In April 2022, Citizen Lab broke the story that at least 65 individuals had been targeted or infected by mercenary spyware. While in the majority of cases the spyware used was Pegasus, in some cases Candiru was also used. The victims were mainly individuals active in the pro-independence movement in Catalonia. Victims include Members of the European Parliament, Catalan Presidents, legislators, jurists and members of civil society organisations.[5]

Citizen Lab did not attribute the attacks to a specific entity, but suggested that circumstantial evidence pointed to a "*strong nexus with one or more entities within the Spanish government*". [6] Citizen Lab lists four points in particular: (i) the targets were of obvious interest to the government, (ii) the timing of the targeting matches moments and events of specific interest to the government, (iii) the baits used to target the victims suggests the attackers had access to the victims' personal information (including governmental ID number), and (iv) the National Intelligence Centre (CNI) had reported being a customer of the NSO group and the Ministry of Interior is reported to possess similar capabilities.[7] The CNI has been suspected of having acquired or used spyware in the past, including FinFisher, as well as other types of spyware.

Shortly after, the Spanish government organised a press conference to announce that the phones of the Prime Minister and the Minister of Defence Margarita Robles (heading the two organisations overseeing the CNI) has been targeted by the Pegasus spyware.[8] While no confirmation of the source of these attacks have been given, there are strong suspicions that the Moroccan authorities (which are suspected to have used Pegasus against targets in France and Italy – see the respective sections on these countries) are responsible for such surveillance operations, in relation to the ongoing discussions about the fate of Western Sahara.[9] The timing of the revelations was seen by some opposition politicians as a smoke screen to hide CNI's role in the scandals uncovered by CitizenLab. This also represented a unique case of a government disclosing information on surveillance operations that had not been revealed beforehand by investigative journalists, NGOs or companies.

---

4 The Guardian, Phone of top Catalan politician 'targeted by government-grade spyware', July 2020, available at: https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware

5 Citizen Lab, CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru, April 2022, available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

6 Ibid.

7 Ibid.

8 Mediapart, Pegasus : Pedro Sánchez espionné, la confusion politique gagne l'Espagne, May 2022, available at: https://www.mediapart.fr/journal/international/020522/pegasus-pedro-sanchez-espionne-la-confusion-politique-gagne-l-espagne

9 NPR, A spying scandal and the fate of Western Sahara, May 2022, available at: https://www.npr.org/2022/05/11/1098368201/a-spying-scandal-and-the-fate-of-western-sahara

In a closed-door meeting of the Spanish parliament's "Commission for the Control of Credits Allocated to Reserved Expenditures" (commonly referred to as the officials' secret commission), the CNI admitted to being responsible for the targeting of 18 pro-independence activists - but claimed it had done so under authorisation from the Supreme Court.[10] There is a discrepancy between what was admitted in the Commission and the 63 people targeted according to CitizenLab.[11]

A few days later, Paz Esteban, the Director of the CNI, was replaced after calls by some politicians and civil society organizations to restore confidence in the country's intelligence community.

2.2. Legal framework for acquisition and use of spyware in Spain

2.2.1. The acquisition of spyware

At the **international level**, the export of spyware is regulated by the non-binding **Wassenaar Arrangement**, to which all EU Member States bar Cyprus are party. The Arrangement was amended in 2012 and 2013 to expand its coverage to include technology under the following terms: 'intrusion software', 'mobile interception or jamming equipment' and 'Internet Protocol (IP) network surveillance systems'.[12] Supporting guidance on the Wassenaar Arrangement further states that export licences should not be issued to a private company if their product may "be used for the violation or suppression of human rights and fundamental freedoms".[13]

At the **EU level**, dual-use exports are governed by **Regulation 2021/821** setting up a Union regime for the control of exports, transfer, brokering and transit of **dual-use items**[14]. The Regulation builds on previous legislation by modernising and updating the list to technologies covered by export controls, in particular in the field of emerging technologies.

The Wassenaar Arrangement is not legally binding, while there are "divergent interpretations and applications"[15] at national level of the terminology used in the Arrangement. In the EU, Regulation 2021/821 allows Member States to address the risk of human rights violations linked with trade in cyber-surveillance technologies. It also enhances the EU's capacity to control the flow of trade in sensitive new and emerging technologies. However, given its recent implementation, it is not possible to assess its effectiveness.[16]

In Spain, the General Secretariat for Foreign Trade (Secretaría General de Comercio Exterior), the Customs Department (Agencia Tributaria - Aduanas) and the Foreign Office Ministry (Ministerio de

---

[10] El Nacional, Spain's CNI admits spying on Aragonès and on Puigdemont's circle, with court approval https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html

[11] CitizenLab, CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru, available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

[12] Bauer, S. and Bromley, M. 2016. The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World. Non-Proliferation Papers by the EU Non-Proliferation Consortium. No. 48.

[13] The Wassenaar Arrangement – On Export Controls for Conventional Arms and Dual-Use Goods and Technologies, About Us. http://www.wassenaar.org .

[14] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)

[15] Immenkamp, B (European Parliamentary Research Service). 2017. Review of dual-use export controls: European Parliament Briefing: EU Legislation in Progress, available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf.

[16] See Portolano Cavallo, European Union adopts new regulation no. 2021/821 on dual use, 2021, available at: https://portolano.it/en/newsletter/portolano-cavallo-inform-compliance/european-union-adopts-new-regulation-no-2021821-on-dual-use.

Asuntos Exteriores, Unión Europea y Cooperación) are the authorities empowered to grant licences and to decide to prohibit the transit of dual-use items.[17]

2.2.2. The use of spyware

The Spanish **Constitution** recognises the right of privacy of communications including the confidentiality of "postal, telegraphic and telephone communication" (Section, 18 (3)).

