Lawyer-Client Confidentiality in a Digitalized Society

May 2023

LAWYERS FOR LAWYERS

Summary

The principle of legal professional privilege and confidentiality (LPPC) is clearly established in international, regional, and domestic legal regimes. The digital society has expanded the communications between clients and their lawyers from written exchanges and face-to-face offline communication to online mail contact/messaging and phone- and videocalls. These digital methods of communication offer many advantages but are also vulnerable to interception by third parties. Several instances of illegitimate surveillance and interference with digital communications of lawyers with their clients have been reported in recent years, including wiretapping and hacking of lawyers' phones through intrusive surveillance software. Additionally, problems posed by a lack of respect for LPPC during investigations by public prosecutors are discussed.

The aim of this report is to create awareness about the threats to LPPC in the digital age and to reiterate the importance of our commitment to protect this principle as part of protecting the rule of law. Our analysis of the current legal framework and case studies relating to LPPC show that the protection of LPPC requires our attention.

Table of contents

1. Introduction

The principles of legal professional privilege and legal professional confidentiality aim to protect the confidentiality of information shared between lawyers and their clients. The principle is recognized in several sources of international law, including in the Basic Principles on the Role of Lawyers.[1] It is also established in most domestic laws relating to the regulation of the legal profession.[2] However, the scope and definition of legal professional privilege and confidentiality is not harmonized worldwide. For the purpose of this report, we refer to legal professional privilege and confidentiality (**LPPC**).[3] Absence of LPPC can create a chilling effect for both lawyers and their clients and discourage potential clients from contacting a lawyer.[4] In addition, other human rights may be at risk if the LPPC is not ensured, including the principle of equality of arms and the right to an effective legal defense.

Despite the legal recognition of LPPC, Lawyers for Lawyers is concerned with regards to the adherence of that principle in the digital sphere. Phone, e-mail, and other digital means of communication, such as video calls have become indispensable means of communication for lawyers to stay in touch with their clients and colleagues. These digital methods of communication do not come without risk, as they are vulnerable to third party interception. In recent years, several incidents of phone tapping, and other digital infractions affecting LPPC have been reported worldwide. In the past years, human rights organizations and lawyers' associations have reported on the increasing prevalence of lawyers' communications with their clients being subject to wiretaps and surveillance.[5] Still, at the time of writing this report, problems with regards to LPPC persist worldwide and surveillance has only become more intrusive in methodology and impact due to the digitalization of society.

1 The UN Basic Principles on the Role of Lawyers provide a concise description of international norms relating to the key aspects of the right to independent counsel. The Basic Principles were unanimously adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in Havana, Cuba on 7 September 1990. Subsequently, the UN General Assembly "welcomed" the Basic Principles in their 'Human rights in the administration of justice' resolution, which was adopted without a vote on 18 December 1990 in both the session of the Third Committee and the plenary session of the General Assembly.

2 Law Society of England and Wales, 'UN Basic Principles on the Role of Lawyers: Independence of the Legal Profession and Lawyer/Client rights worldwide', https://www.lawsociety.org.uk/topics/research/un-basic-principles-on-the-role-of-lawyers, February 2022, p. 53.

3 Throughout this report we will use the term legal professional privilege and confidentiality (LPPC), as this most comprehensively covers the scope of the principle as explained in section 2.1 of this report.

4 ECtHR, S. v. Switzerland, para. 48, 117-118. See also: ECtHR, Michaud v. France (12323/11, 2012), para. 118. ECtHR, R.E. v. United Kingdom (62498/11, 2015), para. 131.

5 In recent years, a decline in rule of law standards around the world has been observed. Those working on human rights and other politically sensitive topics, including lawyers, are faced with suspicion and hostility from governmental authorities and operate in an increasingly shrinking civic space. The exploitation of the vulnerabilities of digital communication methods for surveillance purposes is therefore very concerning but can be seen as a symptom of a wider declining rule of law trend.

The aim of this report is not to redo earlier, very important work by other organizations that has been done on the principle of LPPC. Through this report we show that LPPC is still under threat and give examples of ways in which LPPC can be breached in a digital society. In particular, we provide accounts of lawyers who have been subject to digital surveillance in recent years and the impact that this surveillance has had on them, their clients and their work.

2. Legal framework in a nutshell

2.1 Legal professional privilege and confidentiality: not one definition

A vast majority of legal systems worldwide have recognized the importance of confidential communication between a lawyer and their client. Various terms and definitions are used to describe this principle, such as legal (professional) secrecy, legal (professional) privilege, attorney-client confidentiality, etc.

As mentioned above, the definition is far from uniform, varying among jurisdictions. Examples of different approaches in a nutshell are:

- **Protection of lawyer and / or client.** Different approaches exist relating to which party "owns" the privilege and who has the right to waive it.
- **The definition of a lawyer.** Different approaches exist with respect to which professionals are qualified as a "lawyer". For example, not all jurisdictions provide the same rights or obligations to in-house counsels as they provide to external lawyers admitted to a Bar Association.
- **Protected materials.** The scope of the definition for the materials that are protected under the principle is also different in many jurisdictions.[6]

The more general purpose of the principle is to protect information shared between a client and their lawyer from disclosure with other parties. The principle has a dual nature:

(i) **From a lawyer's perspective.** Ensuring confidentiality is the lawyer's duty, right and / or privilege. It protects lawyers in the exercise of their professional obligations by allowing them to offer expert advice without fear of reprisal. In certain legal systems, professional secrecy also forms part of their obligations as members of their Bar Association which they are obliged to comply with.[7]

(ii) **From a client's perspective.** Ensuring confidentiality is a human right and / or privilege of the client.

According to the International Bar Association, the core of LPPC in almost every country is that a lawyer must not disclose information given to the lawyer by his or her client in the course of legal representation without there being a clear exemption to LPPC.

6 International Association of Lawyers (UIA), 'International Report on Professional Secrecy and Legal Privilege', https://www.uianet.org/sites/default/files/international_report_professional_secrecy.pdf, November 2019.

