FRIEDRICH NAUMANN FOUNDATION For Freedom.
Human Rights Hub

International Press Institute

WATCHING THE WATCHDOGS

Spyware surveillance of journalists in Europe and the ongoing fight for accountability

Jamie Wiseman, Szabolcs Panyi, Konstantina Maltepioti and Thodoris Chondrogiannos

ANALYSIS

Publication Credits

Publisher
Friedrich Naumann Foundation for Freedom
Truman-Haus
Karl-Marx-Straße 2
D-14482 Potsdam-Babelsberg

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit
/stiftungfuerdiefreiheitt

Created by
International Press Institute (IPI)
Spiegelgasse 2/29
1010 Vienna / Austria
ipi.media

On behalf of:
Friedrich Naumann Foundation for Freedom

Authors
Coordinating Author:
Jamie Wiseman

Contributing Authors:
Szabolcs Panyi, Konstantina Maltepioti,
Thodoris Chondrogiannos

Contact
Friedrich Naumann Foundation for Freedom
Human Rights Hub
Rue de Vermont 37-39
1202 Geneva / Switzerland
geneva@freiheit.org

Telefon +49 30 220126-34
Telefax +49 30 690881-02
E-Mail service@freiheit.org

Date
March 2024

Notes on using this publication
This publication is an information offer of the Friedrich Naumann Foundation for Freedom. It is available free of charge and not intended for sale. It may not be used by parties or election workers for the purpose of election advertising during election campaigns (federal, state or local government elections, or European Parliament elections).

Contents

Introduction

In 2024, the European Union enters a new era in the fight to protect journalists and press freedom from illegal spyware abuse. After months of debate and tense final negotiations, EU institutions reached a historic agreement on the European Media Freedom Act (EMFA) in December 2023. Among multiple new rules, the provisional deal includes strengthened safeguards for journalists and their sources from coercive surveillance, including spyware, under Article 4. These new rules outline that surveillance measures can only be permitted on a case-by-case basis "by an overriding reason of public interest", subject to prior authorization by a judicial authority. Explicit references to exemptions under national security grounds were removed, prompting EU leaders to hail the deal as a major step forward in the protection of journalists from unwarranted surveillance.

While the EMFA overall has been welcomed as a timely boost for safeguarding media pluralism and independent journalism, the impact the Article 4 provisions will have on limiting surveillance of the press remains in doubt and certainly falls short of initial expectations. After a spate of major surveillance scandals involving journalists in the EU in recent years, hopes were high that the EMFA would put an end to the abuse of advanced surveillance tools such as Pegasus or Predator to monitor journalists' communications. Yet uneasiness persists over whether the EMFA's provisions will be strong enough or whether the remaining loopholes can still be exploited by bad actors.

This report first reviews the last-minute negotiations over Article 4 of the EMFA, the compromise that was struck, and the loopholes that may remain. It then provides two case studies from EU member states in which highly intrusive spyware tools have been abused to surveil journalists in recent years: Greece and Hungary. These case studies tell the story of two surveillance scandals involving the monitoring of journalists and show how national security exemptions were used in both to circumvent legal restrictions, block accountability, and shield those responsible from scrutiny. The case studies offer worrying examples of why the compromise reached by EU institutions for the EMFA risks being too weak to properly protect journalists from surveillance. The report then reviews other cases of surveillance of journalists in EU member states before offering conclusions and recommendations for how Europe's journalists can best be protected from all forms of illegal surveillance.

A new era: green light for European Media Freedom Act (EMFA)

On December 15, 2023, a historic deal was struck on the passing of the European Media Freedom Act (EMFA). The provisional agreement reached between the European Council and the European Parliament would create a common framework for media services in the EU's internal market for the first time and establish rules to safeguard media freedom, media pluralism, and editorial independence in the EU. The provisional agreement – which is expected to be formally adopted in the spring of 2024 – sets out the obligation for member states to introduce requirements for media to provide transparency over ownership and funding, establishes strong safeguards for the independence of public service media, and provides for a European Board for Media Services to oversee issues of media pluralism and editorial independence. The approval of the Act was cautiously welcomed by media freedom groups in Europe as a landmark in the effort to safeguard media freedom and independent journalism across the bloc.

The last-minute negotiations centred on the strength of safeguards that should be required to protect journalists from intrusive surveillance. For months, national governments had debated the wording of Article 4, which sought to protect media from coercive measures to monitor and identify their sources, including through spyware surveillance. The initial proposal presented by the European Commission in September 2022 included a ban on the use of all types of spyware to hack into the devices of media, journalists, and their families, with exceptions under ten serious categories of crimes. These included offences such as terrorism, crimes against humanity, and the dissemination of child pornography.

Opposition to this element grew within some member states, represented in the EU Council, whose final negotiating position expanded this list to 32 crimes punishable by at least three years' imprisonment, which included offences such as trafficking in cars or hormonal substances. Most controversially, the Council introduced Article 4.4 stating that the aforementioned safeguards on surveillance of journalists would apply "without prejudice to the responsibility of Member States to safeguard national security."

This text was met with strong criticism by press freedom groups who feared this would provide a blanket exemption for Member States to surveil journalists without restriction by citing national security. In November they reiterated their call that protection of sources must align with human-rights standards. and that references to national security must be removed.

Meanwhile the Parliament's negotiating position had set up far higher safeguards including that surveillance and the use of spyware can only be used in a case of overriding public interest, would be decided on a case-by-case basis, require prior authorization from an independent judge, and that any surveillance could not cover a journalist's sources or professional activities.

After final negotiations, the EU Commission announced on December 15 that a deal had been reached which included "improved protection of journalistic sources, including against the use of spyware". The national security article had been replaced by a clause stating that "the Member States' responsibilities as laid down … in the EU Treaties … are respected".

Guarantees were also reached that any surveillance of journalists, their sources, or their families, would require prior authorization from a judicial authority with an overriding reason of public interest. When surveillance does occur, those targeted will have the right to be informed and benefit from judicial protections. Intrusive surveillance of journalists would be justified only in investigations for offences involving crimes punishable by a custodial sentence of at least three years in the respective member state.

After the compromise was announced, the vice-president of the European Commission for Values and Transparency, Věra Jourová, welcomed the agreement, stressing that the EMFA "makes sure that journalists are protected in their work, also against intrusive spyware and that public media does not become a propaganda tool of one party."

