sciendo

A proactive approach to legal privilege in the light of electronic communication

Zoltán Gyurász

Faculty of Law
Institute of Information Technology Law and Intellectual Property Law
Comenius University in Bratislava
Šafárikovo nám. č. 6, P.O. box 313
Bratislava 810 00, Slovakia
zoltan.gyurasz@flaw.uniba.sk

Ondrej Hamuľák

Department of International and European Law
Palacký University Olomouc
17. listopadu 930/8
Olomouc 779 00, Czech Republic
ondrej.hamulak@upol.cz

Department of Law
School of Business and Governance
Tallinn University of Technology
Ehitajate tee 5
Tallinn 19086, Estonia
ondrej.hamulak@taltech.ee

Petra Dražová

Faculty of Law
Institute of Information Technology Law and Intellectual Property Law
Comenius University in Bratislava
Šafárikovo nám. č. 6, P.O. box 313
Bratislava 810 00, Slovakia
petra.drazova@flaw.uniba.sk

Abstract: This article explores the proactive management of legal professional privilege (LPP) in the context of electronic communication, addressing the lack of clarity regarding how the shift to digital communication has affected this fundamental safeguard. Despite LPP being a cornerstone of democratic legal systems, serving both client interests and the administration of justice, the

https://doi.org/10.2478/bjes-2025-0006 *TalTech Journal of European Studies*, 15(1(41))
Tallinn University of Technology (ISSN 2674-4619)

implications of overreliance on electronic communication on this privilege remain largely unexplored. Several questions arise about how this impacts the LPP itself, what challenges attorneys face in maintaining this privilege in digital environments and whether the current legal frameworks are adequate to address the complexities introduced by these technologies. These questions mark a wide gap in understanding, as cases involving the misuse of technology and inadvertent disclosures have started to emerge. The proactive legal approach in lawyering could prioritize risk management and litigation avoidance while simultaneously enhancing the protection of legal privilege in this context. This paper argues that maintaining LPP currently presents unprecedented challenges and aims to advocate for proactive consideration of specific issues, allowing practitioners to preserve the integrity of client confidentiality and fair representation.

Keywords: *confidentiality, electronic communication, legal professional privilege, proactive law, professional secrecy*

1. Introduction

Proactive law, from its inception, can be said to provide a pragmatic and ethical response to practical legal needs (Pohjonen, 2006; Berger-Walliser, 2012), precisely the kind of vacuum that we are experiencing in legal practice resulting from drastic sociotechnical changes (DiMatteo *et al.* 2021; Jones *et al*., 2021). One of these emerges with regard to the common law concept of legal professional privilege (LLP) or professional secrecy (PS) and legal professional confidentiality, which are equivalent notions in the countries of civil law tradition (Fischel, 1998). The ease of access to information has fundamentally transformed societal interactions and has changed or forced the redefinition of legal practices across fields and sectors. Information has become accessible at any given moment and in any location, enabling rapid decision making and enriching qualitative outcomes with hugely improved efficiency. At the same time, it introduces greater vulnerabilities and risks.

It is not rare for attorneys to communicate with clients exclusively through electronic means, especially in the aftermath of the COVID-19 pandemic, when this trend was reinforced by the emergence of a number of technology-driven solutions for remote communication in video, calls and online chats.

In addition, mediated interactions are normalized in practice. Among the most common platforms in use are SlikSafe, Pryvate, Signal, WhatsApp, Telegram, ProtonMail, LINE, Dust, Wickr, Viber, Threema, Silent Phone, Wire, iMessage, FaceTime and KakaoTalk. It goes without saying that email has long since supplanted traditional letter correspondence, except when unavailable, limited or disallowed. For example, it may be required by law that a convicted individual serving a prison sentence or an accused person placed in a detention facility can receive, and at his own expense send, correspondence, only in paper form (see, e.g., *Act no. 475/2005 Coll.*, para. 25(1); *Act no. 221/2006 Coll.*, para. 20(1)).

This shift from traditional office visits and paper mail to digital methods has also been driven by the need for security and efficiency in handling confidential information. Lawyers now routinely manage electronic files and use smart devices, considering that sensitive client data, whether stored locally or in the cloud, is protected by robust security measures, such as end-to-end encryption (E2EE). This promises that a call or a message will not be readable by a third party during its transmission (Dechand *et al.*, 2019). Therefore, confidential information exchanged between attorneys and clients may be stored on local devices within the law office, mobile phones, computers, servers or external hard drives, as well as remotely in cloud-based storage systems.

A pressing concern in this context is the lack of transparency among service providers regarding their policies on stored data reuse. This extends to profiling and behavioral patterns of attorney– client interactions, which are issues oddly neglected in the literature. The digital footprints of legal professionals and their clients may become data points in sophisticated algorithmic mappings that raise questions about privacy, consent, ethics and the boundaries of professional discretion in an interconnected technological landscape (Gnusowski and Lipiec, 2024).

Legal experts should become more strategic than ever in understanding and managing the challenges of the digital age (Corrales Compagnucci, Fenwick and Haapio, 2019; Hietanen-Kunwald and Haapio, 2021) and in strengthening prevention through risk management in terms of litigation avoidance regarding privileged electronic communications and stored data. Adopting a proactive law approach to balance high-quality services and safeguards to the confidentiality required by the LPP-PS responsibilities would meet in form and substance the current legal and ethical standards of the profession (Haapio, 2010; Schartum, 2006, pp. 36–37). Attorneys could

implement diligence programs preventively and promotively, for instance, formulating internal guidelines for digital communication with explanations about how to restrict access to sensitive information, creating protocols to engage with appropriate data governance policies, establishing clear document retention practices, promoting a culture of legal awareness and so on. These steps would reduce legal risks without creating obstacles to the provision of services to clients.

This article will briefly introduce the regulatory and conceptual background of LLP, discuss the privilege of confidentiality in the light of electronic communication and the digital practice and explore whether there are enough legal guarantees for its protection. We draw some conclusions, showing the importance of proactive lawyering strategies in the 21st century (Berger-Walliser, 2012; Haapio, 2010; Pohjonen, 2006; Solarte-Vásquez and Nyman-Metcalf, 2017).