7 Ibid.

The Council of Europe has established a Committee of Experts on the Protection of Lawyers as of January 2022.[8] The Committee is working on a legal instrument with the main objective to strengthen the protection of the profession of lawyers. Although the possible outline of the instrument is still abstract, a study of the Council of Europe does stress the importance of determining the exact scope of confidentiality in dealing with clients.[9]

2.2 LPPC is not absolute

It is nevertheless important to realize that – as is the case with many human rights – LPPC is not absolute. The LAWASIA describes it as "a near absolute protection". The International Bar Association describes three reasons based on which the information protected by LPPC can be disclosed: (i) the lawyer is permitted to disclose it; (ii) the client discloses it; or, (iii) a governmental body or the court is permitted to require its disclosure.[10] Under what conditions for example governmental bodies, including national security agencies, may have access to the information protected by LPPC is heavily debated and regulated differently in all jurisdictions.[11]

Also, some regional bodies have regulated covert surveillance methods and underscored the importance of installing an oversight mechanism that can independently and effectively keep oversight over the actions of national security agencies. The Council of Europe Convention 108+ on the Protection of Individuals with Regard to the Processing of Personal Data is an example of a legal framework that imposes the duty to provide supervisory authorities in this context.[12] This convention is applicable to data processing in the national security domain, including personal data included in information in scope of LPPC.[13] It requires all signatories to Convention 108+ to provide for supervisory authorities with sufficient powers of investigation and intervention. Convention 108+ is also open for signature by non-Member States of the Council of Europe.

2.3 Implementation of LPPC in soft law

8 Council of Europe, 'Committee of Experts on the Protection of Lawyers (CJ-AV)', https://www.coe.int/en/web/cdcj/cj-av, n.d.

9 Council of Europe, 'Profession of Lawyer: Study on Feasibility of a new European legal instrument', https://rm.coe.int/eng-examen-de-faisabilite-d-un-instrument-juridque-europeen-couv-texte/1680a22790, April 2021, p. 99.

10 International Bar Association, 'IBA Statement in Defence of the Principle of Lawyer Client Confidentiality', https://www.ibanet.org/document?id=/IBA-Statement-in-Defence-of-the-Principle-of-Lawyer-Client-Confidentiality, January 2022.

11 It is not in scope of this report to assess and compare the legal framework relating to the interference of LPPC.

12 Council of Europe, 'Convention 108+ On the protection of individuals with regard to personal data processing', https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf, June 2018.

13 Ibid. Article 11 of Convention 108+ regulates the authorized (lawful) exceptions and restrictions to a limited number of provisions of the Convention, specified in article 11, paragraph 1 and 3).

2.3.1 United Nations Basic Principles of the Role of Lawyers (The Basic Principles)

The Basic Principles have been adopted in 1990 as part of the United Nations (**UN**) framework and is the first soft law instrument strengthening the profession of lawyers. This is a non-binding instrument formulated to assist Member States of the UN in their task of promoting and ensuring the important role of lawyers. LPPC is implemented in the Basic Principles of the Role of Lawyers. Article 22 of The Basic Principles specifies that "*Governments shall recognize and respect that all communications and consultations between lawyers and their clients within their professional relationship are confidential.*" Furthermore, Article 8 of The Basic Principles sets out that: "*All arrested, detained or imprisoned persons shall be provided with adequate opportunities, time and facilities to be visited by and to communicate and consult with a lawyer, without delay, interception or censorship and in full confidentiality. Such consultations may be within sight, but not within the hearing, of law enforcement officials.*"

Following The Basic Principles many standards, recommendations and guidelines have been adopted by international organizations and (international) Bar Associations, including but not limited to:

- The Council of Bars and Law Societies of Europe (**CCBE**):
  - Code of Conduct for European Lawyers[14]
  - Charter of Core Principles of the European Legal Profession[15]
  - Recommendations on the protection of client confidentiality within the context of surveillance activities[16]
- The International Bar Association (**IBA**):
  - Standards for the Independence of the Legal Profession[17]
  - Guide for Establishing and Maintaining Complaints and Discipline Procedures[18]
  - International Principles on Conduct for the Legal Profession[19]
  - IBA Statement in Defence of the Principle of Lawyer-Client Confidentiality[20]

14 CCBE, 'Code of Conduct for European Lawyers', https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_CoC/EN_DEONTO_2021_Model_Code.pdf/, 2021.

15 CCBE, 'Charter on the core principles of the European Legal Profession & Code of Conduct for European Lawyers', https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_CoC/EN_DEON_CoC.pdf, 2019.

16 CCBE, 'On the protection of client confidentiality within the context of surveillance activities', EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf, 2016.

17 IBA, 'Standards for the Independence of the Legal Profession', Adopted in 1990.

18 IBA, 'Guide for establishing and maintaining complaints and discipline procedures, https://www.ibanet.org/MediaHandler?id=2A17AA40-79A9-4B99-90A6-D0A7825FD76F, October 2007.

19 IBA, 'International Principles on Conduct for the Legal Profession', https://www.ibanet.org/document?id=IBA-International-Principles-on-Professional-Indemnity-Insurance-for-the-Legal-Profession, 3 November 2022.

20 IBA, 'Statement in Defence of the Principle of Lawyer-Client Confidentiality', https://www.ibanet.org/document?id=/IBA-Statement-in-Defence-of-the-Principle-of-Lawyer-Client-Confidentiality, January 2022.

- The Union International des Avocats (**UIA**):
  - Core Principles of the Legal Profession[21]
  - The Turin Principles on Conduct for the Legal Profession in the 21st Century[22]
  - International report on professional secrecy and legal privilege[23]
- LAWASIA:
  - Resolution on Legal Professional Privilege / Legal Professional secrecy.[24]

2.3.2 Implementation in local laws and regulations

All European countries have provisions protecting the right and duty of lawyers to keep clients' matters confidential.[25] A report published by the Law Society of England & Wales in 2022 on the independence of the legal profession and lawyers concluded that LPPC has been implemented in almost all jurisdictions in scope of the research, including: France, Georgia, Germany, United Kingdom, Brazil, Chile, Colombia, United States of America, Jordan, India, Indonesia, Japan, Malaysia, Kenya and South-Africa.[26] Most legal systems worldwide share a common understanding that LPPC is important to ensure the right to access to legal advice and justice.[27]

21 UIA, 'Core Principles of the Legal Profession', https://www.uianet.org/sites/default/files/core_principles_of_the_legal_profession_-_final_porto.pdf, 30 October 2018.