The **Criminal Code criminalises** a number of actions related to the **use** and **acquisition** of spyware. According to article 197, whoever seizes "*electronic mail messages or any other documents or personal belongings, or intercepts his telecommunications or uses technical devices for listening, transmitting, recording or to play sound or image, or any other communication signal*", is liable to a **prison sentence of up to four years**.

Article 264 ter states that '*whoever, without being duly authorised, produces, acquires for use, imports or, in any way […] provides third parties with' a programme, password an access code or similar data enabling access to all or part of an information system […] shall be punished* with a prison sentence of six months to two years in prison or a fine of three to eighteen months (of the person's salary).

Article 264 criminalises the erasure, damage, deterioration, alteration, suppression or making inaccessible data, computer programmes or electronic documents. However, the article does not criminalise the fact of gaining access to document or communications.

In some cases, set out in in Part I, Chapter V of the Constitution, some rights and freedoms can be suspended. Section 55(2) refers to the suspension of some rights for individuals subjected to investigations of the activities of armed bands or terrorist groups. It does however require "*necessary participation of the courts and proper parliamentary control*"[18].

The Criminal Procedure Act also provides some detail on investigations affecting the rights enshrined in Article 18 of the constitution (i.e. right to privacy). The "***interception*** *of telephone and telematic communications, capture and recording verbal communications with the use of electronic devices, use of technical devices for image surveillance, location and capture, search of mass data storage devices and remote searches of computer equipment*" is allowed in the Act if a **judicial authorisation is issued by a judge** (art 588 a. ii), and fully subject to the following principles (art. 588 a. i.):

- **speciality**: the measure is related to a specific crime;
- **adequacy**: setting out the objective and subjective scope as well as the duration on the measure;
- its **exceptional nature** and **necessity**; no other measure is available, or the investigations would be hampered without the measure), necessity and proportionality of the measure;
- **proportionality**: which includes the severity of the case, its social transcendence or the technological field of production, the strength of existing prima facie evidence and the relevance of the result sought.

[17] Liger Q. et al., The use of Pegasus and equivalent surveillance spyware, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, 2023.

[18] Spanish Constitution, Part I, Chapter V, Section 55(2).

These principles apply to all interceptions listed above, as well as the interception of telephone and telematic communications and extended to any two-way telematic communication system - such as WhatsApp, SMS and covert listening devices.[19]

The Spanish intelligence community is made up of three main organisations:

- the **National Intelligence Service** (Centro Nacional de Inteligencia, CNI), which acts as both a domestic and foreign intelligence service. The CNI is under the control of the Ministry of Defence (reflecting its history as the Higher Centre for Defence Intelligence, which it replaced in 2002). The Director of the service is appointed by the King at the proposal of the Minister of Defence. The Director has a specific relationship with the Prime Minister, being its main advisor for intelligence and counter-intelligence;[20]
- The **Intelligence Center for Counter-Terrorism and Organized Crime** (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, CITCO), the domestic intelligence agency responsible in particular for terrorism, organised crime and violent radical organisations;
- The **Spanish Armed Forces Intelligence Center** (Centro de Inteligencia de las Fuerzas Armadas, CIFAS), the defence intelligence agency; under the Ministry of Defence and Prime Minister.

The **CNI was responsible for the use of spyware targeting journalists, lawyers, human rights defenders and political representatives**. The CNI was established by law 11/2002 that authorises it to carry out "security investigations", without specifying the mechanism or the limits of such investigations.[21]

2.2.3. Oversight and redress in Spain

In a democratic society, law enforcement and intelligence services shall strive to operate effectively while fully complying with democratic norms and standards, rule of law requirements and fundamental rights. They shall be politically neutral and non-partisan, adhere to a strict professional ethic and operate within their legal mandates, in accordance with the constitutional-legal norms and democratic practices of the state. Public accountability is necessary to eliminate any risk of abuse of power.[22]

2.2.4. Ex-ante – oversight

In the field of criminal cases, the Judiciary Police or the Public Prosecution Services must ask authorisation to use special investigative techniques. A judge is responsible for allowing the use of the investigation technique (including the use of spyware). In order for an order to be granted, it must include inter alia:

- The description of the event under investigation,
- A detailed justification of the grounds for the use of the technique,
- The extent of the measure and specification of its content,

---

19 FRA, National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, July 2016.

20 See CNI website, available at: https://www.cni.es/en/about-the-cni/controls-of-the-cni

21 OMCT, Spain: State surveillance on journalists, politicians, and lawyers, May 2022.

22 Gill, Peter. 2003. Democratic and Parliamentary Accountability of Intelligence Services after September 11th. Geneva, January 2003. Geneva Centre for the Democratic Control of the Armed Forces. Working Paper No. 103, quoted in Geneva Centre for the Democratic Control of Armed Forces, Intelligence practice and democratic oversight – a practitioner's view, July 2003.