Concerns, however, persist over the effectiveness the provisions within Article 4 will have in protecting journalists and their sources from surveillance. In the text of the provisional agreement, the number of alleged crimes which security and intelligence authorities can use to break into the private communications of journalists remains broad, and despite the compromise on language, national security justification can be used in certain occasions under the existing EU treaties.

In EU member states with weak rule of law or compromised judicial authorities and courts, judges may continue to approve requests for surveillance of journalists on national security grounds even if they appear unfounded. And as the case studies on Greece and Hungary in this report show, securing accountability for unwarranted surveillance or use of spyware against journalists has been extremely difficult if not impossible, underscoring the limits of domestic remedies.

Overall, Article 4 sets minimum levels of safeguards for the surveillance of journalists that did not previously exist under EU law. These fall short of the standards set out in the case law of the European Court of Human Rights, but do provide a new legal mechanism to protect journalists and their sources. Moreover, EU member states remain legally obliged to follow the ECtHR case law through membership of the Council of Europe.

While member states will be able to adopt stricter or more detailed rules on surveillance of journalists than those set out in Article 4, the bloc's worst offenders will still be able to exploit the loopholes to continue to abuse spyware against journalists. In this light, the inability of EU institutions to agree on a stronger ban on the use of spyware surveillance of journalists was a missed opportunity and risks the continuation of state-sponsored surveillance of journalists.

The following sections provide two case studies from EU member states in which highly intrusive spyware tools have been abused to surveil journalists: Greece and Hungary. In both states, national security exemptions have been used to circumvent legal limitations, block accountability, and shield the intelligence agencies and governments responsible from scrutiny. Both case studies also illustrate how existing rules meant to protect journalists from unjustified surveillance were bypassed using national security justifications, without proper oversight. Ultimately, the stories of surveillance in Greece and Hungary offer worrying examples of why the compromise reached by EU institutions for the EMFA risks being too weak to properly protect journalists from surveillance, with serious implications for media freedom and the rule of law in the European Union.

Predatorgate: The case of Greece

By Konstantina Maltepioti and Thodoris Chondrogiannos, journalists at Greek investigative media Reporters United

Part I: The story so far

The two-fold Greek surveillance scandal, dubbed PredatorGate, started in January 2022 with revelations by independent investigative media outlets regarding the wiretapping for reasons of national security by the Greek National Security Agency (EYP) and the illegal use of Predator spyware against targets in Greece.

The EYP wiretapping of citizens under the pretext of national security had already been reported on November 14, 2021 after leaked internal documents showed the surveillance of journalists, lawyers, and people involved in refugee issues. Journalist Stavros Malichudis discovered through those documents that he had been monitored while covering the ill-treatment of a 12-year-old Syrian child in the Greek islands.

In January 2022, the Greek government controversially amended Law 2225/1994, denying individuals the right to know whether or not they have been the subject of surveillance for reasons of national security by EYP, which was brought under the direct supervision of Prime Minister Kyriakos Mitsotakis in July 8, 2019. On January 7, 2022, it was revealed that Greece appeared as a possible client of the Predator spyware in two separate reports by CitizenLab and Meta (Facebook).

On April 11, 2022, it was revealed that the phone of financial journalist Thanasis Koukakis was infected with the Predator spyware between July 12 and September 24, 2021. A few days later, it was further revealed that between June 1 and August 12, 2020, Koukakis's phone was wiretapped by EYP on national security grounds. Initially, EYP had requested the extension of his surveillance until October 1, 2020, but abruptly terminated it on the day Koukakis filed a request to the Greek Authority for Communication Security and Privacy (ADAE) to know whether he was wiretapped.

On April 18, 2022, a government spokesperson, Yiannis Oikonomou, denied any connection between the government and Predator and attributed Koukakis's surveillance to private individuals. The spokesperson announced that the National Transparency Authority (EAD), which was established by the present government to combat corruption without specific competence for investigating surveillance and was led at the time by a former associate of Prime Minister Mitsotakis, would investigate the matter, despite the fact that competent for this investigation were two constitutionally established independent authorities (Authority for Communication Security and Privacy and Data Protection Authority).

EAD, not constitutionally established, later concluded that the security authorities had committed nothing wrong. However, the authority failed to examine the bank accounts of companies directly or indirectly linked to the case, some of which appear to have been linked to the security services. The conclusions of EAD would be later called into question by media revelations of massive surveillance cases by EYP and Predator, as well as the independent investigations of ADAE and DPA, which confirmed the illegal use of Predator against targets in Greeks and surveillance of EYP against politicians and high-ranking officers of the Greek Armed Forces.

On May 19, 2022, a report by Google's Threat Analysis Group, revealed that Predator has been used against targets in Greece with the most likely customers being government-sponsored entities.

Predator's presence in Greece prompted the Data Protection Authority (DPA) to start its own investigation. In July 2023 the DPA said it had identified at least 92 Greek phone numbers targeted by Predator spyware. According to constitutional law experts such as Evangelos Venizelos, who is also a former minister for the socialist party PASOK, and Xenofon Contiades, such targeting (both by EYP and Predator), which included surveillance attempts against members of the government, opposition politicians, journalists and businesspeople, is illegal under Greek law.

On July 26, 2022, opposition leader and MEP Nikos Androulakis reported to the Greek authorities an attempted Predator attack on his phone, revealed by the digital security service of the European Parliament. On August 5, after an inspection by ADAE to Androulakis's communications provider, it was revealed that he had been surveilled by EYP. The surveillance started in September 2021 and lasted for three months. A year later, on July 26, 2023, Androulakis stated in a parliamentary meeting that, according to the APD findings, he had also been targeted with Predator spyware by EYP on three occasions in 2021 on September 16 and 21 and October 20, while he was running for president of PASOK.

Media revelations about Androulakis's surveillance and connections between figures in the Greek government and Predator led to two key resignations in August 2022: ,the head of EYP, Panagiotis Kontoleon, and the secretary general and nephew of the prime minister, Grigoris Dimitriadis, who was politically responsible for EYP. Prime Minister Kyriakos Mitsotakis said he was unaware of Androulakis's surveillance by EYP and that it was "legal" but "politically unacceptable".

In November 2022, the newspaper Documento published three lists of persons either targeted or surveilled by Predator, including Meta's former cybersecurity policy manager Artemis Seaford, who is a U.S. citizen, and Euractiv journalist Spyros Sideris. The New York Times later revealed that Seaford was wiretapped by EYP from August 2021 and several months into 2022, and according to CitizenLab, her phone was infected with Predator for at least two months from September 2021.