22 UIA, 'Turin Principles of Professional Conduct for the Legal Profession in the 21st Century', https://www.uianet.org/sites/default/files/charteturin2002-en.pdf, 2002.

23 UIA, 'International report on professional secrecy and legal privilege', https://www.uianet.org/sites/default/files/international_report_professional_secrecy.pdf, November 2019.

24 LAWASIA, 'LAWASIA resolution on legal professional privilege / legal professional secrecy', https://lawasia.asn.au/sites/default/files/2018-06/Resolution-Legal-Professional-Privilege-Legal-Professional-Secrecy-12Aug2016.pdf, 12 August 2016.

25 CCBE, 'On the protection of client confidentiality within the context of surveillance activities', EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf, 2016.

26 The Law Society, 'UN Basic Principles on the Role of Lawyers Report', https://www.lawsociety.org.uk/topics/research/un-basic-principles-on-the-role-of-lawyers#download, 17 February 2022.

27 CCBE, 'On the protection of client confidentiality within the context of surveillance activities', EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf, 2016.

3. Importance of LPPC

Rule of law. The core purpose of LPPC is to protect the rule of law. The rule of law is a set of principles that ensures a just, open, and effective society. These principles include – for example – the independence of the judiciary, the requirement of a legal basis for government action, and the presumption of innocence.[28] LPPC is essential to the rule of law, since the principle helps to ensure the right to an effective legal defense for everyone.

Human rights. LPPC can be elevated to a human right and is highly connected to other human rights.[29] The right to privacy, data protection, access to justice and fair trial are human rights that have been established in international, regional, and national legal frameworks, including the Universal Declaration of Human Rights[30], the Convention for the Protection of Human Rights and Fundamental Freedoms[31], Convention 108+[32], the General Data Protection Regulation[33] and similar data protection laws being implemented world-wide (like the PIPL[34], the CCPA[35], the LGPD[36] and the PIPEDA[37]). These human rights have a strong connection and overlapping characteristics with the principle of LPPC.[38]

As stressed by UIA: *"From a client perspective it is indispensable to the preservation of the client's right to counsel, to present a defense, to privacy, data protection and, ultimately, to due process and freedom."* From a lawyers perspective it is also connected to their right to privacy and data protection.[39]

28 IBA, 'Statement in Defence of the Principle of Lawyer-Client Confidentiality', https://www.ibanet.org/document?id=/IBA-Statement-in-Defence-of-the-Principle-of-Lawyer-Client-Confidentiality, January 2022, p. 5.

29 UIA, 'International report on professional secrecy and legal privilege, https://www.uianet.org/sites/default/files/international_report_professional_secrecy.pdf, November 2019.

30 Article 12 & Article 10 UDHR, UN General Assembly 1948.

31 Article 8 & Article 6 ECHR, Council of Europe 1953.

32 Article 1 & Articles 4 to 13 Convention 108+, Council of Europe 2018.

33 General Data Protection Regulation (GDPR), Regulation (EU) 2016/67, https://gdpr-info.eu.

34 Translation of Personal Information Protection Law (PIPL) of the People's republic of China, 7 November 2021. Retrieved from: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

35 California Consumer Privacy Act of 2018 (CCPA), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

36 General Personal Data Protection Act (LGPD) of Brazil, Law No. 13,709, https://lgpd-brazil.info.

37 Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada, https://laws-lois.justice.gc.ca/eng/acts/p-8.6/.

38 CCBE, 'On the protection of client confidentiality within the context of surveillance activities', EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf, 2016.

39 UIA, 'International report on professional secrecy and legal privilege', https://www.uianet.org/sites/default/files/international_report_professional_secrecy.pdf, November 2019.

Enables lawyers to protect the rule of law and human rights. The principle is essential for the "proper administration of justice".[40] The CCBE's Charter of Core Principles of the European Legal Profession describes the importance of confidentiality and trust between a lawyer and its client: *"It is of the essence of a lawyer's function that the lawyer should be told by his or her client things which the client would not tell to others - the most intimate personal details or the most valuable commercial secrets - and that the lawyer should be the recipient of other information on a basis of confidence. Without the certainty of confidentiality there can be no trust.*[41]

As described by the CCBE confidentiality is essential for lawyers to do their job, which includes the protection of the rule of law and the rights of their clients: *"Undermining the confidentiality of lawyer-client communication – whether that confidentiality is founded upon the concept of professional secrecy or (as it is in some jurisdictions) legal professional privilege – means violating international obligations, denying the rights of the accused, and an overall compromising of the democratic nature of the State."*[42]

Unfortunately, the principle is at risk. Early 2022, The International Bar Association issued a statement in defense of LPPC.[43] The statement was very comprehensive and included several accounts of concerning comments of international actors, calling for limitations or even the abolishment of LPPC. In a report published in 2022 on the independence of the Legal Profession and Lawyer/Client Rights Worldwide the Law Society of England & Wales concluded that "*Despite the binding nature of these principles and fair trial rights, many violations of these continue to occur in jurisdictions worldwide (including in jurisdictions analyzed in this report)."*[44]

In the past years, human rights organizations and lawyers' associations have reported on the increasing prevalence of lawyers' communications with their clients being subject to wiretaps and surveillance. For example, in the wake of the Snowden revelations in 2014,

40 LAWASIA, 'LAWASIA resolution on legal professional privilege / legal professional secrecy', https://lawasia.asn.au/sites/default/files/2018-06/Resolution-Legal-Professional-Privilege-Legal-Professional-Secrecy-12Aug2016.pdf, 12 August 2016.

41 CCBE, 'Charter on the core principles of the European Legal Profession & Code of Conduct for European Lawyers', https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_CoC/EN_DEON_CoC.pdf, 2019, p. 8.

42 CCBE, 'On the protection of client confidentiality within the context of surveillance activities', EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf, 2016, p. 5.

43 International Bar Association, 'IBA Statement in Defence of the Principle of Lawyer-Client Confidentiality', https://www.ibanet.org/document?id=/IBA-Statement-in-Defence-of-the-Principle-of-Lawyer-Client-Confidentiality, January 2022.