- The duration of the measure applied for.[23]

The judge has 24 hours to respond to the request. Once granted, the measure has to be limited in time, the Judiciary Police must inform the magistrate about the development and the use of the technique.[24]

In terms of surveillance by intelligence services, the process is different. The ex-ante oversight mechanisms for the CNI (which was responsible for the use of spyware in Spain) are set out in Organic Law 2/2002, which prescribes a special procedure to request judicial authorisation for surveillance activities, and Law 11/2002 which establishes parliamentary control by the Official Secrets Committee of the Spanish Congress. The CNI is under the executive control of the Delegated Committee for Intelligence Affairs which coordinates its intelligence-related activities. Parliamentary oversight is exercised by the Defence Committee of the Congress of Deputies.[25]

The **CNI can ask a Magistrate of the Supreme Court for an authorisation to intercept** communications on the grounds of a threat to the territorial integrity of Spain or the stability of the rule of law "provided that such measures are necessary for the fulfilment of the tasks assigned to the Centre"[26]. The authorisation can be based on much looser concepts, which, in the words of a professor of constitutional law, "almost anything can fit".[27]

Following the revelations of the CNI's use of Pegasus and Candiru, Spain's **Ombudsperson**, the *Defensor del Pueblo* investigated the legality of the practice. The investigation concluded that: "the CNI took action respecting the various legal provisions for prior judicial control of the intervention in communications that took place in the cases of a part (18) of the people alluded to in different media information published in April".[28]

CitizenLab's conclusion on the role of the government, raised "*urgent questions about whether there is proper oversight over the country's intelligence and security agencies, as well as whether there is a robust legal framework that authorities are required to follow in undertaking any hacking activities*".[29]

In May 2022, after the story broke, the government announced two initiatives. The first one is to **update the law on official secrets**, which dates from 1968, and had not been revised since the country's transition to democracy. The second is a **revision** of the Organic Law Regulating Prior **Judicial Control**

---

23 Art 588 a. ii. of the Criminal Procedural Code.

24 Art 588 a. iii. to 588 a. xi. of the Criminal Procedural Code.

25 Florina Cristiana Matei, Andrés de Castro García & Carolyn C. Halladay (2018), On Balance: Intelligence Democratization in Post-Franco Spain, International Journal of Intelligence and CounterIntelligence, 31:4, 769-804, DOI: 10.1080/08850607.2018.1466588 p.776, available at: https://doi.org/10.1080/08850607.2018.1466588

26 Law 2/2002, 6 May, Regulating The Prior Judicial Control Of The National Intelligence Center (Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.), available in English at: https://www.global-regulation.com/translation/spain/1451142/law-2-2002%252c-6-may%252c-regulating-the-prior-judicial-control-of-the-national-intelligence-center.html

27 EPRS, Europe's PegasusGate – countering spyware abuse, July 2022.

28 Defensor del Pueblo, El Defensor del Pueblo verifica que la actuación del CNI se ha realizado conforme a la Constitución y la Ley en los casos examinados, 18 May 2022 available at: https://www.defensordelpueblo.es/noticias/defensor-del-pueblo-verifica-la-actuacion-del-cni-se-ha-realizado-conforme-la-constitucion-la-ley-los-casos-examinados/

29 Citizen Lab, CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru, April 2022, available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

of the CNI with the aim to strengthen the guarantees of this control, as well as to ensure maximum respect for individuals' political and individual rights.[30]

The public consultation for the update of the law on official secrets was initiated in August 2022 and its contents were criticised by civil society organisations, as well as the fact that holding the consultation in August discouraged citizens' participation.[31]

2.2.5. Ex-post – sanctions and remedies

Information related to intelligence services and their activities is excluded from the law on Transparency and Access to Public Information and Good Governance.[32]

Ex-post mechanisms in Spain are principally under the auspices of:

- Spain's **Ombudsperson**, the ***Defensor del Pueblo***. As mentioned above, the *Defensor* can undertake inquiries on topics related to gathering intelligence by law enforcement authorities. It may ask the public authorities all documents deemed necessary for the development of its function, including those classified with the nature of secrets in accordance with the law. It must be noted that the *Defensor* treats complaints by individuals in relation to activities conducted by the police but not by the CNI;
- **Official Secrets Committee** of the Spanish Congress (officially the Commission for the Control of Credits Allocated to Reserved Expenditures)[33]. The Committee was created in 1995.[34] The law setting up the CNI mentions that the Committee has access to classified matters. The CNI must have appropriate information on the running and activities of intelligence objectives assigned by the Government, with an annual activity report. However, by the time the committee convened in light of the Pegasus and Candiru scandals, this was its first sitting in over two years.

The fact that the *Defensor* has only been able to focus its investigation on 18 people which were targeted by spyware following a court authorisation and to conclude on the lack of breach of the legal framework in those cases demonstrates that this ex-post oversight mechanism is not as effective as it could be. The same can be said about the parliamentary commission, given it had not convened in over two years at the time when a scandal was unfolding.

From a judicial point of view, there are no specialised judges appointed for surveillance cases in Spain[35]. Anyone has the right to obtain effective protection of the Judges and the Courts in the exercise their legitimate rights and interests. In this sense, any citizen considering their fundamental rights have been violated can seek **judicial redress**.

---

30 La Moncola, president's news, Pedro Sánchez announces a reform of the legal control regulation of the National Intelligence Centre (CNI) to strengthen its guarantees, May 2022, available at: https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx

31 See Access Info, Alegaciones al Anteproyecto de la Ley de Información Clasificada, August 2022, available at: https://www.access-info.org/wp-content/uploads/2022-08-12-Access-Info-Alegaciones-Ley-de-Informacion-Clasificada.pdf

32 Law 19/2013 on Transparency, Access to Public Information and Good Governance (Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno).

33 Comisión de control de los créditos destinados a gastos reservados, usually called Comisión de Secretos Oficiales.

34 Law 11/1995, of May 11, regulating the use and control of credits for reserved expenses Ley 11/1995, de 11 de mayo, reguladora de la utilización y control de los créditos destinados a gastos reservados, available at: https://www.boe.es/buscar/act.php?id=BOE-A-1995-11339

35 Article 24 of the Spanish Constitution.

Targets of the Pegasus and Candiru spyware from the CNI have **filed a lawsuit** in Spain, as well as in the countries where the targets were located when spied upon. The lawsuit is **against NSO, one of its subsidiaries, and its three founders, but not against the Spanish state**.[36] The case is still pending.