The Predator lists contained journalists Antonis Delatolas, publisher of newspaper To Pontiki; the TV presenters Eva Antonopoulou and Maria Sarafoglou, Nana Palaitsaki and Menios Fourthiotis; CEO of TV Channel Star Panos Kyriakopoylos; and newspaper directors Alexis Papachelas of Kathimerini, Yiannis Kourtakis of Parapolitika, Stefanos Chios of Makeleio, and Petros Kousoulos of Mpam. The list also included people at state positions, such as Antonis Samaras (former Prime Minister), Michalis Chrysochoidis (Minister of Citizen Protection), Nikos Dendias (Minister of Foreign Affairs), Adonis Georgiadis (Minister of Development and Investment), Vassilis Kikilias (former Minister of Health), and Olga Kefalogianni (former Minister of Tourism).

On December 16, 2022, Euractiv revealed that MEP Giorgos Kyrtsos and journalist Tasos Teloglou had also been surveilled by EYP. Further reports in October and November 2022 revealed that journalists Tasos Telloglou and Eliza Triantafyllou of Inside Story, Thodoris Chondrogiannos and Nikolas Leontopoulos of Reporters United, as well as the freelance journalist Thanasis Koukakis were surveilled by the security services with a system of antennas tracking their position and the position of their sources. It was also revealed that they were monitored by police who followed them physically while investigating the Predatorgate scandal.

In December 2022, ADAE announced the formation of a special team investigating potential wiretaps by EYP. On 6 May 2023 it was revealed that the Greek Ministry of Foreign Affairs had granted two licences to Intellexa, the company selling Predator, for the export of spyware equipment to Madagascar and Sudan. The latter was conducted with the involvement of Krikel, the Greek state's frequent supplier of communications and surveillance equipment and its shareholder Yiannis Lavranos, Dimitriadis's best man[1].

In October, the cross-border investigation Predator Files, coordinated by the European Investigative Collaborations network, reported that Nexa, a company based in France and with ties to Intellexa, had stored surveillance equipment in Greece. A former employee of Cytrox, the North Macedonia-based company that developed Predator, told the investigation that there was a training centre for agents in the use of Predator in Athens.

On November 3, the Predator Files revealed that Grigoris Dimitriadis's mobile phone number had been used to send messages with a link infected with illegal Predator spyware to 11 targets in Greece. At the time the messages were sent, Dimitriadis was serving in the prime minister's office and oversaw the EYP. Dimitriadis has denied any wrongdoing and any involvement in the case.

Part II: Legal remedies

Some of the aforementioned surveillance victims have taken judicial action. The similarities of these reported cases have resulted in the formation of a joint case file of 12 incidents which is under investigation.

In February 2022, journalist Stavros Malichudis and his colleagues at Solomon filed a lawsuit before Greece's Supreme Court for violation of their constitutional rights. In April 2022 the Prosecutors' Office of Athens opened a preliminary investigation into Koukakis's surveillance by both Predator and by EYP. Later that year, Thanasis Koukakis filed a lawsuit challenging his surveillance with Predator and another against Intellexa's directors Felix Bitzios, Tal Dilian, and Sara Hamou. The case file also contained the lawsuit before the Supreme Court of Nikos Androulakis for the attempted targeting of his phone with Predator ín July 2022.

Two more cases have joined the same case file: the findings of the Financial Crime Prosecutor's investigation and a file from the Prosecutors' Office of the Supreme Court containing publications on the surveillance of ministers, politicians, journalists and businessmen by Predator.

Journalist Spyros Sideris has also taken legal action after his name appeared in Documeto's list, while both Koukakis and Androulakis filed complaints to the European Court of Human Rights in 2022. All these cases are pending.

Part III: Lack of accountability

According to Greek law, the competent authority for the protection of privacy from possible illegal surveillance is the independent Authority for Communication Security and Privacy (ADAE), established by the Constitution. However, according to reports, the Greek government has attempted to stifle its efforts to shed light on the Predatorgate scandal.

On 10 March 2021, ADAE, having confirmed the surveillance of Thanasis Koukakis after a check with the journalist's telecommunications provider, submitted an official request to the prosecutor of EYP, Vasiliki Vlachou. With this request, ADAE wanted to confirm that the conditions of the law were fulfilled in order for it to inform Koukakis about his surveillance by EYP. The two conditions for such official notification were firstly, that the surveillance had been terminated and, secondly, that the purpose for which the surveillance was carried out (national security) was not compromised. However,

1 Dimitradis became the godfather to Lavranos's second child on May 28, 2022

later that month the Greek government changed the law (Law 2225/1994) to prohibit ADAE – under any condition – from informing affected citizens about surveillance of them for reasons of national security. Given the timing, it has been widely assumed in Greece that the amendment was passed to keep information about Koukakis's surveillance quiet.

Right after the amendment, three active members of ADAE, including president Christos Rammos (a former chief judge at the country's highest administrative court) and lawyer Aikaterini Papanikolaou, argued in an op-ed that the new provision may be in breach of the Greek Constitution, the European Convention on Human Rights, and the Charter of Fundamental Rights of the European Union. In April 2022, the Greek government bypassed the two competent authorities for the protection of privacy and data (ADAE and DPA) to publicly entrust the investigation on Koukakis's surveillance to the EAD, which was then headed by Angelos Binis, a former associate of Prime Minister Mitsotakis. The EAD was established in 2019 by the present government to prevent and combat acts of corruption, but has no competence to investigate issues of surveillance.

Dead-end parliamentary inquiry

In August 2022, Androulakis requested the formation of a parliamentary inquiry committee to investigate his wiretapping by EYP. During a hearing on September 20, 2022, the president of ADAE revealed that EYP's surveillance files of Androulakis and Koukakis were destroyed by order of the former director of EYP, Panagiotis Kontoleon. The destruction of evidence took place on July 29, 2022, the day Androulakis filed a complaint about his surveillance to the Prosecutor's Office of the Supreme Court. Rammos, the president of the ADAE, also highlighted that the prosecutor of EYP and its new head "refused to cooperate" in ADAE's investigation.