44 Law Society of England and Wales, 'UN Basic Principles on the Role of Lawyers: Independence of the Legal Profession and Lawyer/Client rights worldwide', https://www.lawsociety.org.uk/topics/research/un-basic-principles-on-the-role-of-lawyers, February 2022, p. 53.

Human Rights Watch reported on the impact of surveillance by the US government on lawyers and their clients.[45] In 2016, the CCBE also published a report regarding lawyers and surveillance in response to reports of mass surveillance in European states.[46]

In recent years, a decline in rule of law standards around the world has been observed.[47] Those working on human rights and other politically sensitive topics, including lawyers, are faced with suspicion and hostility from governmental authorities and operate in an increasingly shrinking civic space.[48] The exploitation of the vulnerabilities of digital communication methods for surveillance purposes is therefore very concerning but can be seen as a symptom of a wider declining rule of law trend.

45 Human Rights Watch, 'With liberty to monitor all', https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and, July 2014.

46 CCBE, 'CCBE Recommendations on the protection of client confidentiality within the context of surveillance activities', https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf, 2016.

47 Freedom House, 'Freedom in the world 2023', https://freedomhouse.org/sites/default/files/2023-03/FIW_World_2023_DigtalPDF.pdf, March 2023.

48 Amnesty International, 'Situation of the World's Human Rights Defenders', https://www.amnesty.org/ar/wp-content/uploads/2021/05/IOR4086002018ENGLISH.pdf, 2018, p. 10.

4. Case studies

As outlined in the legal framework above, the principle of LPPC is well-established through international, regional, and domestic laws. However, as also already mentioned, the principle has come under pressure. The case studies in this section – Pegasus, wiretapping of Polish lawyers, and gathering of protected communication by the Dutch prosecutor's office – highlight the various ways in which LPPC can be breached and impacts of this upon lawyers' work and personal life.

4.1 Pegasus Surveillance of Lawyers

Pegasus is a software developed by the Israeli company NSO Group (**NSO**). Pegasus is a hacking software that can be used to turn your phone into a 24-hour surveillance device. It can copy your messages, see your photos, film you, record your calls and activate the microphone to record your conversations. Pegasus software uses flaws or bugs in operating systems to infect phones.[49]

During a data breach in 2021 a list of more than 50,000 phone numbers was revealed that had possibly been targeted with Pegasus. The phone numbers have been identified as those of people of interest by clients of NSO since 2016. The data did not reveal whether the device in question was actually hacked, or subject to an attempted hack. Still, the data is indicative of the potential targets that NSO's clients had identified for surveillance.[50] In the so-called 'Pegasus Project', Citizen Lab and Amnesty International's Security Lab reached out to potential targets of the Pegasus software and performed in-depth forensic analysis of phones. Their research confirmed the widespread and ongoing unlawful surveillance of human rights defenders and other civil society members.[51] The Pegasus surveillance software has been used in 45 different countries.[52]

Amongst the human rights defenders who were targeted are also lawyers. Lawyers for Lawyers has spoken to a number of lawyers who have been targeted by the Pegasus surveillance software. The three cases described below illustrate the impact that a Pegasus infection of their phones has on lawyers.

49 European Parliament, 'Pegasus and surveillance spyware', https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf, May 2022, p. 4.

50 Ibid, p. 4.

51 Amnesty International, 'Forensic Methodology Report: NSO Group's Pegasus', https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/, 18 July 2021.

52 European Parliament, 'Pegasus and surveillance spyware', https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf, May 2022, p. 4.

Hala Ahed Deeb

Hala Ahed Deeb is a Jordanian lawyer who has worked on a range of human rights issues. She is active for several human rights and feminist organizations through which she defends civil rights, women's rights, labour rights, and prisoners of conscience. She was a member of the legal team defending the Jordan Teacher's Syndicate, a large Jordanian labour union that was dissolved by the government in reaction to mass protests.[53] To sustain her human rights work, she also takes cases relating to trade issues, financial law, and criminal law.

In November 2021, Ms. Deeb was contacted by Front Line Defenders, who informed her that phones In Jordan had been infected and offered to test her phone.[54] She sent her phone for testing and Front Line Defenders, Citizen Lab, and the Amnesty International Security Lab confirmed that her phone had been infected. They informed her that her phone had been infected in March 2021.

Ms. Deeb changed her phones once she learned about the infection with the Pegasus Spyware. She also distanced herself from some of the human rights groups she had been working with for fear that she might have endangered them. After the story came out, she lost quite a few of her clients for whom she did non-human rights work, which affected her income. The clients felt that it might be unsafe to contact her, and that the surveillance might harm their case.

Besides the impact on her work, Ms. Deeb expressed that she felt the Pegasus infection as a deep violation of her privacy. There was a lot of information on her phone, including personal information about family and friends. After she learned about the Pegasus infection, she felt unsafe and like she was being followed.

Ms. Deeb has strong reasons to believe that the Jordanian government was behind her Pegasus infection, as she was working on politically sensitive cases, such as Jordan Teacher's Syndicate case, at the time. Other lawyers working on that case were also infected, and Citizen Lab and Amnesty International were able to trace that hack back to the Jordanian authorities. Although she could have taken the surveillance to court, she refrained from doing so as Ms. Deeb did not believe that this would lead to an independent and impartial investigation. She expressed frustration with the situation, as she is unsure how she and other lawyers can protect themselves from unlawful surveillance in the future.

53 Human Rights Watch, 'Jordan: Teachers' Syndicate Closed; Leaders Arrested', https://www.hrw.org/news/2020/07/30/jordan-teachers-syndicate-closed-leaders-arrested, 30 July 2020.

54 Front Line Defenders, 'Unsafe Anywhere: Women human rights defenders speak out against Pegasus attacks', https://www.frontlinedefenders.org/en/resource-publication/unsafe-anywhere-women-human-rights-defenders-speak-out-about-pegasus-attacks, 16 January 2022.