[36] Mediapart, Pegasus : vers un nouveau front judiciaire pour les indépendantistes catalans, April 2022, available at: https://www.mediapart.fr/journal/international/250422/pegasus-vers-un-nouveau-front-judiciaire-pour-les-independantistes-catalans

3. CONSIDERATIONS ON RULE OF LAW, DATA PROTECTION AND PRIVACY IN SPAIN

3.1. Rule of law in Spain

2022 Rule of law report indicated in its Spanish chapter that the fact that the renewal of the Council for the Judiciary is pending since December 2018 remains a concern. In this context, there have been further calls to modify the Council's appointment system in line with European standards so that no less than half of judges-members are elected by their peers.

Legal amendments were adopted aiming at an increased transparency of relations between the Government and the Prosecutor General, while concerns on the coincidence in the term of office of the Prosecutor General and the Government remain.

The Judicial Ethics Committee issued an opinion on the ethical duties of judges who return to their judicial functions after having held political office.

Among other issues indicated in the report are:

- on 1 January 2022, Spain had **23 leading judgments from the European Court of Human Rights pending implementation**. At that time, Spain's rate of leading judgments from the past 10 years that remained pending was at 61%, the average time that the judgments had been pending implementation was 3 years and 1 month;

- the reform of the **Citizen Security Law** continues to be discussed in Parliament. On 8 February 2022, the Council of Europe Commissioner for Human Rights indicated that the reform is still not addressing important aspects affecting the rights of freedom of expression and freedom of assembly and makes a number of recommendations to tackle these aspects. Stakeholdershave continued raising concerns about the law, as already noted in the 2021 Rule of Law Report. Those concerns relate to, among others, offences in the context of meetings and demonstrations, and the use of images or data by the police.

The 2022 Rule of law report of the European Commission noted as well that the use of Pegasus and equivalent spyware surveillance software was subject to **an investigation by the Ombudsperson and judicial proceedings in Spain**. On 24 April 2022, the office of the Ombudsperson announced a public investigation into the use of the Pegasus and equivalent spyware surveillance software. It has been revealed that a number of political representatives, including high-ranking members of the Government, as well as several lawyers, had been allegedly targeted by said spyware. Two judicial investigations have also been launched.

On 24 October 2022, Mr. Fernand de Varennes, UN Special Rapporteur on minorities, Ms. Irene Kahn, UN Special Rapporteur on freedom of opinion and expression and Mr Clement Nyaletsossi Voule, UN Special Rapporteur on freedom of peaceful assembly and of association, expressed their concerns and requested Spanish government for information in connection with the activities of espionage through the use of Pegasus and Candiru spyware over a wide number of Catalan personalities and activists during the period 2017-2020, indicating that the victims of the complex and sophisticated spy programs included Catalan leaders, members of the European Parliament, legislators, jurists and members of civil society organizations as well as their families.

Spanish government replied in the letter of 22 Decemer 2022, indicating that there are ongoing judicial proceedings as well as pointing at conclusions of the investigation launched by Spanish Ombudsperson, according to which the actions of the National Intelligence Center (CNI) in the cases

examined in the context of the Pegasus, have been carried out in accordance with the Constitution and the laws.

On 2 February 2023, the UN Rapporteurs stated that "Spanish authorities must conduct a full, fair, and effective investigation into these allegations, publish the findings and stop any unlawful interference into the fundamental rights of the Catalan minority activists in Spain" as well as that they were "deeply concerned by what appears to be a very troubling interference into the human rights of Catalan leaders and other minority activists to freely hold and express their views, exchange information and ideas, assemble peacefully and participate in associations. They are entitled to a private life, the privacy of correspondence and to be treated equally before the law".

3.2 Data protection and privacy in Spain in the context of Pegasus

The study on the impact of Pegasus on fundamental rights and democratic processes prepared by Policy Department C for PEGA Committee clarified that the use of spyware is usually justified by invoking national security or law enforcement purposes. However, **it appears that in many cases spyware is used for other purposes, often pertaining to partisan political objectives or to the repression of social and political dissent.** It has been recognised that many states have used national security as a pretext to curtail freedom of expression, legitimise torture and other ill-treatment, and exert a chilling effect on minorities, activists, and political opposition. In particular, extensive evidence exists on Pegasus being used to target individuals not having any connection to serious crimes or national security threats, such as political opponents, human rights activists, lawyers, and journalists. To prevent an expansive use of the notion of national security, this notion should be understood restrictively and distinguished from the concept of internal security, the latter having a broader scope, including the prevention of risks to individual citizens, and in particular the enforcement of criminal law.[37]

According to the study the EU law notion of national security —while accommodating different national evaluations relative to what serious threats most endanger a national community—**certainly cannot include activities aimed at targeting political opponents or minorities**.[38]

The first communication on data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, prepared by the European Commission, covering the period during which Member States used Pegasus, does not mention Pegasus. The staff working with reference to Sparin indicates in a general way that between May 2018 and end of November 2019, Spain was among Member States with the highest numbers of complaints to data protection authorities (18 000 complaints).

The first report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 (LED), published by the European Commission on 25 July 2022, covering the period during which Member States used Pegasus, does not mention Pegasus.

WIth regard to Spain the report recalls that in 2021, the Commission referred its infringement action against Spain to the CJEU because it had still **failed to transpose the Law Enforcement Directive and**

[37] Sartor, G. et al., The impact of Pegasus on fundamental rights and democratic processes, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, December 2022, p. 35.