The hearings of the inquiry committee were conducted between September 7, 2022 and October 13, 2022, with the government majority refusing to call witnesses directly related to the case, including Prime Minister Kyriakos Mitsotakis and his nephew Grigoris Dimitriadis, as well as Intellexa's Tal Dilian, Sara Hamou, and Felix Bitzios, Krikel's Yiannis Lavranos, prosecutor of EYP Vasiliki Vlachou, as well as surveilled journalists.

Kontoleon and Dimitriadis were summoned in August 2022 in a parliamentary hearing by the Institutions and Transparency Committee, the body of the Greek parliament overseeing EYP. According to reports, both of them invoked confidentiality and avoided answering questions on Androulakis' surveillance.

Pressure on ADAE

The story took another twist when, in August 2022, the Supreme Court Prosecutor Isidoros Doyakos (appointed by the Greek government) announced a judicial investigation into several journalists and their sources for possible leak of classified information (on 15th April 2022 Reporters United had published classified information proving Thanasis Koukakis as surveilled by EYP). In October 2023, in the context of this judicial investigation, the Greek judiciary summoned two members of ADAE as suspects for the offence of leaking sensitive state secrets to the journalist Thanasis Koukakis, despite the fact that Koukakis himself had disclosed that he became aware of his surveillance by EYP when notified by the journalists of the investigative media outlet Reporters United, which broke the story that the journalist was under surveillance by EYP. This move has been criticized as an attempt to intimidate the members of ADAE because they are investigating the case within the bounds of the competences of the independent authority. On February 20, 2024, the Athens Prosecutor's Office closed the case against the members of ADAE, as there was "no indication of any criminal act" and, according to the competent prosecutor, Thanasis Koukakis was informed of his surveillance by EYP through the journalistic investigation of Reporters United.

In January 2023, Doyakos issued a legal opinion which asserted that ADAE, under Law 5002/2022 passed in December 2022, does not have the institutional competence to manage requests from citizens who ask to be informed if they have been surveilled by the state security services, nor can they address telephone providers over this issue. Doyakos issued this opinion following checks made by ADAE with telecommunications providers which revealed that the National Intelligence Service was monitoring six senior officials including serving ministers and senior armed forces personnel.

However, 15 legal experts expressed their opposition to the Supreme Court Prosecutor's opinion, underscoring that the supervisory power of the independent authority is conferred on it directly by the Constitution (Article 19(2)) and its scope cannot be limited in any way by the legislature. ADAE, therefore, according to these legal experts, has not only the ability but also the constitutional obligation to ensure that state agencies are not abusing their power.

The government also attacked the president of ADAE, Christos Rammos. On December 17 2022, the Minister of State, George Gerapetritis issued a broadside against ADAE after it revealed the surveillance of Kyrtsos and Telloglou by EYP through their telecommunications provider. In November 2023, Prime Minister Mitsotakis accused Rammos of having an "agenda". In January 2023, the government spokesperson publicly accused him of "activism" for the sake of "sensationalism". The same month, Development Minister Adonis

Georgiadis said that "Rammos has touched the boundaries of treason". Rammos denounced Prime Minister Mitsotakis's verbal attack launched against him. "These are not the right conditions for the head of an independent authority in a European country to carry out his duties", he said.

In September 2023, some members of ADAE were quickly replaced by the Conference of Presidents of the Parliament (a parliamentary body controlled by the government), after which ADAE did not impose a planned fine on the EYP. The government said that the term of office of some ADAE members had expired (according to Greek law, until they are replaced, members retain their position even after their term of office has expired). However, it is widely speculated in Greece that the replacement was an attempt to avoid having ADAE fine the EYP, which is under the direct competence of the Prime Minister. The fine, amounting to 100,000 euros, was to be imposed because the EYP destroyed evidence from the files it kept on the surveillance of journalist Thanasis Koukakis and the leader of the opposition party PASOK, Nikos Androulakis. The destruction of this evidence created difficulties in clarifying details of the surveillance scandal for both ADAE and other state and judicial authorities.

After these events, MEP Sophie in 't Veld, rapporteur of the EU's Committee of Inquiry to investigate the use of the Pegasus and equivalent surveillance spyware (PEGA), sent a letter to the European Commissioner for Justice Didier Reynders stating that, "Events this week seem to confirm the concerns over political interference and possible obstruction of the inquiry". Opposition parties PASOK and Syriza lodged an objection to the authority's composition change for being in violation of the constitutionally required majority of 3/5 of the Parliament members. On October 23, the Prosecutor of the Supreme Court, Georgia Adilini, ordered the transfer of the Predatorgate judicial investigation from the first-instance prosecutor's office to the Supreme Court, at a time when the first-instance prosecutor was investigating connections and common surveillance targets between the EYP and the illegal Predator spyware. This judicial decision was met with criticism, as it's expected to bring about yet more delays in the investigation.

The result of all of these developments is that, so far, nobody has been summoned by the Greek judicial authorities or has been prosecuted for the use of the Predator spyware. Instead, ironically, the only criminal prosecution that has emerged from the scandal is against the members of ADAE, while journalists investigating the surveillance are facing civil lawsuits and SLAPPs. The upshot is that there is currently a complete lack of accountability for one of the most serious attacks on press freedom in Greece in recent years. The "Greek Watergate" is a worrying example of how state authorities and government entities tasked with unearthing illegal surveillance of journalists have played a part in keeping such information hidden. The implications of this scandal and the impunity with which it was conducted risk long-lasting negative effect on the freedom of the press and Greek democracy.

Concerns around the compatibility of new legislation on the privacy of communications with the Constitution and the ECHR

In December 2022 the government passed the surveillance reform bill seen as an effort to address the scandal. However, according to experts, the law has resulted in mainly cosmetic changes.

Concretely, on December 9, 2022, the Greek government passed Law No. 5002/2022, introducing changes to the procedure for surveillance with the stated aim of more effectively protecting privacy, imposing a stricter criminal penalty for the use of prohibited Predator-type spyware, and reforming EYP to better fulfill its mission of protecting national security.

However, legal bodies and experts have expressed serious concerns about the compatibility of the new regulations with both the Greek Constitution and privacy protections contained in international treaties such as the ECHR and the EU Charter of Fundamental Rights.

ADAE highlighted several concerns. Firstly, it expressed concern that surveillance would still be carried out based on an order from the prosecutor of the intelligence services, i.e. the prosecutor who operates organically within EYP. This, according to ADAE, results in the prosecutor's being integrated into the culture and mentality of the intelligence services, creating questions around the office's independence.