2. Conceptual background and legal framework

2.1 Definitions and relevance of the LPP-PS

The concepts of protected confidentiality, LPP and PS, respond to a universal principle. Each country implements it differently based on national legal traditions, but it is an institution that exists in all legal systems with the purpose of protecting the client and the relationship between the client and their legal counsel. It is typically rooted in constitutional, professional conduct and procedural laws and is regulated by bar associations, professional codes and statutory frameworks (CCBE, 2016).

The scope of confidentiality covers all client communications, documents and information; it generally extends beyond direct legal representation, which means that the protection granted by the privilege or protection continues after the professional relationship ends. It takes shape as a right and/or duty and is associated with enforcement mechanisms ranging from disciplinary actions to criminal penalties in case of inobservance or breach. The severity depends on the given regulatory system and varies from financial fines to professional disqualification.

Narrowly, the LPP or 'attorney–client privilege' denomination originates in English common law. It is defined as legal protection that shields

communications made for legal advice from compelled disclosure. In civil law traditions, PS or legal professional confidentiality diverges in that 'privilege' is absent as a formal legal construct, so it represents a somewhat comprehensive obligation encompassing all client-related information (King, 2001; CCBE, 2016). It is a duty that prohibits disclosure, with exceptional circumstances where it may be legally or ethically mandated; the obligation supports societal interests by preventing harm and precludes the use of confidentiality as a shield for criminal activities. Unlike client-owned privilege in common law, civil law frames confidentiality as a professional conduct obligation that is owed directly to the client and a right to resist information exposure to law enforcement or judicial authorities. We could say that the main distinction thus lies in this systemic approach.

Three compelling reasons illustrate why LPP-PS matters in legal practice. First, it helps support the due process, securing the right to a fair trial and protection against self-incrimination. Secrecy preserves the integrity of the attorney–client relationship and guarantees equal footing in legal disputes. In their absence, fear of disclosure could compromise legal representation, affecting the administration of justice and public trust in the legal system. Second, it materializes the duty of confidentiality, an ethical and professional integrity principle. The independence of the legal profession is reinforced by a clear assurance that lawyers will act in the interests of their clients free from external pressures or coercion. If lacking, legal representation would not be possible or impartial (Thaman and Bachmaier, 2021). Third, LPP-PS upholds constitutional rights beyond the ones linked directly to a fair trial, such as privacy. Confidentiality protects individuals from potential state overreach, unjust surveillance or misuse of "privileged" information. This constitutional dimension refers to the role of LPP-PS as an essential safeguard present in all democratic societies.

2.2 Emerging challenges to LPP-PS and the general regulatory framework

Digital communication technologies challenge legal professional confidentiality, with unprecedented and systemic vulnerabilities. Electronic exchange creates intrinsic risks of interception, compelling lawyers to become "smarter" and develop sophisticated encryption and secure communication strategies. The confidentiality duty now transcends traditional document protection, demanding appropriate measures for digital information management in multiple communication modes and platforms; for example,

they should be vigilant about metadata exposure in digital documents to avoid facilitating unintended revelations. This technological evolution does not relate only to the professional obligation to protect client information's integrity but also to a need for these to be aware of the risks of electronic communication and follow guidance concerning more secure practices.

The main difficulty lies in balancing innovation with the "sacrosanct" principle of legal professional confidentiality, which requires continuous adaptation and technological sophistication from legal professionals to protect client interests in an increasingly complex digital environment. As noted previously, the obligation supports societal interests by preventing harm; however, some jurisdictions explicitly preclude the use of confidentiality as a shield for criminal activities. Regardless of provisions in this respect, electronic communication has increased tensions between privacy and state investigative powers precisely because digital exchange is more susceptible to interference and "hacking". Instances of illegitimate surveillance have been reported in recent years, with governments exploiting digital vulnerabilities, producing a grave decline in democratic guarantees (Banks, 2016; European Parliament, 2022). Such a capacity for constraining civil "spaces" threatens access to justice and makes states less accountable, eroding public trust.

Thus, digital transformation extends the long-standing professional duty to preserve client confidentiality, demanding more careful and technologically informed approaches to the management of sensitive information. Therefore, lawyers must now integrate a certain degree of technological expertise with the established ethical standards, while transforming confidentiality from a static principle to a proactive, dynamic and adaptive professional capability (Barton, 2009).

The preservation of attorney–client confidentiality in the digital age seems to have received more attention in countries like the US, but LLP-PS remains fundamental to the rule of law and is contemplated by international and European Union (EU) legal standards (Kameoka, 2023). European legal systems have adopted a structured and situational approach, balancing confidentiality against public interests and showing ongoing legal refinement. Nordic and Baltic countries demonstrate more flexible interpretations, whereas German and Southern European systems tend to have stricter protection (Helgesson and Mörth, 2018; Bachmaier Winter and Thaman, 2020; Pico i Junoy and López, 2022).

In Europe, various provisions have established confidentiality as a

fundamental safeguard within the scope of human rights and fair trial guarantees. The protection of confidentiality is rooted in the right to private correspondence under Article 8(1) of the *European Convention on Human Rights* and is closely tied to the right to a fair trial under Article 6(1). *The Charter of Fundamental Rights of the European Union* (*EU Charter*) speaks of privacy in Article 7, which specifies the right to private and family life, home and communications and backs up the principle. In addition, Article 47 of the *EU Charter* contemplates the right to legal advice, defence and representation and Article 48(2) upholds the right to a defence.

In sum, the principle of confidentiality could be more clearly understood to have a dual nature as a professional duty for lawyers but not only incumbent to them. It is also a fundamental human right of the client, as recognized in the *Council of Bars and Law Societies of Europe Charter* (*CCBE Charter*) and reinforced by international human rights law (*Charter of Core Principles of the European Legal Profession and Code of Conduct for European Lawyers*, 2013). While the scope, emphasis and application of 'attorney–client privilege' differ depending on the jurisdiction, its purpose to ensure that legal representation is effective, uninhibited and protected from external interference is universal. The confidentiality of communications, documents and information exchanged in the course of legal representation is essential for individual client protection and for upholding the rule of law to preserve the fairness and credibility of democratic legal systems.