[38] Idem, p. 48

notify the Commission of its transposition measures. Given the seriousness and duration of the infringement, the CJEU, for the first time, imposed both a lump sum and a penalty payment on Spain,[39]

Leuven University, on the request of Policy Department C, prepared a study **providing a more detailed assessment of the implementation of the Law Enforcement Directive**.

The study points that Spain is among a few Member States that provide for explicit definitions of national security within their national legal orders. Spain, along with Cyprus, Czech Republic, Hungary, Italy, Luxembourg, Malta and Romania, understand national security as intertwined with public security, including aspects such as the fight against organised crime and terrorism, as well as the safeguarding of financial interests and **internal security**.

The study points that **the use of Pegasus constitutes targeted surveillance**, which is regulated by national law, as well as it **must abide by EU law insofar as it falls within its scope, including the Charter, the EPD and the LED**. Purely governmental activities in pursuance of national security purposes fall outside the scope of EU law, however they **must still meet national and international, including the European Convention on Human Rights (ECHR), requirements against unlawful use**.

The study points that besides the questionable uses of Pegasus for national security purposes, **all uses for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, certainly fall under the scope of EU law, and thereby must abide by the Charter, EU data protection and other relevant legal frameworks**.

In his assessment of the compliance of the use of Pegasus with Article 52(1) Charter, the European Data Protection Supervisor found that **it would likely not reach the necessity and proportionality threshold, while it also affects the essence of the right to privacy**. Therefore, the EDPS suggested a ban on the development and the deployment of spyware with the capability of Pegasus in the EU, while he considers that, in case certain features of Pegasus were to be nevertheless applied in exceptional situations, for instance to prevent a very serious imminent threat, a number of steps and measures should be enforced to prevent unlawful use. In that regard, the **strict implementation of the EU legal framework on data protection, especially the LED transposition and enforcement, and of the relevant CJEU judgements (e.g. above on data retention) would be of outmost importance**.[40]

[39] Judgment of 25 February 2021, European Commission v Kingdom of Spain, C-658/19, EU C 2017 548.

[40] Vogiatzoglou, P. et al., Assessment of the implementation of the Law Enforcement Directive, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, December 2022, p. 44.

ANNEX

Comparative table of legal systems concerning spyware, including Spain

	FR	DE	IT	NL	PL	HU	ES	EL
Right to privacy - confidentiality of communica-tions - data protection	- not in the Constitution - Article 9 of the *Code Civil,* - Post and Electronic Communications Code (*Code des postes et des communications électroniques*) - domestic law application of the European Convention on Human Rights. - French Constitutional Court jurisprudence	the right to privacy of correspondence, posts and telecommunications is included in the German Constitution (Basic Law – Grundgesetz §10) and has been highly protected	While the Italian Constitution does not expressly refer to a right to privacy or data protection, the Constitutional Court and Supreme Court regularly defined the privacy as a fundamental human right	The right to privacy is protected by articles 10 (general right to privacy), 11 (inviolability of one's body), and 13 (secrecy of correspondence) of the constitution.	The right to privacy is protected by article 47 of the constitution, with the right the privacy of communications covered by art. 49.	**- in the Fundamental law**	**Constitution recognises the right of privacy of communications**	The Greek constitution enshrines the rights to be "protected from the collection, processing and use, especially by electronic means, of their personal data" (art. 9A)
Definitions Hacking, spyware etc.	**- spying:** capture, saving or transmission of voice, images and geo-localisation information without the knowledge or consent of the person targeted (art. 226-1). - **opening, deleting, slowing or diverting** the transmission […] and **obtaining the contents** of the communication (art. 226-15). **- hacking:** "*to access or stay in a fraudulent manner in all or part of an automated data processing system*" - **use of spyware** (article 323-3 of the	**- hacking** (i.e. unauthorised access) according to Sec. 202a and Sec. 202b (so called "**data espionage**", Sec. 202a , and "**phishing**" Sec. 202b). Sec. 202a defines "data espionage" as unlawfully obtaining data for oneself, or another, that was not intended for one and was especially protected against unauthorised access, and circumventing protection. - Depending on the case, "hacking" could possibly come under the definition of both	- **hacking**: art. 615-quarter of the Codice Penale, covers anyone who "*illegally procures, holds, produces, reproduces, disseminates, imports, communicates, delivers, makes available to others or installs equipment in any other way, tools, parts of equipment or tools, codes, keywords or other means suitable for accessing a computer or telematic system, protected by security measures*".	**hacking** is defined as 'computer intrusion" and is defined as the 'unlawful intrusion of automated systems". The crime covers the use of spyware (access by a technical intervention).	- **hacking**: *"whoever without authorisation obtains access to an information not meant for them, by opening a sealed letter, connecting into a telecommunications network, or by breaking or avoiding electronic, magnetic, informatic or other special protection of such network..."* - other related similar crimes (see below sanctions) - phishing - **infecting IT systems with malware**	**- Hacking: illegal data acquisition** - criminal **offences against information systems**	**hacking** - seizing electronic mail messages or any other documents or personal belongings, or intercepts his telecommunications or uses technical devices for listening, transmitting, recording or to play sound or image, or any other communication signal	**hacking** as the unauthorised access to electronic data, (art. 370B(1), the unauthorized access to information systems or to information transmitted through **telecommunications systems, which (art. 370D(2).**