Salah Hammouri

Salah Hammouri is a French-Palestinian human rights lawyer. He works for the Addameer Prisoners Support and Human Rights Association[55], through which he supports the rights of political prisoners held in Israeli and Palestinian prisons. Mr. Hammouri has faced many repercussions for his human rights work, including arrests, imprisonment, travel bans, and ID-revocation. Mr. Hammouri has spent a total of 9 years and 6 months in Israeli prison and is currently living in exile in France, after he was forcibly deported in December 2022. A case regarding his forced deportation is still pending.[56]

In November 2021, Mr. Hammouri was contacted by Citizen Lab, who informed him that his phones had likely been hacked with the Pegasus surveillance software. Mr. Hammouri and some of his colleagues sent their devices to the Amnesty International Security Lab, who found that his phone had indeed been infected with the spyware.[57]

Consequently, Mr. Hammouri turned off his devices and did not use a phone for weeks. He received a new secure device, but no longer felt free to speak on the phone. He refrained from contacting clients, colleagues, and family members through his devices, as he feared that his interactions were still not secure, and he did not want to put them and himself at risk. The surveillance had a large impact on his sense of personal safety and privacy.

Also Mr. Hammouri's work was severely impacted by the surveillance. First, because he knew that the Israeli government had had access to all information on his phone. This included information about cases, such as sensitive information regarding (anonymous) witnesses and case strategies. Secondly, Mr. Hammouri felt that his clients became afraid to talk to him openly and share all information with him. Moreover, going to see his clients physically rather than communicating through calls, direct messaging and email took a lot of time.

Mr. Hammouri shared his strong concerns that information on his phone had been used by the Israeli authorities. Against his clients, but also against him personally, for example during the proceedings of his deportation case in 2022.

Mr. Hammouri initiated a case against NSO Group before the French courts that is still pending.

55 Addameer Prisoner Support and Human Rights Association, https://www.addameer.org, n.d.

56 For more information on Salah Hammouri and the repercussions for his work, please see: https://justice-for-salah.net.

57 Amnesty International & Citizen Lab, 'Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware', https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/, 8 November 2021.

Shalini Gera

Shalini Gera is an Indian human rights lawyer and the co-founder of the Jagdalpur Legal Aid Group through which she provides free legal aid to the minority Adivasi people. Furthermore, Ms. Gera has worked on cases relating to violations in conflict zones, including extrajudicial killings.

In the fall of 2019, Ms. Gera was informed by Citizen Lab that her phone had been targeted for digital surveillance through Pegasus.[58] She had lost the infected phone before she had been contacted by Citizen Lab, so she was already using a new phone. Ms. Gera was working as a defense lawyer in a nationwide terrorism case at the time she was targeted. Even though she already had a new phone, Ms. Gera became less trusting of using her phone for sensitive phone calls. Furthermore, she says that she knows that some people stopped communicating with her after the Pegasus news came out. She believes she was targeted with Pegasus by the Indian authorities.

Ms. Gera and other targeted lawyers and human rights defenders attempted to put pressure on the government by getting journalist to report on the case and participating in the inquiry committee set up by the Indian Supreme Court. Still, to this date, the Indian State has not responded to allegations of having used the spyware against Ms. Gera and other Indian human rights defenders.[59] Overall, Ms. Gera stated that there are no effective oversight mechanisms to State authorities surveillance powers in India.

It was also not the first time that Ms. Gera had been subjected to unlawful surveillance. In 2016, when she was working in a conflict zone, she and other lawyers were wiretapped by the authorities. She found out that their phones had been tapped, because every time Ms. Gera and her colleagues went somewhere, the police would be there waiting for them. There was no other way they could have known where they were going. The goal seemed to be to intimidate Ms. Gera and her colleagues.

Ms. Gera expressed that she experienced the Pegasus spyware to be even more intrusive than the wiretapping she was subjected to in 2016. Through the Pegasus software those who spied on her could access all the information on her phone, including personal data and sensitive case information. Ms. Gera expressed that she felt this as a totally new level of violation, compared to the wiretapping.

58 Amnesty International, 'India: Human Rights Defenders Targeted by a Coordinated Spyware Operation', 15 June 2020, https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/.

59 The Wire, 'Pegasus: Malware found in five phones, Government 'refused to cooperate' with probe, says CJI', https://thewire.in/law/supreme-court-pegasus-technical-committee, 5 August 2022.

The case study regarding Pegasus surveillance against lawyers shows the impact that surveillance of this kind has on lawyers' work and on them personally. They alter their behaviour, such as leaving devices in other rooms during sensitive conversations, refraining from using devices at all, or refraining from speaking about sensitive information over the phone. The cases above also show that clients are deterred from speaking freely with their lawyer when they know that there is a possibility that the lawyer is subject to online surveillance. Lawyers further report feeling violated in their privacy, in particular spyware infections such as Pegasus are experienced as very intrusive.

Overall, this type of systematic and unlawful surveillance creates a strong chilling effect on both lawyers and their clients, and breaches LPPC. It also shows that lawyers in many jurisdictions do not have access to an effective recourse mechanism. Even when those frameworks and oversight mechanisms to State authorities' surveillance powers do exist, in some countries they do not operate independently from the government. This leaves many lawyers with very few options to gain insight into surveillance practices and to challenge surveillance when it does occur.

This confirms that unlawful surveillance of this kind that interferes with LPPC tends to exist against the backdrop of a declining rule of law and shrinking space for civil society. At the same time, the surveillance shrinks this space further as human rights lawyers are hindered in their work and the surveillance impacts on their personal sense of privacy and safety.

4.2 Surveillance of online and phone communications of Polish lawyers

Lawyers in Poland have in recent years been systematically and on large scale been subjected to surveillance operated by Polish counter-intelligence agencies. The Pegasus case study showed the strong negative implications of lawyers being targeted directly with surveillance software like Pegasus. The case study of Polish lawyers corroborates this finding. It also shows the additional problematic nature of when it is not the lawyer themselves who is targeted for surveillance of their communications but their client, and no distinction is made between protected and unprotected conversations.

Lawyers for Lawyers spoke with Mikolaj Pietrzak, who is the Dean of the Warsaw Bar Association.[60] As a lawyer, Mr. Pietrzak is specialized in criminal law and human rights protection. Mr. Pietrzak is currently the applicant in a case before the European Court of Human Rights concerning the lack of transparence and recourse with regards to unlawful monitoring of telecommunications and digital communications in Poland.[61] This case is currently still pending.