We consider that confidentiality qualifies as a general legal principle, already deeply connected to fundamental rights as it is inseparable from legal representation. In the context of new and emerging technologies, it should move from being an ethical obligation for attorneys to uniformly becoming a strict legal requirement to maintain relational and institutional trust (CCBE, 2020). Beyond the traditional content demanding lawyers to refrain from disclosing client-related information unless explicitly authorized (clear, voluntary and unequivocal client expression) through informed consent, the obligation should be promotive of additional commitments to cover the literacies referred to above, responding proactively to current and future needs.

3. Outlining LPP in the light of electronic communication

In 1982, the Court of Justice of the European Union acknowledged LPP under EU law, stating that communications between External European Economic Area-qualified lawyers and their clients were safeguarded, provided that they had the purpose and occurred in the interest of defending clients' legal rights ('AM and S Europe Ltd. v. Commission', 1982). Subsequent rulings further unpacked the extent of professional legal privileges. It was determined that LPP cannot be limited to direct communications between the client and an external attorney, but it should include internal summaries, notes and reports of legal advice received from that legal counsel, as well as documents created exclusively for the purpose of seeking legal support in relation to the rights of defence (e.g., 'Akzo Nobel Chemicals and Akcros Chemicals v. Commission', 2007). Consequently, these limitations should be weighed according to the specific cases. In this respect, an example of interest is 'Akzo Nobel v. Commission', a case stemming from a 2003 antitrust investigation for potential anti-competitive practices that provided the general scope of the LPP in EU law. Documents were seized at Akzo's UK premises in the United Kingdom, including communications between company employees and their *in-house legal counsel*. Even though Akzo Nobel contended with claims of LPP, the European Court of Justice decided against extending the protection to communications with in-house lawyers *in the context of EU competition law investigations*. They stated that in-house lawyers lack the necessary level of independence due to their employment relationship with the company, which could realistically influence their ability to provide impartial legal advice.

Notwithstanding the boundaries established in EU case-law, uncertainty persisted regarding the scope of LPP. Specifically, it was unclear whether this privilege extended to documents and communications related to the exercise of defence rights or to any legal advice. A more recent decision, the Orde van Vlaamse Balies judgment, clarifies that confidentiality of communications (between external counsellors and their clients) concerns communication between clients and European Economic Area-qualified external lawyers, regardless of whether it pertains to the clients exercising their rights of defence; consequently, LPP covers legal advice more broadly ('Orde van Vlaamse Balies and Others v. Vlaamse Regering', 2022). This does not alter the fact that unfounded privilege claims might qualify as an obstruction to the investigation and call for pecuniary sanctions. The same degree of protection is afforded to oral, written and electronic forms.

Similarly, the European Court of Human Rights (ECtHR) adopted a dynamic interpretation of "correspondence" under Article 8 of the European Convention on Human Rights, adapting to technological advancements in communication. The ECtHR's jurisprudence ensures robust protection of privacy rights across various forms of communication, including older electronic methods such as telexes, as seen in 'Christie v. the United Kingdom' (1994); telephone conversations, as in 'P.G. and J.H. v. the United Kingdom' (2001); pager messages, as in 'Taylor-Sabori v. the United Kingdom' (2002); and electronic messages, as recognized in 'Copland v. the United Kingdom' (2007). Additionally, the ECtHR has extended these protections to other electronic data, such as that seized during law office searches, as discussed in 'Wieser and Bicos Beteiligungen GmbH v. Austria' (2007).

The proposed *ePrivacy Regulation*, currently in its First Reading before the Council of the EU, addresses most of the concerns we have commented directly ('Proposal for a Regulation COM/2017/010', 2017). The Regulation is designed to modernize privacy protection in electronic communications, strengthen confidentiality safeguards and, in addition to its role in advocacy, it will become a milestone in European legislation, as it connects with the wider EU purpose of contributing to building its digital ecosystem of trust (European Commission, 2022). Article 5 prohibits third parties from intercepting, monitoring or storing electronic communications data without user consent or a legitimate legal basis. The provision extends from content to metadata to cover information such as sender and recipient identities, timestamps and transmission details in any layer of the text, protecting it from unauthorized access, while Article 6 mentions the circumstances permitting the said data to be processed. The two are general rules on privacy and data protection in electronic communications but are to become *lex specialis* to the norms of the General Data Protection Regulation (GDPR).

Institutions are reshaping confidentiality safeguards in view of pressing circumstances. This is reflected in the stance of the Council of Bars and Law Societies of Europe, asserting that "oral or written information, as well as information obtained electronically, are considered confidential information to which the lawyer's obligation of confidentiality applies" (CCBE, 2016). The Council of the CCBE has consistently emphasized the indispensability of legal professional privilege, advocating for stronger protections in evolving regulatory frameworks.

Furthermore, the ECtHR case-law establishes that the confidentiality of attorney–client communications is not contingent on the situation in

which they occur ('Iliya Stefanov v. Bulgaria', 2008). The duty, privilege or protection is presumed to start from the initial interaction between an attorney and a prospective client and is effective if this first contact is made in person, via telephone, email or video call. Additionally, this obligation does not hinge on whether a formal legal services contract is eventually executed. It extends throughout the entirety of the relationship and ends either by explicit release from the client or on legal grounds, such as a disclosure mandate for failing to prevent a criminal offense.

The Constitutional Court of the Czech Republic arrived at a similar conclusion in the Ruling no. II. ÚS 889/10 of October 25, 2010 (Constitutional Court of the Czech Republic, 2010, para. 25), where it stated that the attorney's obligation to maintain confidentiality basically occurs when the client requests legal services and begins to familiarize the attorney with their legal problem. This is also the case when, after becoming acquainted with the facts, the legal services terminate. This is because anyone can reasonably expect that their communications with an attorney will be privileged and confidential, regardless of how long, productive or intense they were, or the subject matter. Since in the view of the ECtHR, it is unnecessary to distinguish between communications related to representation in civil proceedings or defence or representation in criminal proceedings or communications related to the provision of legal services in general, each of these categories enjoys the same degree of privilege within the meaning of the Convention ('Altay v. Turkey', 2019).