ADAE suggested that the power to issue surveillance orders should be entrusted to a three-member judicial council (and not necessarily prosecutors) and cease to be exercised by a single prosecutorial body. ADAE also pointed out that the new framework still does not demand the inclusion of important information (such as the reasons for the surveillance and the name of the citizen being surveilled) in the prosecutor's order. This is problematic, since, as the independent authority notes, the justification of all decisions of state bodies, in particular those which are unfavourable to the persons concerned, is an inherent element of the principles of the rule of law and of the constitution of a liberal parliamentary democracy.

Elisavet Simeonidou-Kastanidou, a professor of criminal law at Aristotle University of Thessaloniki, referred to the same issue in detail, noting that within 24 hours after receiving a request for surveillance, the prosecutor "must issue an order accepting or rejecting the request. As in the previous law, it is not stated that the order must be reasoned." She commented: "[S]uch a burdensome state act cannot be unjustified. The provision must in any event describe the elements which show that the lifting of confidentiality is justified and in accordance with the principle of proportionality."

According to ADAE, another problematic provision of the new law is that the government, for the first time in 18 years, removed from the independent authority the power to inform the affected citizens about the lifting of the confidentiality of their communications for reasons of national security. As already mentioned, in March 2021 the Greek government changed the law to prohibit ADAE under any condition from informing affected citizens about surveillance of them for reasons of national security. The compatibility of this legislation with the Constitution and the ECHR has also been questioned.

The new legislation provides that the competence of informing citizens about the lifting of their privacy for national security reasons is no longer assigned to ADAE, but to a three-member body consisting of the chief of EYP, the prosecutor of EYP and the president of ADAE.

Here, ADAE notes that under Article 19(2) of the Constitution, the final guarantor of the legality of the whole procedure is ADAE. Moreover, according to the case law of the European Court of Human Rights, the relevant legislation should provide that subjects of surveillance should have a right to be informed – even under specific conditions, e.g. after the end of the surveillance and provided that the purpose for which the surveillance was ordered is no longer at stake – by an independent authority with guarantees of independence. In this case, the three-member body foreseen by the law lacks the necessary guarantees of independence.

In its note to the Parliament on the Law. 5002/2022, the National Commission for Human Rights (NCHR) stated that, "the proposed regulations introduce critical changes that are in sharp contrast to human rights and implicitly confirm the findings of the latest annual report of the European Union's Fundamental Rights Agency (FRA) which notes that 'effective safeguards to ensure that data and technology are used in a manner that complies with human rights are still lacking.'"

Finally, a mission by international media freedom groups in September 2023 also expressed concern about the surveillance reform bill and called for new legislation to:

→ Oblige competent prosecutors to provide a justification for any surveillance undertaking in the interests of national security that can allow for proper scrutiny of its legality and proportionality

→ Set up independent and effective judicial oversight

→ Allow for effective access to information by persons targeted with surveillance by removing the arbitrary three-year time limit and reinstating the sole responsibility of the Hellenic Authority for Communication Security and Privacy (ADAE),

→ And establish specific safeguards for journalists

The mission further called on the Greek courts to provide justice to the victims of the spyware scandal in a swift, independent and transparent manner, using the evidence provided by the journalists' investigations and treating the specific cases as a felony and not just a misdemeanor which expires after five years.

Pegasus surveillance in Hungary

By Szabolcs Panyi, investigative editor at VSQUARE and investigative journalist at Direkt36 in Hungary

Confirmed Hungarian targets and the use of Pegasus against them

Two and a half years ago, in July 2021, the international "Pegasus Project" investigation revealed how journalists, media company owners, and other critics of Hungarian Prime Minister Viktor Orbán's populist right-wing government were targeted with NSO Group's military-grade Pegasus spyware. Hungarian media representatives were among the nearly 200 journalists worldwide, from Mexico to France to India, who fell victim to abusive spyware surveillance.

The investigation was based on a leaked list of phone numbers, which were selected as spyware targets by NSO Group's clients. Among the 50,000 phone numbers on the list, more than 350 Hungarian numbers were identified, over a dozen of which belonged to Hungarian journalists, reporters, media company owners, and their close circles:

→ Reporter **Dávid Dercsényi**, who worked for independent news site HVG.hu at the time covering mostly daily news, but occasionally sensitive stories as well, was targeted through three phone numbers, including one used by his ex-wife.

→ Crime reporter and investigative journalist **Brigitta Csikász**, who was working for non-profit investigative outlet Atlatszo.hu on multiple corruption-related stories, including a series on EU fraud.

→ Investigative journalists **Szabolcs Panyi** (the author of this case study) and **András Szabó**, working for local "Pegasus Project" partner Direkt36.hu, a non-profit investigative journalism outlet which helped uncover the Pegasus surveillance in Hungary. They mostly covered Russia and Russian financing-related national security and corruption stories.

→ A photojournalist, who asked to remain anonymous, worked as a fixer for a U.S.-based outlet at the time. NSO Group doesn't allow its customers to target American (+1) phone numbers, so targeting an American journalist's local fixer could be a way to overcome this hurdle. The journalist and the fixer were working on the same Russia-related topic as Direkt36's Panyi and Szabó. Moreover, the journalist and Panyi met in person during the surveillance.

→ After the initial revelations, all based on the leaked database, which only contained Hungarian phone numbers from early 2018 to mid-2019, **Dániel Németh**, an investigative photoreporter who regularly uncovers the lavish lifestyle of Orbán's entourage, was also identified as a victim of Pegasus surveillance. He was spied on in 2021 while documenting the pro-Orbán elite's vacationing on luxury yachts for Partizán, a popular independent Youtube channel.

→ Crime reporter-turned-pilot **György Pető**, who helped various journalists with their investigations into the luxury private jet trips of Hungarian government politicians and their friends. He was very likely included in the list for being a source to journalists.

→ **Zoltán Varga**, owner of Central Media Group, and six of his friends. Varga owns Hungary's largest independent news site, 24.hu, whose editorial team is led by former journalists of Népszabadság, which was Hungary's largest leftwing newspaper before being bought up and closed down by Orbán proxies in 2016. Varga himself was also a target of numerous blackmail and intimidation attempts by government proxies, trying to force him to sell his media portfolio.