Mr. Pietrzak places the problems with unlawful surveillance of lawyers in Poland firmly within the rule of law problems that Poland has been experiencing since 2016. He expresses his belief that *"the abuse of surveillance powers has a much more severe impact in the context of authoritarian rule. It weakens the control mechanisms".* In the years leading up to 2016, Poland failed to implement the rulings by two different courts in 2014 that mandated legislative changes to install control mechanisms on counter-intelligence agencies.[62] Mr. Pietrzak stated that a lot of the surveillance problems could have been avoided if these judgements had been implemented and effective control mechanisms had been installed.

Mr. Pietrzak expresses that Polish lawyers are subject to a range of threats to LPPC. However, the most important violation – wiretapping – is also the one that is the hardest to find out about. He estimates that the Bar only finds out about a very small percentage of wiretaps being used against lawyers. He states that *"wiretapping is the easiest way to breach lawyer-client privilege, and the hardest to find out about".*

Mr. Pietrzak found out that conversations of his co-counsel with their client in a domestic terrorism case had been recorded through a wiretap targeted against his client. The public prosecutor shared all wiretap recordings of Mr. Pietrak's client with the court, which included several conversations of his client and his co-counsel. During these recorded conversations sensitive information was discussed, such as defense strategies and evidence. The information was shared as opensource to the Court. The fact that the conversation was recorded at all and then shared in such a public manner with the court constituted a clear violation of the LPPC. Mr. Pietrzak believed that the light-heartedness with which the public prosecutor shared the wiretap recordings shows how accepted wiretaps of this kind are within the Polish system.

60 Warsaw Bar Association, https://www.ora-warszawa.com.pl/czlonkowie-ora/, 'CZŁONKOWIE ORA: Prezydium', n.d.

61 ECtHR, Pietrzak v Poland, no. 72038/17.

62 ECtHR, Al-Nashiri v. Poland, no. 28761/11, 24 July 2014. Constitutional Tribunal of Poland, Judgement dated July 30, 2014, case no K23/11.

When information about the wiretapping of lawyers became known amongst the legal community in Poland, Mr. Pietrzak described that this brought about a chilling effect and forced Polish lawyers to start using different strategies to avoid surveillance. For example, meetings where even slightly sensitive information was being discussed are held in person, rather than on the phone or online. When Polish lawyers do speak to each other or to their client over the phone, they often make a disclaimer before starting the conversation that the conversation is protected by LPPC and that it is a crime for anyone to listen to it and record it.

Mr. Pietrzak expressed that the strategies described above do not solve the surveillance problem. He deems it highly undesirable that lawyers and human rights defenders have to rely on a technological arms race to try to counter the intelligence agencies' surveillance. He believes that the solution lies in implementing effective oversight mechanisms over counter-intelligence agencies. He states that "*as a lawyer, I should not have to rely on being technologically more advanced than the intelligence agency".* Overall, he states that the wiretapping and other forms of surveillance employed by the intelligence agencies lead to a chilling effect on the Polish legal community.

4.3 Seizure of protected communications by Dutch prosecutor

In January 2022, Dutch law firm Stibbe filed a complaint against the Dutch State for systematically violating the principle of LPPC which is protected under Dutch law.[63] Specifically, Stibbe accused the Dutch Public Prosecutor of having gathered and read email communications between Stibbe's lawyers and their clients. Stibbe's client in this case had been accused of fraud and as part of the Dutch Public Prosecutor's criminal investigation, they had seized the client's email servers. As a result, the Prosecutor also got access to email communications that were protected by LPPC. Stibbe argued that since 2015 the Dutch Public Prosecutor in this case had accessed 3115 emails between Stibbe's lawyers and their client.[64] Stibbe discovered the violation after the Dutch Public Prosecutor searched for a report that had only been mentioned in confidential email communications between Stibbe's lawyers and the client.

63 Article 272 (1) Wetboek van Strafrecht.

64 Rietbroek, 'Stibbe vs. de Staat over verschoningsrecht: 'Werkwijze OM is fundamenteel fout'' in *Advocatie*, https://www.advocatie.nl/nieuws/stibbe-vs-de-staat-over-verschoningsrecht-werkwijze-om-is-fundamenteel-fout/, 23 February 2022.

On 22 March 2022, the preliminary relief court (in Dutch: '*voorzieningenrechter*') ruled in favour of Stibbe.[65] In its judgment, the Court directly prohibited the Dutch State from viewing protected communications between lawyers and their clients.[66] It also mandated that the Prosecutor's code of conduct for handling protected communications should be clarified. The Court concludes that there is a real danger that LPPC has been or is being violated in criminal investigations.[67] Lawyer Tim de Greve of Stibbe commented on the judgment that "*when [the Public Prosecutor] is not allowed to read the letters of a lawyer, this prohibition should equally apply to the emails of that lawyer"*.[68]

The State appealed the judgement. On 27 February 2023, the Court of Appeal (in Dutch: '*Gerechtshof*') again found that the State had violated LPPC in this case.[69] The Court of Appeal stated that in this case the Dutch Public Prosecutor had willfully accepted the risk of violating LPPC.[70]

The example of the seizure of protected emails by the Dutch Public Prosecutors shows that the Public Prosecutor should have clear guidelines with regards to the treatment of protected communications, and that these guidelines should be subject to oversight by an independent mechanism. This case study further illustrates that even in countries that generally score high on rule of law indicators, there can still be issues with regards to LPPC.

65 Rechtbank Oost-Brabant, 22 March 2022, ECLI:NL:RBOBR:2022:1035, https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOBR:2022:1035.

66 Pijnappels, 'Het eindeloze gevecht om het verschoningsrecht' in *Advocatenblad*, https://www.advocatenblad.nl/2022/03/31/het-eindeloze-gevecht-om-het-verschoningsrecht/, 31 Maart 2022.

67 Rechtbank Oost-Brabant, 22 March 2022, ECLI:NL:RBOBR:2022:1035. par. 4.22.

68 Pijnappels, 'Het eindeloze gevecht om het verschoningsrecht' in *Advocatenblad*, : https://www.advocatenblad.nl/2022/03/31/het-eindeloze-gevecht-om-het-verschoningsrecht/, 31 Maart 2022.