In advocating a proactive approach to LPP-PS concerning electronic communications, we coincide with Pohjonen's (2006) perspective, which sees the value of counting with legal rules, clear procedures and logic as essential regulatory components that might be utilized to varying extents but having more options. It is necessary to diversify when the emphasis of legal practice is on the specific issue at hand, preventing harm, promotive collaboration and solving real-life problems (Pohjonen, 2006), rather than strictly adhering to conventional legal methodologies. This realism is especially useful for the management of new methods of working and relevant to LPP-PS in the digital realm, an area that exemplifies the need for adaptive and pragmatic legal strategies. Law firms that are proactive look forward to increasing client engagement in terms of transparent communication about the security measures safeguarding their information. This helps clients understand and participate in decisions about the tools used and take their own preventive measures. Our approach suggests adhering to confidentiality rules and adjusting to other non-legal requirements to effectively protect legal privilege.

3.1 Reflections about communication privilege in the digital world

We argue that interpreting the norms governing both analogue and digital communications cannot be rigidly formalistic; instead, behavioral standards and other contextual factors have to be acknowledged. Consider the commonplace practice of individuals keeping their mobile phones and other portable devices permanently connected to their work emails, files and other professional resources and what should be the regulatory response to it. On the one hand, even if such practices do not inherently constitute a breach of confidentiality (they may still violate specific privacy guidelines or policies), clients are likely to be uncomfortable with their attorneys carrying hard copies of personal files everywhere or having their information accessible through multi-point access or shared digital folders. On the other hand, accessibility on the go and interoperability are achievements that make work more efficient and improve the provision of legal services. To maintain a balance between contrasting and sometimes incompatible expectations and adherence to strictly growing rules to preserve confidentiality and maintain client trust across digital platforms, attorneys must expand their strategies.

To respect LPP-PS in the digital world, practitioners should resort to being more proactive (Nystén-Haarala, 2006). Proactivity in law serves to be practical and beneficial in all sectors and regulatory levels (Saliternik and Agon, 2024), as this way of approaching rule-making activities and lawyering is broadly associated with anticipatory thinking and basic conflict management and dispute prevention (Haapio, 2006a; 2006b; 'Opinion of the European Economic and Social Committee C 175/26', 2009; Solarte-Vásquez, Järv and Nyman-Metcalf, 2016; Solarte-Vásquez and Hietanen-Kunwald, 2020). If proactive lawyers are skilled at detecting the risks of legal disputes, taking control of potential issues and envisioning solutions, as well as at initiating mitigating of promotive actions rather than reactively responding to failures and shortcomings, all for their clients (Sorsa, 2011; Berger-Walliser, 2012), they could approach their own performance with similar commitments. This forward-thinking strategy may not only pre-emptively, responsively and promotively handle grand legal challenges but in scenarios such as the one at hand on LPP-PS being at stake, end up contributing to the protection of fundamental rights.

There are instances in which the likelihood of a confidentiality breach is high and too common, when data and information are stored on remote servers, the cloud included, and when devices are not secure for data integrity (Bentajer *et al*., 2018).

In public cloud storage systems, the confidentiality of sensitive data continues to represent a critical challenge. Despite the proliferation of technical solutions and techniques aimed at ensuring confidentiality, encryption-based models are the primary means to realistically achieve this objective (Chow *et al*., 2011; Liu *et al*., 2017; Singh and Singh, 2018; Inam *et al*., 2023). More importantly, it is erroneous to assume that cloud storage would be a secure method for storing confidential data if there were guarantees of integrity and confidentiality alone (Rady, Abdelkader and Ismail, 2019). The problem is more complicated from a legal point of view, as storing data in a cloud environment has the repercussion of effectively shifting the data management responsibility to the—cloud—service provider. This results in a reduction in the costs associated with different resources, such as hardware, software and expert maintenance of the system (Makhlouf, 2020; Al-Marsy, Chaudhary and Rodger, 2021, p. 4). However, the data and the execution of database queries are under the control of cloud service providers (Sandhu, 2021, pp. 32–40). Consequently, the primary security concerns associated with outsourcing data or databases to cloud servers are the loss of control over the data by the data owner and the transition of the role of the primary data manager from the data owner to the cloud service provider (Akhtar *et al*., 2021; Ferrari, 2010). In essence, this signifies that the responsibility for managing confidentiality falls on the cloud service provider, evidencing the complicated nature of digital data management. The server itself could potentially engage in malicious activities, such as inserting unauthorized records, altering existing ones or deleting them, affecting the confidentiality of file contents and metadata, with file names and locations. Researchers have grouped the range of threats into four categories: attacks that target the confidentiality of data directly, those that compromise file data integrity, ones designed to manipulate metadata and attacks that enable the unauthorized injection of files into a user's storage to mimic legitimate uploads (Hofmann and Truong, 2024).

One potential solution, among the various more technical, is the use of confidential computing. Confidential computing protects data during processing using trusted execution environments (TEE), which isolate sensitive operations from a broader system. A confidential cloud operates within the public cloud infrastructure, using hardware-based security from CPU vendors (such as Intel SGX, AMD SEV, etc.). The idea is to create encrypted enclaves where data becomes inaccessible to unauthorized entities, *including the cloud provider*, mitigating risks from multi-point access, shared storage and certain modifications, in compliance with confidentiality requirements (Arockiam and Monikandan, 2014).

It is reasonable to question whether attorneys who rely on cloud storage are aware of and whether they would opt for confidential computing in the absence of legal or other normative requirements. The primary reason why cloud storage is chosen is convenience and, in some cases, because it is offered for free; legal practice is primarily a business and any additional security costs directly impact financial considerations. Because of these uncertainties, we maintain that storing confidential information in the cloud is inherently insecure and, given the evolving landscape of cyber threats, may even constitute a breach of legal privilege.

It is not only the outsourcing of data for storage to external entities that presents a potential security risk; the same holds true for the precarious security of the data integrity of devices. One illustrative example is the downloading and use of applications, such as TikTok. The privacy policy for this social platform states that the application will collect the user's date of birth, email address, telephone number, IP address, keystroke patterns or rhythms, activity across devices, search history, settings and other information about the actions they have taken outside the platform (TikTok, 2024). TikTok collects the data using several collection methods, as it has the ability to reach contact lists, access calendars, scan hard drives (including external ones) and geolocate devices on an hourly basis (Touma, 2022). The collection of seemingly insignificant data points can reveal more about users than intended, frequently exceeding reasonable limits. This intrusive data-gathering allowances create access to sensitive information or information that may be confidential. As a result, unrestricted or careless interactions with applications could expose legal professionals to the risk of unintentionally disclosing privileged information.