	FR	DE	IT	NL	PL	HU	ES	EL
	criminal code): "*fraudulent introduction, extraction, detention, reproduction transmission, deletion or modification of data in an automated data processing system*". - **spyware** (guideline published in the official journal): "*software designed to collect and transmit to third parties and without the knowledge of user data about the user or information relevant to the system she uses"*	of the offences set out above, depending on the level of protection applied to the data in question. .- **Infection of IT systems with malware**						
Sanctions (in general, hacking is criminalized in the Criminal Code)	up to three years' imprisonment and a fine of up to EUR 100 000.	- **hacking**: imprisonment not exceeding three years, or a fine. - phishing: imprisonment for up to two years or a fine, unless the offence is subject to a more severe penalty under other provisions	- **hacking** (i.e. the unauthorised access to IT and telematic systems - art. 615-ter): of **up to three years imprisonment**. - **five years in specific cases**	**Hacking** is a crime under article 138ab of the Code of Criminal Procedure is liable to up to two years in prison and a fine of fourth category. When the instruction leads to taking control of a device or the taping of data stored or transmitted from the device, the sanction rises to four years in prison.	- Art 267: imprisonment of up to **two years** for **hacking**, **eavesdropping**, using visual or other tools or programs, revealing information obtained by means described above to another person. Offences are prosecuted upon the request of the victim. - **fine** of up to EUR 2.3 million - GDPR penalties: up to EUR 20 million or, in the case of an enterprise, up to 4% of its total annual global turnover	- unauthorised **interceptions**: up to three years' imprisonment - **spyware**: up to two years' imprisonment	**prison sentence of up to four years**	Up to five years' imprisonment

	FR	DE	IT	NL	PL	HU	ES	EL
					- **phishing** up to 5 years imprisonment - **infecting IT systems with malware**: up to 5 years imprisonment			
Spyware	**Criminal Code forbids** manufacture, import, possession, display, offer, rental or sale, or installation (art. 226-3).	The infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses) constitutes a criminal offence according to the German Criminal Code ("computer sabotage")	Criminal Code prohibits it (art. 615-quarter) and acts like: *illegally procures, holds, produces, reproduces, disseminates, imports, communicates, delivers, makes available to others or installs equipment in any other way, tools, parts of equipment or tools, codes, keywords or other means suitable for accessing a computer or telematic system, protected by security measures*"	**hacking** is defined as 'computer intrusion" and is **Hacking** is defined as the 'unlawful intrusion of automated systems". The crime covers the use of **spyware** (access by a technical intervention).	- criminal offences under Section 269b of the Criminal Code: **distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime**.	- spyware: up to two years' imprisonment	According to article 197, whoever seizes "electronic mail messages or any other documents or personal belongings, or intercepts his telecommunications or uses technical devices for listening, transmitting, recording or to play sound or image, or any other communication signal", is liable to a prison sentence of up to four years	Infecting an IT system with malware (including spyware) is a criminal offence and covered by different articles of the criminal code depending on the type of infection. This includes art. 292 on crimes against the security of telephone communications, art. 292B on hindering the operation of information systems, art. 370 on the violation of the secrecy of letters
Sanctions on spyware	up to **five** years' imprisonment and a fine of up to EUR 300 000.	up to **five** years' imprisonment	punished by up to **one year imprisonment** and a **fine** of EUR 5 164	up to two years in prison and a fine of fourth category	- Anyone who creates, obtains, transfers or allows access to hardware or software adapted to commit cybercrime (e.g. damaging, databases, preventing automatic collection and transmission of data, or hindering access to data) is liable to imprisonment for up to **five** years.	- spyware: up to two years' imprisonment	up to four years' imprisonment	up to five years' imprisonment

	FR	DE	IT	NL	PL	HU	ES	EL
					- Anyone who **creates, obtains, transfers or allows access to hardware or software adapted to commit cybercrime**, including computer passwords, access codes or other data enabling access to the information collected in the computer system or telecommunications network, is liable to imprisonment for up to **three** years. - **Unsolicited penetration testing:** fine (up to PLN 1.08 million), restriction of liberty or imprisonment for up to two years			
Criminal cases – Who can **request** the use of special investigative techniques	Law Enforcement purposes - requested by public prosecutor or investigative judge	President of the Federal Criminal Police Office or public prosecutor	the public prosecutor	public prosecutor to submit a written request asking for a written prior authorisation	investigative authority	Public prosecutor's office	Public Prosecution services	investigative authority
Criminal cases – Who can **authorise** the use of special investigative techniques	the liberty and custody judge (juge des libertés et de la détention) if requested by the public prosecutor. Otherwise the investigative judge	Judge (court)	Judge	The investigative judge	local district court	Judge	Judge - has 24 h to respond	Prosecutor of the court of appeal or a judicial council for more serious crimes
Criminal cases – which	Offences falling within the scope of Articles	Criminal cases considered relevant for	The crimes include crimes for which the	Any offence which warrants pre-trial	Almost all crimes - Evidence may not be	The surveillance of private citizens can only	Suspension of some rights for individuals	Organised crimes, counterfeiting, human