69 Gerechtshof Den Haag, 27 February 2023, ECLI:NL:GHDHA:2023:298, https://www.recht.nl/rechtspraak/uitspraak/?ecli=ECLI:NL:GHDHA:2023:298.

70 Gerechtshof Den Haag, 27 February 2023, ECLI:NL:GHDHA:2023:298, par 5.3. See also: 'Opnieuw oorvijg om verschoningsrecht' in *Advocatenblad*, https://www.advocatenblad.nl/2023/03/02/opnieuw-oorvijg-om-om-verschoningsrecht/, 2 March 2023.

5. Conclusions

LPPC insufficiently protected. This report demonstrates that lawyers' electronic communications with their clients are far from safe, despite being protected in a range of domestic, regional, and international legal instruments under the principle of LPPC. The findings of this report align with that of earlier reports on lawyer-client confidentiality and/or lawyers and surveillance. In 2022 the IBA published its Statement in Defence of the Principle of lawyer-client confidentiality, where it defended the principle after becoming subject of increasingly hostile rhetoric. In 2014 and 2016, respectively, Human Rights Watch and the CCBE published their reports on surveillance of lawyers in the United States and in Europe, and the concerning impact on lawyers and their work.

Development of increasingly sophisticated surveillance methods. Unfortunately, the situation does not appear to have improved. In fact, the situation may even have worsened over the years, as increasingly sophisticated and intrusive surveillance methods have been developed. Lawyers' digital communications with their clients are the subject of increasingly refined surveillance that is difficult to challenge, not in the least because it is often difficult to establish that the surveillance has even occurred. The case studies in this report show that LPPC with regards to digital communications can be breached in various ways. In some countries, lawyers are personally targeted for surveillance by national security agencies because they work on politically sensitive cases. In others, protected communications can be swept up in criminal investigations by public prosecutors. In those cases, the client is targeted rather than the lawyer themselves, but this nonetheless breaches LPPC. In countries where the legal system functions effectively and independently, lawyers are more likely to have access to a recourse mechanism through which they can force the national security agencies and/or public prosecutor's office to comply with the principle of LPPC. However, this may not be the case worldwide.

Lack of transparency and foreseeability. Moreover, transparency and foreseeability of surveillance is an issue. Lawyers report finding out that they have been subject to unlawful surveillance by chance, or when they are contacted by organizations investigating unlawful surveillance practices, such as Citizen Lab or Amnesty's Security Tech Lab in the Pegasus cases. Several lawyers further state that even when they knew that their phones had been infected with spyware or they had been surveilled in another way, they had no way of finding out which communications the security agencies had specifically accessed and in which ways these communications had been used. The lack of transparency, foreseeability and recourse in many jurisdictions creates a situation in which many lawyers are powerless in finding out whether or not their communications have been subject to surveillance, and equally powerless in situations where they have evidence that LPPC has been breached.

Chilling effect and impact on fundamental human rights. Furthermore, the impacts of these types of unlawful surveillance are worrying. Lawyers report a large impact on their work and on their clients. Lawyers have moved parts of their communications offline, meeting colleagues and clients in person to discuss sensitive subjects. Additionally, some clients are even deterred from speaking with the lawyers at all, after they learn about the surveillance. Furthermore, it is very concerning that state agencies have gained access to protected communications that possibly detail information that is relevant for ongoing cases that involve state agents. Surveillance thus negatively impacts on the work of lawyers and on their clients as it erodes the trust in the confidentiality of communications between lawyers and their clients and can give the state an unfair advantage in legal cases. Further, if clients are deterred from reaching out to their lawyers, or from contacting certain lawyers, due to reports of surveillance against those lawyers, this impacts upon their free choice of counsel. The use of unlawful surveillance thus has a chilling effect on lawyers and their clients and impacts not only the principle of LPPC, but also the right to privacy, data protection, access to justice and fair trial.

Impact personal lives lawyers. Lawyers also report a large impact on their personal lives and sense of safety because of unlawful surveillance. Multiple lawyers stated experiencing feelings of unsafety and distress upon learning that their communications had been targeted for surveillance. In particular, the use of invasive spyware technology, such as Pegasus, that gives full access to all information on an infected phone, was experienced by the lawyers as very invasive. The lawyers reported feeling concern for everyone with whom they had communicated through the infected phone, such as family, friends, and acquaintances, next to colleagues, clients, and witnesses. The risk is present that lawyers might be deterred from taking up cases that they know will likely illicit surveillance methods being used against them in order to protect their personal privacy.

Lawyers for Lawyers condemns the unlawful infringements to LPPC, including the unlawful use of surveillance methods infringing LPPC. As shown in this report, not all states effectively protect LPPC. LPPC is important worldwide but codified and defined in diverging ways in domestic and regional systems. Making specific recommendations as to the changes necessary within specific legal regimes to better protect LPPC is not feasible within the scope of this report.

Further enhance transparency and foreseeability. However, we can conclude that it is desirable that states clearly define LPPC and the limited situations in which interference may be lawful within their laws to enhance transparency and foreseeability. Furthermore,

it is important that agencies involved in law enforcement, including national security agencies and public prosecutors, are educated on the concept of LPPC and those limited situations in which LPPC may be infringed upon. These agencies should be subject to independent oversight mechanisms that have sufficient powers for effective investigation and intervention. These oversight mechanisms should be accessible for lawyers to turn to if they suspect an unlawful breach of LPPC.

Further reporting on interferences with LPPC is necessary. Lawyers for Lawyers encourages further reporting on LPPC, its legal protection in national jurisdictions, and the challenges posed to it by surveillance. We also encourage actors at the national, regional, and international level to speak out against instances of unlawful surveillance that violates LPPC. In a digital world, breaching LPPC is easier than ever before and harder to challenge than ever before. LPPC is of key importance to the protection of fundamental rights and the rule of law, and its protection deserves our continued commitment.