In sum, the shift of LPP-PS from analogue to digital introduces multiple vulnerabilities, many of which attorneys and clients may overlook. A lack of awareness and competences complicates regulatory enforcement and the handling of 'privilege' breaches in data storage, collection and exposure to new threats. In view of these risks, we need a deeper understanding of how privilege is preserved in a landscape where sensitive information is constantly transmitted and stored. With electronic communication now standard, providers of legal services must develop a forward-thinking approach. This means embedding confidentiality measures into daily practice. Staying ahead, adhering to legal requirements and strengthening professional responsibility are essential to maintaining 'privilege' as a professional and ethical duty, a legal right for the client and a necessity in modern legal work.

In practical terms, proactivity means complying with regulations while considering the interests of all parties and recognizing the benefits of stronger confidentiality measures. Protecting client privilege requires law firms and lawyers to take concrete steps, starting with better control over communication channels and data security.

Client portals and messaging apps should be encrypted, secured with two-factor authentication and protected by strong passwords. Regular updates to security software and operational protocols help defend against cyber threats. Policies must be clear and restrictive, limiting access to sensitive information and ensuring that only those who need it can handle client data. They should also provide guidelines for secure storage and communication, covering everything from document-sharing protocols to internal data management practices.

Ongoing cybersecurity training keeps legal professionals aware of new risks and best practices, helping them adapt to evolving security challenges. By staying ahead of potential threats, firms and practitioners can strengthen confidentiality and maintain trust in their professional responsibilities.

4. Sufficiency of guarantees

As previously stated, to focus on preventing legal issues rather than resolving them after the fact, the legal profession should work toward reducing risks that could compromise privilege and promoting a structured, preventive approach (Haapio, Barton and Corrales Compagnucci, 2021; Bronstein and Solomon, 2021). However, LPP-PS is not a unilateral duty of attorneys, no matter how proactive their strategies may be. The state also has a role in establishing a legal framework that upholds its preservation. To that end, the state must act as a guarantor in the attorney–client relationship, ensuring that the confidentiality of their communications is not only protected, but that attorneys can uphold it without undue external pressures or systemic vulnerabilities. This reflects a positive duty to shape a legal environment that preserves privilege and facilitates its application.

The extent to which national legal frameworks meet this obligation has been contemplated in the jurisprudence of the ECtHR (see 'Petri Sallinen and Others v. Finland', 2005; 'Smirnov v. Russia', 2007; 'Wieser and Bicos Beteiligungen GmbH v. Austria', 2007; 'Iliya Stefanov v. Bulgaria', 2008).

The Court has examined whether national laws offer adequate safeguards to protect attorney–client confidentiality, recognizing its fundamental role in securing the right to a fair trial. The question of the "sufficiency of guarantees under national law" has shaped the ECtHR's decision-making practice, establishing that communication privilege must be upheld through concrete protections rather than only through abstract legal principles.

The ECtHR recently addressed the issue of legal privilege and procedural safeguards in 'Saber v. Norway' (2020). The case did not center on a direct violation of LPP-PS under Article 8(2) of the European Convention on Human Rights but rather on the lack of sufficient predictability in national regulations governing 'privileged' communications. The Court found that Norwegian law lacked explicit procedural provisions concerning the protection of attorney–client confidentiality in criminal proceedings, considering the legal framework inadequate in this regard. The case first surfaced when law enforcement authorities seized the mobile phone of an applicant and created a digital copy of its contents as part of a criminal investigation. The phone also contained communications between the applicant and his attorney in a separate criminal case, which was entitled to the protection of legal privilege under national law. Despite that, law enforcement did not exclude the privileged material from their review.

In response, the applicant sought a court-supervised filter for privileged data, but before it was implemented, a supreme court ruling in a separate case allowed full law enforcement access. The lower court followed suit by analogy, granting unrestricted access to the duplicated data. The applicant contested the decision before the ECtHR, alleging a violation of his right to respect for private life under Article 8 of the Convention. The case justified claims about the lack of procedural safeguards for privileged attorney–client communications in criminal proceedings, exposing a gap that affects the essence of legal privilege.

What follows then is to learn whether, in line with the principle that the protection of information disclosed to an attorney should not depend on the manner of disclosure and that a breach of confidentiality in the analogue world is equally a breach in the digital world, certain scenarios require closer examination. A review of case-law shows that most instances concern attorneys or law firms in a procedural position such as that of an accused or suspect in criminal proceedings. In this regard, the jurisprudence of the Supreme Court of the Czech Republic is especially relevant and offers a valuable perspective that reflects the broader principle that privilege is tied to the nature of the information and its custodian (the attorney) rather than

its physical location (Supreme Court of the Czech Republic, 2015). At this stage, what is clear is that this principle holds, regardless of the medium through which legal communications are conducted (Smejkal, 2015).

5. Conclusion

We examined the concept of LPP-PS and its proactive management in the context of electronic communication. This article discussed how digitalization affects these fundamental safeguards in view of current normative uncertainties and the unresolved challenges posed by new technologies. It explored the risks they pose, the difficulties attorneys face in upholding privilege in digital environments and the extent to which current legal frameworks provide adequate protection.

By looking at the legal developments, theory and case-law, the study demonstrated the need for a more strategic approach to legal practice, one that can place more emphasis on responding to well-researched needs and collaborative risk management. The discussion showed that traditional LPP-PS will apply to digital communication only if deliberate safeguards are in place, requiring legal practitioners and regulators to better understand vulnerabilities. The paper identified remote storage and device security as two major vulnerabilities that complicate the protection of privileged communication. Remote storage raises concerns about data integrity and confidentiality, as responsibility often shifts to third-party service providers whose security measures may not coincide with legal privilege standards. Meanwhile, personal and work devices introduce risks due to shared access, multi-point synchronization and inadequate security controls, making them weak points in 'privileged' or protected exchanges.

Despite these challenges, digital tools offer efficiency and accessibility that legal professionals cannot forgo. We argued that maintaining LPP in the digital age presents unprecedented constraints and calls for proactive measures to strengthen confidentiality, procedural fairness and the protection of attorney–client relationship. Addressing these hurdles is not just a matter of compliance but a fundamental requirement for preserving trust in legal representation. Therefore, we believe that taking legislative or other forms of regulatory action would be a prudent step toward greater legal certainty. Nevertheless, the scope of the work at hand is limited and the options should be further discussed in the wider legal and policy discourse.