	FR	DE	IT	NL	PL	HU	ES	EL
offenses are covered?	706-73 and 706-73-1 of the code of criminal procedure.	Telecom Surveillance (100a STGB): • Crimes of peace treason, high treason and endangering the democratic constitutional state as well as treason and endangering external security ; • Corruption and bribery of elected officials; • Offenses against national defence • criminal offenses against public order; • Counterfeiting money and stamps; • Offenses against sexual self-determination; •Distribution, acquisition and possession of child and youth pornographic content; •Murder and manslaughter; •Offenses against personal liberty; •Gang theft; •Crimes of robbery and extortion; •Commercial stolen goods, gang stolen goods and commercial gang stolen goods; •Money laundering; •Fraud and computer fraud;	penalty is over four years' imprisonment, crimes related to drugs, weapons and explosives, as well as smuggling, pedo-pornography, selling fraudulent foods, counterfeit goods, fraud and sale of fraudulent goods, persecution, and involvement on organised crime (associazione di tipo mafioso). In addition, crimes using the telephone as an object are also covered.	detention. This includes all crimes for which the prison sentence imposed is over 4 years, Further crimes include breaking and entering, squatting, hacking, wiretapping, participation in an organised criminal group, the use of recurring discriminatory or insulting language, illegal disposal of a body, paedophilia, grooming and child pornography, violation of secret, use of violence, fraud, destruction of property (and data), hijacking of ships or planes, money-laundering.	considered inadmissible solely on the grounds of the fact that it has been obtained in violation of the rules of procedure or by means of a prohibited act referred to in Article 1(1) of the Criminal Code, unless the evidence has been obtained in connection with the performance by a public official of his/her personal duties with regard to a murder, wilful injury or deprivation of liberty	be carried out with judicial approval. In matters of terrorism, however, the Police Act refers to the investigatory surveillance mentioned in the National Security Act. Under this provision, judicial approval does not have to be sought to approve the use of these techniques Instead the Minister of Justice is responsible for providing the authorisation.	subjected to investigations of the activities of armed bands or terrorist groups. It does however require "necessary participation of the courts and proper parliamentary control".	trafficking, rape and sexual abuse of a minor, child pornography) are explicitly mentioned as crimes warranting special investigative techniques. Corruption investigations are also included and covered by a separate article of the code of criminal procedure

	FR	DE	IT	NL	PL	HU	ES	EL
		•Subsidy fraud; •Sports betting fraud and manipulation of professional sports competitions; •Withholding and embezzlement of wages; •Criminal offenses of document forgery; •Bankruptcy; •Criminal offenses against competition; •Criminal offenses dangerous to the public; •Corruption and bribery.						
export of dual-use technologies must be authorised by	*Commission interministérielle des biens à double usage* (Cibdu) covered by national defence secret and therefore not public.	Federal Office for Economic Affairs and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle)	Ministry of Foreign Affairs and International Cooperation National Authority – UAMA (Unit for the Authorizations of Armament Materials)	Ministry for Foreign Affairs (Directorate-General for International Relations - Department for Trade Policy and Economic Governance)	Ministry of Entrepreneurship and Technology Department for Trade in Strategic Goods and Technical Safety	Government Office of the Capital City Budapest Department of Trade, Defence Industry, Export Control and Precious Metal Assay Export Control Unit	the General Secretariat for Foreign Trade (Secretaría General de Comercio Exterior), the Customs Department (Agencia Tributaria - Aduanas) and the Foreign Office Ministry (Ministerio de Asuntos Exteriores, Unión Europea y Cooperación) are the authorities empowered to grant licences and to decide to prohibit the transit of dual-use items	The Ministry of foreign affairs is responsible for authorising the export of dual-use goods (General Secretariat of International Economic Relations and Openness).
Security services	- Directorate General of Interior Security (Ministry of Interior) - Directorate General of External Security	There are 19 intelligence services, the most important are: - **Federal Intelligence Service**	- Agenzia Informazioni e Sicurezza Esterna (AISE),	**- General Intelligence and Security Service** (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) domestic, foreign	- Internal Security Agency - Intelligence Agency (foreign threats)	National Security Service: - Information Office (Prime Minister's office)	**- National Intelligence Service** (Centro Nacional de Inteligencia, CNI (internal / external)	• The National Intelligence Service (Ethnikí Ypiresía Pliroforión – EYP) – which is the country's national intelligence

	FR	DE	IT	NL	PL	HU	ES	EL
	(Ministry of the Armed Forces) - Directorate of Intelligence and Security of Defence (Ministry of the Armed Forces) - National Directorate of the Intelligence and Customs Investigations (Ministry of Economics and Finance)	**(Bundesnachrichtendienst – BND)** (foreign and military - chancellor's office) - **Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz - BfV)**: domestic, ministry of the interior, - **Military Counterintelligence Service (Militärischer Abschirmdienst - MAD)**: military	- Agenzia Informazioni e Sicurezza Interna (AISI)	and signals intelligence, protecting national security (Ministry of the Interior). - **Dutch Military Intelligence and Security Service**	- Central Anti-corruption Bureau	- the Constitution Protection Office (Minister of the Interior) - Military National Security Service (Ministry of Defence) - Counter-Terrorism Information and Criminal Analysis Centre - Special Service for National Security: assistance for other security services to gather intelligence.	**- Intelligence Center for Counter-Terrorism and Organized Crime** (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, CITCO), (domestic); - **Spanish Armed Forces Intelligence Center** (Centro de Inteligencia de las Fuerzas Armadas, CIFAS)	agency subject to the authority of the Prime Minister (following a change of law in 2019) and is responsible for both foreign and domestic intelligence gathering. • The Hellenic Police Intelligence Division (Διεύθυνσης Διαχείρισης και Ανάλυσης Πληροφοριών - HPiD) constitutes an independent central service acting as a central point for intelligence in the Hellenic Police. It is the intelligence Hub of the Hellenic Police, focusing on combating all forms of crime, but mainly Serious and Organised Crime and Terrorism.
Exceptions for security services	- Loi renseignement 2015 and 2021 regulates duration, severity of the threat, prime ministerial authorisation, etc	Since 2021 all **intelligence services can use state trojans**	Can do surveillance and hacking to achieve their aims	The decision is taken on the basis of a proportionality assessment and both the request by the public prosecutor and the authorisation decision of the investigative judge must be motivated on this basis. The Explanatory Memorandum of the	Procedures as simial to criminal cases, with a specific court in charge of authorising the use of special investigative techniques	- No need for judicial authorisation? - Special investigative techniques require the prior authorisation from a judge, the Minister of Justice, or the general directors of the National Security Services	CNI is authorised by law to carry out "security investigations" without specifying the mechanism or the limits of such investigations	For intelligence services, the process is similar to criminal cases, although the judicial order must have been issued by the Public Prosecutor of the Court of Appeal, specially assigned to the EYP, who supervises the EYP and controls the legality of its special operational activities as