→ Phone numbers of **Ádám Simicska** and **Ajtony Csaba Nagy**, son and lawyer, respectively, of media tycoon and former close Orbán-ally Lajos Simicska. At the time, the Simicska's media had become fiercely critical of Orbán's government. Simicska outlets such as Hír TV news channel and Magyar Nemzet daily were later taken over by Orbán proxies too.

→ **Zoltán Páva**, publisher of an anti-Orbán, openly pro-opposition leftwing news site, ezalenyeg.hu, also had his phone hacked with Pegasus in 2021. His surveillance was uncovered after the initial investigation.

In the case of reporters Csikász, Németh, Panyi, and Szabó, as well as media company owner Páva, the technical forensic analyses of their iPhones found clear traces of Pegasus infection. The forensic analyses were carried out by Amnesty International's Tech Lab as well as Citizen Lab, corroborating each other's findings. Further analyses of Zoltán Varga's friends' phones also found traces of attempted hacking in one case and successful hacking in another case. Similar in-depth analysis was unable to be carried out in other cases. This mostly was due either the victims having already discarded their phones or them owning Android devices, which are much harder to investigate forensically.

Later, Direkt36 revealed that Hungarian broker company Communication Technologies Ltd – a firm linked to the inner circle of Viktor Orbán's minister of interior – was behind the acquisition of the Pegasus spyware. Citizen Lab also found technical traces of another Israeli spyware, Candiru. Company registry data also shows that a third spyware, Predator, has ties to Hungary through the Intellexa group's locally registered company, Cytrox.

Direkt36.hu also reported that a tool by Israeli surveillance technology developer Picsix has also been used in Hungary recently, at least for testing purposes – Israeli representatives wiretapped random Hungarian phone conversations during a demo showcase. These revelations suggest that the use of Pegasus in Hungary may only be just the tip of the iceberg.

Aftermath, legal framework, and botched investigations

Hungary's government initially denied allegations of using spyware against its critics, then tried to dodge all related questions for months. Meanwhile, government-controlled media started a smear campaign against journalists involved in the "Pegasus Project", trying to discredit them as agents of Hungarian-American billionaire George Soros as well as U.S. intelligence services, portraying them as threats to national security.

At the same time, the Hungarian Parliament's national security committee was unable to scrutinize the surveillance scandal as MPs of the governing party boycotted the hearings. Later, when the committee could finally convene, its minutes got classified until 2050, preventing opposition MPs from informing the public on what was revealed. Civilian oversight of national security services in Hungary is non-existent, and this committee is the only body that has at least limited powers to question Hungarian intelligence services.

In November 2021, however, a senior lawmaker from Hungary's governing party eventually admitted in public that the Hungarian government had indeed used the Pegasus spyware. Fidesz MP Lajos Kósa claimed that the „Pegasus software (sic) is a simple piece of software, there are many similar ones used in national security work by authorized bodies, I see nothing wrong with that." Likewise, the Orbán government argued that all surveillance had been completely lawful and justified. Opposition MPs were told by Interior Minister Sándor Pintér at a closed-door committee hearing that anyone can be surveilled, regardless of their occupation, if they are suspected of being involved in organized crime, terrorism, or espionage activities.

The "Pegasus Project" investigation in Hungary not only revealed dozens of cases of actual surveillance of the government's critics, but also highlighted two serious problems with the Hungarian legal framework. "In most countries, there are either strict rules about who and when the state can monitor, or there is strong, not only political, but also legal control over how various agencies carry out their work. None of these are present in Hungary", said Máté Dániel Szabó, director of programs at the Hungarian Civil Liberties Union (HCLU).

According to Hungarian law, there are two different procedures for authorities to acquire a permit or warrant for surveillance. The first procedure involves criminal investigations, typically carried out by the police and other law enforcement, where permits are issued by a judge. In such cases, surveillance is typically used for collecting evidence for pressing subsequent charges. However, there is a second procedure when authorities request a surveillance permit justified on national security grounds. In such cases, typically handled by national security and intelligence agencies, permits are approved by a member of the Hungarian government, the minister of justice, specifically.

Already in 2016, the European Court of Human Rights (ECtHR) in Strasbourg ruled that the Hungarian regulation of surveillance is incompatible with European human rights standards, and the Hungarian government must obtain judicial permits for all surveillance activities. Despite the ruling, the Hungarian government as well as the Hungarian Parliament, where Viktor Orbán's Fidesz party has a supermajority, has failed to act and reform laws regulating surveillance. Since Hungary has been using the Pegasus spyware since February 2018, this means that underlying surveillance permits signed by the Ministry of Justice were all issued contrary to the ECtHR's ruling.

Hungary's Pegasus surveillance was investigated by two ostensibly independent bodies, the National Authority for Data Protection and Freedom of Information (NAIH) and the prosecutor's office. NAIH, led by Orbán government appointee Attila Péterfalvi, completely exonerated the Hungarian government in January 2022, stating that all surveillance was carried out according to the law. Details, however, are unknown as NAIH's full report is classified until 2051. At a press conference, Péterfalvy at least revealed that, in cases reported in the media – i.e. the surveillance of journalists, media company owners, lawyers etc – the justification for surveillance was "risk to national security".

But while it cleared the government's surveillance, NAIH's investigation did identify one suspected act of wrongdoing: namely the "Pegasus Project", on the grounds that the journalists obtained the leaked database of potential Pegasus targets. According to NAIH, the leak could have been the result of an unlawful data processing operation, or even espionage. NAIH therefore filed a criminal complaint with the Hungarian police, which investigated the complaint until March 2023 when they finally closed the case "in the absence of criminal offenses."

In spring 2022, NAIH even launched a separate investigation for alleged "illegal data management" against "Pegasus Project" member and Pegasus spyware target Szabolcs Panyi (the author of this analysis) following a complaint by an

intelligence officer working for the Special Service for National Security (SSNS), the agency operating spyware tools such as Pegasus. The officer complained because his personal data was obtained by the journalist as Panyi had reported for Direkt36.hu that he identified the officer's phone number in the leaked target list – most probably because the officer tested the spyware on his own number and device. After four months of investigation, NAIH closed the case and found no wrongdoing.

In September 2022, the ECHR's ruling in the case of Hüttl v. Hungary – on the surveillance of a human rights lawyer by Hungarian authorities – essentially found that there is no independent external oversight of surveillance operations in Hungary, and that the NAIH is unable to fulfill this responsibility. Reacting to NAIH's investigation, HCLU also highlighted that the authority "fails to perform its essential functions and is unable to take action against unlawful surveillance", and it didn't even investigate if "the whole system of surveillance infringes fundamental rights."