Acknowledgements

Ondrej Hamuľák participated in the preparation of this paper as part of the implementation of the research project no. IGA_PF_2024_010 'Forming of Catalogues of Digital Human Rights', funded by the Palacký University Olomouc IGA projects scheme.

Zoltán Gyurász is a graduate of the Faculty of Law of Comenius University in Bratislava. Since 2022, he has been working as an assistant professor at the Institute of Information Technology and Intellectual Property Law, as an international fellow at the Information Society Law Center at the Università degli Studi di Milano and has been part of the Expert Map on the Ethics and Regulation of Artificial Intelligence of the Permanent Commission on the Ethics and Regulation of Artificial Intelligence (CERAI). Since 2023, he has been Of Counsel for NextGen Legal, where he is involved in the application of new technologies. His professional and scholarly work focuses on the regulation of emerging technologies and application issues in artificial intelligence and the Internet of Things. His teaching focuses on legal theory, information technology law and legal informatics.

Ondrej Hamuľák is a senior lecturer at the Faculty of Law, Palacký University Olomouc, Czech Republic, and an adjunct professor of digital constitutionalism at TalTech Law School, Estonia. He specializes in the relations and interactions between EU law and national law, the theoretical impacts of EU membership on state sovereignty, legitimacy and rule of law within the EU, protection of fundamental rights within the supranational system of law and also the EU's regulatory capacity over digital space, the challenges of digital constitutionalism, digital sovereignty and protection of fundamental rights in the realms of the digital age.

Petra Dražová graduated from the Faculty of Law at Comenius University in Bratislava. She is currently an assistant professor at the Institute of Information Technology Law and Intellectual Property Law at the Faculty of Law, Comenius University. Moreover, she completed a long-term research stay at the University of Vienna as part of her doctoral studies. She specializes in criminal procedural law, digital evidence and cybercrime and is an active participant at national and foreign scientific conferences, seminars and workshops.

References

Act No. 221/2006 Coll. of the Slovak Republic on the enforcement of detention and on the amendment of certain laws (2006) 15 March. *Zbierka zakonov*, 78, pp. 1286–1301. Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2006/221/20160701 (Accessed: 10 December 2024).

Act No. 475/2005 Coll. of the Slovak Republic on the execution of a prison sentence and on the amendment of certain laws (2005) 22 September. *Zbierka zakonov*, 191, pp. 4422–4451.

Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A. and Praveen, S. (2021) 'A comprehensive overview of privacy and data security for cloud storage', *International Journal of Scientific Research in Science Engineering and Technology*, 8(5), pp. 113–152. Available at: https://doi.org/10.32628/IJSRSET21852

'Akzo Nobel Chemicals and Akcros Chemicals v. Commission' (2007) Case no. T-125/03; ECLI:EU:T:2007:287, 17 September.

Al-Marsy, A., Chaudhary, P. and Rodger, J.A. (2021) 'A model for examining challenges and opportunities in use of cloud computing for health information systems', Applied System Innovation, 4(1), article 15. Available at: https://doi.org/10.3390/asi4010015

'Altay v. Turkey' (2019) Case no. 11236/06, 9 April. Available at: https://hudoc.echr.coe.int/fre?i=001-192210 (Accessed: 15 December 2024).

'AM and S Europe Ltd. v. Commission of the European Communities' (1982) Case no. 155/79; ECLI:EU:C:1982:157, 18 May.

Arockiam, L. and Monikandan, S. (2014) 'Efficient cloud storage confidentiality to ensure data security', in *2014 International Conference on Computer Communication and Informatics*, Coimbatore, India, 3–5 January, pp. 1–5. Available at: https://doi.org/10.1109/ICCCI.2014.6921762

Bachmaier Winter, L. and Thaman, S.C. (2020) 'A comparative view of the right to counsel and the protection of attorney–client communications', in L. Bachmaier Winter, S.C. Thaman and V. Lynn (eds) *The right to counsel and the protection of attorney-client privilege in criminal proceedings. Ius Comparatum—global studies in comparative law*, 44. Springer, pp. 7–73. Available at: https://doi.org/10.1007/978-3-030-43123-5_2

Banks, W.C. (2016) 'Cyber espionage and electronic surveillance: beyond the media coverage', *Emory Law Journal*, 66(3), p. 513.

Barton, T.D. (2009) *Preventive law and problem solving: lawyering for the future*. Vandeplas Publishing.

Bentajer, B., Hedabou, M., Abouelmehdi, K. and Elfazazi, S. (2018) 'CS-IBE: a data confidentiality system in public cloud storage system', *Procedia Computer Science*, 141, pp. 559–564. Available at: https://doi.org/10.1016/j.procs.2018.10.126

Berger-Walliser, G. (2012) 'The past and future of proactive law: an overview of the development of the proactive law movement', in G. Berger-Walliser and K. Østergaard (eds) *Proactive law in a business environment*. DJØF Publishing, pp. 13–31. Available at: https://ssrn.com/abstract=2576761 (Accessed: 15 December 2025).

Bronstein, J. and Solomon, Y. (2021) 'Exploring the information practices of lawyers', *Journal of Documentation*, 77(4), pp. 1003–1021. Available at: https://doi.org/10.1108/JD-10-2020-0165

'Camenzind v. Switzerland' (1997) Case no. 21353/93, 16 December. Available at: https://hudoc.echr.coe.int/eng?i=001-58125 (Accessed: 15 December 2024).

CCBE (2016) *Model article on confidentiality*. Available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_Postion_Papers/EN_DEON_20161202_Model_Article_on_Confidentiality.pdf (Accessed: 10 December 2024).

CCBE (2020) *CCBE Considerations on the legal aspects of artificial intelligence*. Available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf (Accessed: 10 December 2024).

Charter of Core Principles of the European Legal Profession and Code of Conduct for European Lawyers (2013). Available at: https://www.ccbe.eu/NTCdocument/EN_CCBE_CoCpdf1_1382973057.pdf (Accessed: 10 December 2024).

Chow, S.S.M., Chu, C.K., Huang, X., Zhou, J. and Deng, R.H. (2012) 'Dynamic secure cloud storage with provenance', in D. Naccache (ed) *Cryptography and security: from theory to applications*. Lecture notes in computer science, 6805. Springer, pp. 442–464. Available at: https://doi.org/10.1007/978-3-642-28368-0_28.