	FR	DE	IT	NL	PL	HU	ES	EL
				law further requires the Central Review Commission (Centrale Toetsingscommissie) to provide advice to the investigative judge before it takes its decision.				set out in art. 5 of Law 3649/2008
Oversight: Ex-ante	**- Commission nationale de contrôle des techniques de renseignement (CNCTR) :** - mixed control committee - access and legal check - non-binding opinions, annual report = no enforcement mechanism **- Commission nationale de l'informatique et des libertés (CNIL)** **- Défenseur des droits** (Ombudsman)	- Criminal procedure code and law on the police: only be **ordered by the Court at the request of the Public prosecutor's office** **-** if imminent danger: public prosecutor office; falls if not confirmed by the court within three working days - 3 months max + 3	Spyware can be used with specific guarantees (Trojan di Stato): only org crime, only by LEAs, specific place, logged, data security	- **Secret services** can intercept with prior approval of the Minister responsible + authorisation of Investigatory Powers Commission. - In cases where a lawyer or a journalist is targeted, the additional oversight of a court is necessary, with the **District court of the Hague** being responsible for granting **permission** **Three-pronged authorisation:** 1 - internal controls - investigators to convince their internal jurists of the validity of the need for the use of the special investigative technique 2 - seek the approval of the Minister in charge of the services (Ministry	**- Sejm and Sejm Committee on Security Services** - **Supreme Audit Office** – exercises oversight of the services within the scope of responsibilities of the Office. **- Commissioner for Human Rights** over complaints **- State government bodies (Prime Minister, Minister** – Coordinator of Security Services, Government Council on Security Services) - **Courts and prosecutors** – supervise the conduct of secret surveillance and other surveillance operations by security services. **- The Internal Oversight Bureau of the Ministry of the**	- Parliamentary Committee on National Security: can request info - procedural guarantees: judicial authorisation by Budapest Metropolitan Court and Minister of Justice	- CNI is under the executive control of the Delegated Committee for Intelligence Affairs - Parliamentary oversight is exercised by the Defence Committee of the Congress of Deputies - CNI shall ask a Magistrate of the Supreme Court for authorisation to intercept communications on the grounds of a threat to the territorial integrity of Spain or the stability of the rule of law	- • The Special Standing Committee for Institutions and Transparency – a parliamentary committee in charge of overseeing policies; administration and management; and the legitimacy of the activities of the EYP. The committee oversees the National Intelligence Service

	FR	DE	IT	NL	PL	HU	ES	EL
				of Defence or of the Interior) 3 - Investigatory Powers Commission (Toetsingscommissie inzet bevoegdheden - TIB), whose role is to assess the legality of the approval. The TIB's decision is binding. The TIB is composed of two judges and one technical expert.	**Interior and Administration** supervises the secret surveillance operations carried out by the Police, the Border Guard and the State Protection Service.			
Oversight: Ex-post	**Commission nationale de contrôle des techniques de renseignement (CNCTR)** *See above*	The activities of the BKA and the German intelligence services are subject to judicial control and the technical and legal supervision of the government departments responsible for them (such as the Federal Chancellery, the Federal Ministry of Interior, the Federal Ministry of Defence). For the parliamentary control of the Federal Intelligence Service (BND) there is also the Parliamentary Control Committee of the Bundestag	Parliamentary Committee for the Security of the Republic (*Comitato parlamentare per la sicurezza della Repubblica* - COPASIR)	For LEAs: - Inspection of Public Order and Safety (*Inspectie Openbare Orde en Veiligheid)* - Obligation for LEAs to notify the target of surveillance For the intelligence agencies: - Review Committee on the Intelligence and Security Services: access, check legality of actions	**- Minister of Interior** annual (general) **report to the Polish Parliament**	- right to lodge a complaint with the Minister in charge - if dissatisfied, complaint to the National Security Committee of the Hungarian Parliament - complaint to the Ombudsperson, inquiry, can start criminal proceedings or involve the - National Authority for Data Protection and Freedom of Information: only recommendations	- Defensor del Pueblo / Ombudsman can make inquiries on police activities - but not CNI's - **Official Secrets Committee** of the Spanish Congress (officially the Commission for the Control of Credits Allocated to Reserved Expenditures: competent on CNI	• The Authority for Communication Security and Privacy (ADAE) – which is non-parliamentary committee designated by Parliament and appointed by the Minister of Justice, Transparency and Human Rights overseeing the EYP, the Hellenic police and the State Security Division. • The Hellenic Data Protection Authority (HDPA). An independent Authority not subjected to any administrative control. It pertains and answers to the Minister of Justice for budgetary purposes.

This briefing contains background materials for PEGA Committee's mission to Spain.
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 752.602

Print ISBN 978-92-848-0940-0 | doi:10.2861/63891 | QA-09-23-355-EN-C
PDF ISBN 978-92-848-0939-4 | doi:10.2861/745301 | QA-09-23-355-EN-N