Following multiple criminal complaints, including from opposition politicians, the Hungarian prosecutor's office also opened an investigation into alleged unlawful surveillance, which was dropped "in absence of crime" in June 2022. The prosecutors confirmed that multiple victims of surveillance reported by the "Pegasus Project" were indeed spied on, but lawfully, it claimed, also adding that they became targets of surveillance "not necessarily as criminal suspects". This is underscored by the fact that, in every single reported Hungarian case involving the surveillance of journalists, no subsequent criminal proceedings were launched against them.

Such use of Pegasus targeting Hungarian journalists is also not in line with the spyware's original purpose. According to Pegasus manufacturer NSO Group's claims, their technology is only used against the most serious criminals, including terrorists and drug dealers. In Israel, NSO Group Shalev Hulio vowed to launch an investigation during an interview with the Israeli Military Radio in July 2021 after hearing the case of Pegasus surveillance of journalists in Hungary. However, it's unknown what came out of this as NSO never talks about its clients and possible termination of contracts.

Seeing that official investigations have gone nowhere, multiple Hungarian Pegasus victims, the majority of them journalists, have launched legal action with HCLU's help both in Hungary and abroad. Israeli human rights lawyer Eitay Mack also filed a complaint with the Israeli attorney general on behalf of three Hungarian Pegasus victims as the Israeli spyware technology was sold to a foreign government with a known track record of lax surveillance regulations and cracking down on media freedom. None of these proceedings have achieved anything so far, proving that it is practically impossible for Hungarian victims of surveillance to obtain justice. Moreover, in Israel, an internal investigation revealed in June 2023 that the attorney general's office delayed processing the Hungarian victims' case.

EU's role in putting an end to unregulated surveillance in Hungary

Since the first Pegasus surveillance revelations in Hungary, the only meaningful investigations were carried out at a European Union level – for example, by the European Parliament's PEGA Committee or by the Parliamentary Assembly of the Council of Europe (COE), both condemning the Hungarian government for its abusive surveillance practices.
The PEGA Committee's investigation – with Sophie in 't Veld as rapporteur – concluded that "political control over the use of surveillance in Hungary is complete and total. The Orbán-led Fidesz regime has made it so that they can target lawyers, journalists, political opponents and civil society organizations with ease and without fear of recourse." Following the PEGA investigation, the European Parliament (EP), with an overwhelming majority, adopted a resolution in outlining the reforms necessary to curb spyware abuse both in Hungary and other countries.

The COE Assembly's September 2023 report – with Pieter Omtzigt as rapporteur – reached similar conclusions as the EP, making recommendations to the Hungarian government such as to "conduct effective, independent and prompt investigations on all confirmed and alleged cases of abuse of spyware and provide sufficient redress to targeted victims in cases of unlawful surveillance; refrain from using blanket secrecy rules to deny oversight mechanisms' and targeted persons' access to information on the use of spyware."

However, none of these independent investigations, their recommendations, or conclusions are legally binding. Hungary's government and its representatives flat-out refused to cooperate with these inquiries. Then-Minister of Justice Judit Varga, for example, ignored the PEGA Committee's delegation during its visit to Budapest in February 2023. Neither the EP/PEGA, nor the COE probes resulted in any positive change in Hungary, and the situation for Hungarian journalists and civil society is grimmer than ever before.

In December 2023, the Hungarian parliament passed the so-called "Sovereignty Protection Act", creating a new authority which could investigate without court oversight the "foreign funding" of the opposition, NGOs, and media. Independent Hungarian media outlets issued a joint statement, warning that the new law is "capable of severely restricting the freedom of the press". This new legislation, which follows years of government smear campaigns against NGOs and independent media, labeling them as foreign agents and threats to Hungarian national security, creates a pretext for all future surveillance against them.

IPI analysis

Under these circumstances, the EMFA was the only hope to put an end to current surveillance practices in Hungary. As this analysis has shown, it has been proven multiple times that Viktor Orbán's government has specifically used national security justifications for targeting Hungarian investigative journalists who scrutinize corruption and abuses of power. Yet despite its good intentions, the EMFA is unlikely to be robust enough to prevent further abuse of spyware by the Hungarian government. The EMFA's requirement that any surveillance operation must receive prior authorisation by a "judicial authority or an independent and impartial decision-making authority" may restrict the powers of ministers to order surveillance, but the Fidesz government has a long established record of using theoretically independent bodies that are effectively captured by party loyalists. Concerns remain about judicial independence, despite some reforms that have been welcomed by the European Commission. It is entirely unclear whether the removal of the explicit national security exemption from Article 4 will be enough to prevent Hungary from continuing to use vague references to "national security" as a justification for surveillance and withholding information about it.

Spyware cases across the EU

Documented cases

While Hungary and Greece present the most problematic examples of the mass surveillance of journalists in the EU in recent years, there are multiple other examples across Europe of journalists' private communications being unjustly monitored using different spyware tools, with damaging effects on media freedom and privacy. While in Hungary the state has admitted to carrying out the surveillance, and in Greece there is credible evidence of coordinated surveillance of journalists using legal wiretapping and then illegal spyware, indicating the involvement of intelligence services, in most other cases in Europe journalists have been surveilled by foreign authorities.

In 2023 it was revealed that Pegasus spyware had been used to hack into the telephone of Galina Timchenko, head of the independent Russian-language news outlet Meduza while she was in Berlin. According to a report published by NGO Access Now, Timchenko's iPhone was infected with the zero-click spyware in February 2023. The attack took place on February 10, when Timchenko was traveling in Germany, just two weeks after Russian authorities designated Meduza as an "undesirable organization", effectively banning the outlet's operations in Russia. During the hacking, hackers had real-time access to her phone's screen, to the device's camera and microphone, and other files, applications and photos. Based on the timing of the hack, Timchenko has speculated that the spyware could have been used to surveil a closed meeting of independent Russian journalists in Berlin, which took place on February 11, 2023. According to Access Now, it was the first documented case of Pegasus surveillance of a Russian journalist. The investigation reported that the attack could have come from the Russian Federation, one of its allies, or an EU state. Timchenko is based in Latvia along with other Meduza staff. Investigations continue but so far so authority or actor has yet been held accountable.