'Christie v. the United Kingdom' (1994) Case no. 21482/93, 27 June.

Constitutional Court of the Czech Republic (2010) Ruling no. II. ÚS 889/10, 25 October.

'Copland v. the United Kingdom' (2007) Case no. 62617/00, 3 April. Available at: https://hudoc.echr.coe.int/eng?i=001-79996 (Accessed 15 December 2024).

Corrales Compagnucci, M., Fenwick, M. and Haapio, H. (2019) 'Digital technologies, legal design and the future of the legal profession', in M. Corrales Compagnucci, M. Fenwick and H. Haapio (eds) *Legal tech, smart contracts and blockchain*. Springer, pp. 1–15. Available at: https://doi.org/10.1007/978-981-13-6086-2_1

Dechand, S., Naiakshina, A., Danilova, A. and Smith, M. (2019) 'In encryption we don't trust: the effect of end-to-end encryption to the masses on user perception', in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, Stockholm, Sweden, pp. 401–415. Available at: https://doi.org/10.1109/EuroSP.2019.00037

DiMatteo, L.A., Janssen, A., Ortolani, P., de Elizalde, F., Cannarsa, M. and Durovic, M. (eds) (2021) *The Cambridge handbook of lawyering in the digital age*. Cambridge University Press. Available at: https://doi.org/10.1017/9781108936040

European Commission (2022) *Shaping Europe's digital future: proposal for ePrivacy Regulation*. [Press release] 7 June. Available at: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation (Accessed: 10 December 2024).

European Parliament (2022) *Pegasus and surveillance spyware*. Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf (Accessed: 10 December 2024).

Ferrari, E. (2010) 'Database as a service: challenges and solutions for privacy and security', in *2009 Asia-Pacific Services Computing Conference (APSCC)*, Singapore, pp. 46–51. Available at: https://doi.org/10.1109/APSCC.2009.5394141

Fischel, D.R. (1998) 'Lawyers and confidentiality', *The University of Chicago Law Review*, 65(1), article 1, pp. 1–33.

Gnusowski, M. and Lipiec, S. (2024) 'Silent boundaries: exploring the limits of legal confidentiality in Poland', *International Journal of the Legal Profession*, 31(3), pp. 267–291. Available at: https://doi.org/10.1080/09695958.2024.2401819

Haapio, H. (2006a) 'Business success and problem prevention through proactive contracting', in P. Wahlgren (ed) *A proactive approach. Scandinavian studies in law*, 49. Stockholm: Stockholm Institute for Scandinavian Law, pp. 21–34. Available at: https://scandinavianlaw.se/pdf/49-2.pdf (Accessed: 10 December 2024).

Haapio, H. (2006b) 'Introduction to proactive law: a business lawyer's view', in P. Wahlgren (ed) *A proactive approach. Scandinavian studies in law*, 49. Stockholm: Stockholm Institute for Scandinavian Law, pp. 149–194. Available at: https://scandinavianlaw.se/pdf/49-9.pdf (Accessed: 10 December 2024).

Haapio, H., Barton, T.D. and Corrales Compagnucci, M. (2021) 'Legal design for the common good: proactive legal care by design', in M. Corrales Compagnucci, H. Haapio, M. Hagan and M. Doherty (eds) *Legal design: Integrating business, design and legal thinking with technology*. Cheltenham: Edward Elgar Publishing, pp. 56–81. Available at: https://doi.org/10.4337/9781839107269.00011

Helgesson, K.S. and Mörth, U. (2018) 'Client privilege, compliance and the rule of law: Swedish lawyers and money laundering prevention', *Crime, Law and Social Change*, 69, pp. 227–248. Available at: https://doi.org/10.1007/s10611-017-9753-8

Hietanen-Kunwald, P. and Haapio, H. (2021) 'Effective dispute prevention and resolution through proactive contract design', *Journal of Strategic Contracting and Negotiation*, 5(1–2), pp. 3–23. Available at: https://doi.org/10.1177/20555636211016878

Hofmann, J. and Truong, K.T. (2024) 'End-to-end encrypted cloud storage in the wild: a broken ecosystem', in *CCS '24: Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, pp. 3988–4001. Available at: https://doi.org/10.1145/3658644.3690309

'Iliya Stefanov v. Bulgaria' (2008) Case no. 65755/01, 22 May. Available at: https://hudoc.echr.coe.int/eng?i=001-86449 (Accessed: 15 December 2024).

Inam, M.A., Chen, Y., Goyal, A. *et al.* (2023) 'SoK: history is a vast early warning system: auditing the provenance of system intrusions', in *2023 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA. IEEE, pp. 2620–2638. Available at: https://doi.org/10.1109/SP46215.2023.10179405

Jones, E., Ryan, F., Thanaraj, A. and Wong, T. (2021) *Digital lawyering: technology and legal practice in the 21st century*. Routledge. Available at: https://doi.org/10.4324/9780429298219

Kameoka, E. (2023) 'History of LPP', in *Legal professional privilege in EU competition investigations*. Edward Elgar Publishing, pp. 29–38. Available at: https://doi.org/10.4337/9781803922782.00011

King, B.A. (2001) 'Preserving the attorney-client privilege in the corporate environment', *Alabama Law Review*, 53(2), pp. 621–638.

'Klaas v. Germany' (1993) Case no. 15473/89, 22 September. Available at: https://hudoc.echr.coe.int/eng?i=001-57826 (Accessed: 15 December 2024).

'Kopp v. Switzerland' (1998) Case no. 23224/94, 25 March. Available at: https://hudoc.echr.coe.int/eng?i=001-58144 (Accessed: 15 December 2024).

Liu, H., Mu, Y., Zhao, J., Xu, C., Wang, H., Chen, L. and Yu, Y. (2017) 'Identity-based provable data possession revisited: security analysis and generic construction', *Computer Standards & Interfaces*, 54(1), pp. 10–19. Available at: https://doi.org/10.1016/j.csi.2016.09.012

Makhlouf, R. (2020) 'Cloudy transaction costs: a dive into cloud computing economics', *Journal of Cloud Computing*, 9(1), article 1. Available at: https://doi.org/10.1186/s13677-019-0149-4

Nystén-Haarala, S. (2006) 'Contract law and everyday contracting', in P. Wahlgren (ed) *A proactive approach. Scandinavian studies in law*, 49. Stockholm: Stockholm Institute for Scandinavian Law, pp. 263–268. Available at: https://www.scandinavianlaw.se/pdf/49-15.pdf (Accessed: 15 October 2024).