Bibliography

- Law Society of England and Wales, 'UN Basic Principles on the Role of Lawyers: Independence of the Legal Profession and Lawyer/Client rights worldwide', https://www.lawsociety.org.uk/topics/research/un-basic-principles-on-the-role-of-lawyers, February 2022.
- International Association of Lawyers (UIA), 'International Report on Professional Secrecy and Legal Privilege', https://www.uianet.org/sites/default/files/international_report_professional_secrecy.pdf, November 2019.
- Council of Europe, 'Committee of Experts on the Protection of Lawyers (CJ-AV)', https://www.coe.int/en/web/cdcj/cj-av, n.d.
- Council of Europe, 'Profession of Lawyer: Study on Feasibility of a new European legal instrument', https://rm.coe.int/eng-examen-de-faisabilite-d-un-instrument-juridque-europeen-couv-texte/1680a22790, April 2021.
- International Bar Association, 'IBA Statement in Defence of the Principle of Lawyer Client Confidentiality', https://www.ibanet.org/document?id=/IBA-Statement-in-Defence-of-the-Principle-of-Lawyer-Client-Confidentiality, January 2022.
- Council of Europe, 'Convention 108+ On the protection of individuals with regard to personal data processing', https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf, June 2018.
- CCBE, 'Code of Conduct for European Lawyers', https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_CoC/EN_DEONTO_2021_Model_Code.pdf/, 2021.
- CCBE, 'Charter on the core principles of the European Legal Profession & Code of Conduct for European Lawyers', https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_CoC/EN_DEON_CoC.pdf, 2019.
- CCBE, 'On the protection of client confidentiality within the context of surveillance activities', EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf, 2016.
- IBA, 'Standards for the Independence of the Legal Profession', Adopted in 1990.
- IBA, 'Guide for establishing and maintaining complaints and discipline procedures, https://www.ibanet.org/MediaHandler?id=2A17AA40-79A9-4B99-90A6-D0A7825FD76F, October 2007.
- IBA, 'International Principles on Conduct for the Legal Profession', https://www.ibanet.org/document?id=IBA-International-Principles-on-Professional-Indemnity-Insurance-for-the-Legal-Profession, 3 November 2022.
- UIA, 'Core Principles of the Legal Profession', https://www.uianet.org/sites/default/files/core_principles_of_the_legal_profession_-_final_porto.pdf, 30 October 2018.

- UIA, 'Turin Principles of Professional Conduct for the Legal Profession in the 21st Century', https://www.uianet.org/sites/default/files/charteturin2002-en.pdf, 2002.
- UIA, 'International report on professional secrecy and legal privilege', https://www.uianet.org/sites/default/files/international_report_professional_secrecy.pdf, November 2019.
- LAWASIA, 'LAWASIA resolution on legal professional privilege / legal professional secrecy', https://lawasia.asn.au/sites/default/files/2018-06/Resolution-Legal-Professional-Privilege-Legal-Professional-Secrecy-12Aug2016.pdf, 12 August 2016.
- Human Rights Watch, 'With liberty to monitor all', July 2014. Retrieved from: https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and.
- Freedom House, 'Freedom in the world 2023', https://freedomhouse.org/sites/default/files/2023-03/FIW_World_2023_DigtalPDF.pdf, March 2023.
- Amnesty International, 'Situation of the World's Human Rights Defenders', https://www.amnesty.org/ar/wp-content/uploads/2021/05/IOR4086002018ENGLISH.pdf, 2018.
- European Parliament, 'Pegasus and surveillance spyware', https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf, May 2022.
- Amnesty International, 'Forensic Methodology Report: NSO Group's Pegasus', https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/, 18 July 2021.
- Addameer Prisoner Support and Human Rights Association, https://www.addameer.org, n.d.
- Amnesty International & Citizen Lab, 'Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware', https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/, 8 November 2021.
- Amnesty International, 'India: Human Rights Defenders Targeted by a Coordinated Spyware Operation', 15 June 2020, https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/.
- The Wire, 'Pegasus: Malware found in five phones, Government 'refused to cooperate' with probe, says CJI', https://thewire.in/law/supreme-court-pegasus-technical-committee, 5 August 2022.
- Human Rights Watch, 'Jordan: Teachers' Syndicate Closed; Leaders Arrested', https://www.hrw.org/news/2020/07/30/jordan-teachers-syndicate-closed-leaders-arrested, 30 July 2020.
- Front Line Defenders, 'Unsafe Anywhere: Women human rights defenders speak out against Pegasus attacks', https://www.frontlinedefenders.org/en/resource-publication/unsafe-anywhere-women-human-rights-defenders-speak-out-about-pegasus-attacks, 16 January 2022.

- Warsaw Bar Association, https://www.ora-warszawa.com.pl/czlonkowie-ora/, 'CZŁONKOWIE ORA: Prezydium', n.d.
- Rietbroek, 'Stibbe vs. de Staat over verschoningsrecht: 'Werkwijze OM is fundamenteel fout'' in *Advocatie*, https://www.advocatie.nl/nieuws/stibbe-vs-de-staat-over-verschoningsrecht-werkwijze-om-is-fundamenteel-fout/, 23 February 2022.
- Pijnappels, 'Het eindeloze gevecht om het verschoningsrecht' in *Advocatenblad*, https://www.advocatenblad.nl/2022/03/31/het-eindeloze-gevecht-om-het-verschoningsrecht/, 31 Maart 2022.
- Opnieuw oorvijg om verschoningsrecht' in *Advocatenblad*, https://www.advocatenblad.nl/2023/03/02/opnieuw-oorvijg-om-om-verschoningsrecht/, 2 March 2023.

Cited Caselaw:

- ECtHR, *S. v. Switzerland*, App. No. 12629/87; 13965/88, 28 November 1991.
- ECtHR, *Michaud v. France*, App. No. 12323/11, 6 December 2012.
- ECtHR, *R.E. v. United Kingdom,* App. No. 62498/11, 27 October 2015.
- ECtHR, *Pietrzak v Poland*, App. No. 72038/17.
- ECtHR, *Al-Nashiri v. Poland*, App. No. 28761/11, 24 July 2014.
- Constitutional Tribunal of Poland, Judgement dated 30 July 2014, case no K23/11.
- Rechtbank Oost-Brabant (Netherlands), 22 March 2022, ECLI:NL:RBOBR:2022:1035.
- Gerechtshof Den Haag (Netherlands), 27 February 2023, ECLI:NL:GHDHA:2023:298.