In France, revelations surfaced in 2021 that multiple journalists working for French media companies were allegedly targeted by Moroccan security services using Pegasus spyware. These reportedly included journalists and media workers at Le Monde, Agence France-Presse and FRANCE 24. Mediapart revealed that the phones of its founder and director, **Edwy Plenel**, was among those targeted in July and August 2019. A colleague of Plenel, Lenaïg Bredoux, was also targeted using the same technology. Mediapart filed a legal complaint to French authorities. The revelations came after the Pegasus Project was published. Morocco denied the claims and said it "never acquired computer software to infiltrate communication devices". Like the cases above, no one has been held accountable.

In 2022, revelations surfaced about the use of Pegasus by Spanish authorities. In April it was revealed that at least four Catalan journalists were amongst those to have their smartphones targeted or infected with the spyware between 2017 and 2020, after Catalonia's failed independence bid. According to Citizen Lab, the journalists targeted included Meritxell Bonet, the spouse of an activist who chaired the Catalan NGO Òmnium. Also targeted were journalist and historian Marcel Mauri, who later became vice-president of Òmnium, as well as journalist and former Catalonia MP Albano Dante Fachin, and journalist Marcela Topor, wife of former president of Catalonia Carles Puigdemont. All those targeted had links to the Catalonian independence movement or figures within it. Separately, Spanish journalist **Ignacio Cembrero**, a correspondent specializing in coverage of the Maghreb, has been identified as a potential target for surveillance using Pegasus and has alleged Moroccan authorities were responsible.

According to research by Access Now, Pegasus is known to have been used in at least 14 countries and 22 state institutions within the European Union. While many of these countries' use of spyware has not proven to have been directed at journalists, the widespread use of spyware and the risk of abuse in countries without sufficient safeguards and weak rule of law is clearly high. Other EU countries have been shown meanwhile to have granted export licences for Pegasus. Reports by NSO previously suggested that EU member states Cyprus and Bulgaria granted export licenses for NSO's technology. While numerous revelations have come to light in recent years, the failure to control the acquisition, trade and use of such intrusive technology inside the EU means that the number of member states to have bought Pegasus or other similar cyber-surveillance technology remains unknown. This opacity poses significant threats to journalistic sources, privacy and safety, undermines media freedom and constitutes a clear failure by the EU to close the gaps in its regulatory framework.

Conclusion

The surveillance of journalists, including using spyware technology, poses a fundamental threat to media freedom, the digital safety of journalists, and source protection within the European Union. The agreement on the European Media Freedom Act in December 2023 offers some further protections against the fast evolving threat to journalists and their sources. Those involved in pushing the deal over the line and ensuring the removal of explicit references to national security in exemptions deserve credit. Yet the full impact of the Article 4 provisions – as all other new rules in the EMFA – remains to be seen and effective implementation will be vital. Greece and Hungary offer the strongest examples of why strong enforcement will be needed. However, both countries have already demonstrated how overly broad and vague exemptions for national security have already been used to justify the otherwise unjustifiable surveillance of journalists.

In Greece, rather than those behind the illegal surveillance of journalists in 2021 and 2022 being identified and prosecuted, journalists who revealed the abuse of spyware tools have been hit with SLAPP lawsuits by powerful figures. While a new law in Greece prohibits the use of spyware, the export of such spyware technologies remains legal. In Hungary, meanwhile, no accountability has been achieved, with authorities instead targeting the journalists who exposed the surveillance scandal. Concerns persist that the same flimsy justifications provided by authorities will continue to be used in the future, without proper oversight. In both states, governments and, in some cases, captured institutions have obstructed accountability. In both, domestic legal remedies have not proven successful in achieving justice.

This complete lack of accountability is a major stain on press freedom in Europe and has been a central factor to the decline of media freedom in both states. While the EU's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA) helped shine a light on the abuses of spyware across the bloc, the majority of its recommendations have not been implemented. Likewise, while the EU's new dual-use mechanism encompassing cyber surveillance tools represented a positive development, it also offers states the ability to refuse to provide information to the EU Commission on the sale, trade, and use of spyware tools under national security grounds, offering further protections from scrutiny.

Ultimately, while the EMFA and Article 4 are welcome developments overall, uncertainty remains over the potential surveillance of journalists both in Greece and Hungary, and across the bloc. As spyware tools proliferate and more companies enter a fragmented spyware-for-hire market, concerns over the use of such tools against the press will likewise persist. Further developments are needed to continue the momentum provided by the PEGA Inquiry and support the provisions developed in Article 4 of the EMFA. In light of these conclusions, the report outlines a number of recommendations.

Recommendations

To EU Member State governments

→ The rules agreed under Article 4 of the EMFA represent the minimum standard to protect journalists from surveillance. Member states must adopt strong safeguards in national legislation to prevent the abuse of spyware.

→ National authorities must carry out prompt, thorough, and credible investigations into reports of the use of spyware against journalists. These investigations must result in holding those responsible for illegal surveillance to account.

→ Provide detailed information to the European Commission on the use, trade, and export of all types of advanced cyber surveillance technology in a timely manner, without withholding information based on national security exemptions

→ Refrain from all use of spyware unless national legislation is firmly in line with the human rights standards set by the European Court of Justice and European Court of Human Rights.

→ Repeal all export licenses for spyware and other advanced surveillance technology that is not in line with EU export control legislation

→ To the **Greek government**: Cease all efforts to obstruct the independent operations of the Hellenic Authority for Communication Security and Privacy (ADAE); and invite Europol to join the investigations of the Greek justice system into the illicit spying on journalists.

→ To the **Hungarian government**: End the state of impunity for the illicit use of spyware against journalists through an independent investigation that results in accountability for those responsible and in changes to relevant laws and regulations to prevent the abuse of spyware in the future. Ensure full compliance with European Court of Human Rights judgements on surveillance and cooperation with EU and other international investigation

To European institutions

→ Renew the mandate of the European Parliament's PEGA committee in order to monitor the implementation of the EMFA's rules under Article 4 and the implementation of its 2023 recommendations

→ Put a spotlight on cases of the surveillance of journalists within the European Commission's annual Rule of Law report and provide detailed recommendations about required reforms from Member State governments

→ Enforce strict implementation of the EU's dual-use regulations regarding the use, trade, and export of all forms of spyware technology and report on a bi-annual basis on developments

→ Bring forward a stand-alone regulation on the use of spyware