'Opinion of the European Economic and Social Committee (EESC) on 'The proactive law approach: a further step towards better regulation at EU level" (2009) *Official Journal* C 175/26, 28 July. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:175:0026:0033:EN:PDF (Accessed: 15 December 2024).

'Orde van Vlaamse Balies and Others v. Vlaamse Regering' (2022) Case no. C-694/20; ECLI:EU:C:2022:963, 8 December. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62020CJ0694 (Accessed: 15 December 2024).

'P.G. and J.H. v. the United Kingdom' (2001) Case no. 44787/98, 25 September. Available at: https://hudoc.echr.coe.int/eng?i=001-59665 (Accessed: 15 December 2024).

'Petri Sallinen and Others v. Finland' (2005) Case no. 50882/99, 27 September. Available at: https://hudoc.echr.coe.int/eng?i=001-70283 (Accessed: 15 December 2024).

Pico i Junoy, J. and López, J.A.A. (2022) 'Private communication between lawyers as evidence in a judicial process: a comparative journey', *The International Journal of Evidence & Proof*, 26(1), pp. 61–80. Available at: https://doi.org/10.1177/13657127211055232

Pohjonen, S. (2006) 'Proactive law in the field of law', in P. Wahlgren (ed) *A proactive approach. Scandinavian studies in law*, 49. Stockholm: Stockholm Institute for Scandinavian Law, pp. 53–70. Available at: https://www.scandinavianlaw.se/pdf/49-4.pdf (Accessed: 12 September 2024).

'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final' (2017) EUR-Lex. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 (Accessed: 10 December 2024).

Rady, M., Abdelkader, T. and Ismail, R. (2019) 'Integrity and confidentiality in cloud outsourced data', *Ain Shams Engineering Journal*, 10(2), pp. 275–285. Available at: https://doi.org/10.1016/j.asej.2019.03.002

'Saber v. Norway' (2020) Case no. 459/18, 17 December. Available at: https://hudoc.echr.coe.int/fre?i=001-206519 (Accessed: 15 December 2024).

Saliternik, M. and Agon, S.S. (2024) 'Proactive international law', *Hastings Law Journal*, 75(3), p. 661. Available at: https://repository.uclawsf.edu/hastings_law_journal/vol75/iss3/4 (Accessed: 10 December 2024).

Sandhu, A.K. (2021) 'Big data with cloud computing: discussions and challenges', *Big Data Mining and Analytics*, 5(1), pp. 32–40. Available at: https://doi.org/10.26599/BDMA.2021.9020016

Schartum, D.W. (2006) 'Introduction to a government-based perspective on proactive law: a proactive approach', in P. Wahlgren (ed) *A proactive approach. Scandinavian studies in law*, 49. Stockholm: Stockholm Institute for Scandinavian Law, pp. 35–51. Available at: https://www.scandinavianlaw.se/pdf/49-3.pdf (Accessed: 15 December 2024)

Singh, N. and Singh, A.K. (2018) 'Data privacy protection mechanisms in cloud', *Data Science and Engineering*, 3(1), pp. 24–39. Available at: https://doi.org/10.1007/s41019-017-0046-0

Smejkal, V. (2015) 'Ochrana dat advokátů v elektronických úložištích', *Bulletin advokacie*, (3), pp. 15–22.

'Smirnov v. Russia' (2007) Case no. 71362/01, 7 June. Available at: https://hudoc.echr.coe.int/eng?i=001-80953 (Accessed: 15 December 2024).

Solarte-Vásquez, M.C. and Hietanen-Kunwald, P. (2020) 'Transaction design standards for the operationalisation of fairness and empowerment in proactive contracting', *International and Comparative Law Review*, 20(1), pp. 180–200. Available at: https://doi.org/10.2478/iclr-2020-0008

Solarte-Vásquez, M.C., Järv, N. and Nyman-Metcalf, K. (2016) 'Usability factors in transactional design and smart contracting', in T. Kerikmäe and A. Rull (eds) *The future of law and eTechnologies*. Springer International Publishing, pp. 149–176. Available at: https://doi.org/10.1007/978-3-319-26896-5_8

Solarte-Vásquez, M.C. and Nyman-Metcalf, K. (2017) 'Smart contracting: a multidisciplinary and proactive approach for the EU digital single market', *Baltic Journal of European Studies*, 7(2), pp. 208–246. Available at: https://doi.org/10.1515/bjes-2017-0017

Sorsa, K. (2011) *Proactive management and proactive business law: a handbook*. Turku University of Applied Sciences.

Supreme Court of the Czech Republic (2015) Opinion no. Tpjn 306/2014, Collection of Court Decisions and Opinions under no. R 35/2015.

'Taylor-Sabori v. the United Kingdom' (2002) Case no. 47114/99, 22 October. Available at: https://hudoc.echr.coe.int/eng?i=001-5879 (Accessed: 15 December 2024).

Thaman, S.C. and Bachmaier, L. (2021) 'Attorney-client confidentiality as a fair trial right in criminal proceedings', in *General reports of the XXth General Congress of the International Academy of Comparative Law – Rapports généraux du XXème Congrès général de l'Académie internationale de droit comparé*. Springer International Publishing, pp. 589–610. Available at: https://doi.org/10.1007/978-3-030-48675-4_21

TikTok (2024) 'Privacy policy'. Available at: https://www.tiktok.com/legal/page/eea/privacy-policy/en (Accessed: 10 December 2024).

Touma, R. (2022) 'TikTok has been accused of 'aggressive' data harvesting. Is your information at risk?' *The Guardian*, 19 July. Available at: https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk (Accessed: 10 December 2024).

'Wieser and Bicos Beteiligungen GmbH v. Austria' (2007) Case no. 74336/01, 16 October. Available at: https://hudoc.echr.coe.int/eng?i=001-82711 (Accessed: 15 December 2024).

'X v. the United Kingdom' (1978) Case no. 7215/75, 12 October. Available at: https://hudoc.echr.coe.int/eng?i=001-57602 (Accessed: 15 December 2024).