https://doi.org/10.38044/2686-9136-2020-1-2-41-52

ARTICLES

PRIVATE LIFE AND SURVEILLANCE IN A DIGITAL ERA: HUMAN RIGHTS IN EUROPEAN PERSPECTIVE

Roman V. Prudentov

Freshfields Bruckhaus Deringer LLP
65, Fleet str., London, UK, EC4Y 1HS

Abstract

This paper focuses on identifying key legal considerations and developments in the area of surveillance in Europe in human rights, with its emphasis on the jurisprudence of the European Court of Human Rights. The aim of this research was to enhance and align law and practices in this area in Russia and Europe. The author analysed the core and most novel Court cases that may be applicable to the subject matter, including by analogy, as well as the latest research in this area. This paper considers, *inter alia*, ability to challenge relevant law and practices *in abstracto*, legitimate aims justifying interference, the requirements for the relevant laws, fetters to authorities' discretion on surveillance matters, and appropriate nature of supervision by authorities and the scope of their powers, as well as certain other safeguards. This paper also discusses interactions and balances between freedom and security, modern approaches taken by the EU and the US, and tensions on pervasive surveillance matters. This paper reveals that, in a COVID-19 world, with those privacy issues that arise from the "track and trace" system and similar practices having already been widely scrutinised by the courts, it is possible to fight COVID-19 through surveillance methods with minimum interference with human rights. Key considerations outlined in this paper are pertinent to all sorts of surveillance features in the modern world. This paper should serve as an impetus for enhancing human rights protection through case law and legal framework in this area, with a view to strengthen democratic values without compromising health and safety concerns.

Keywords

surveillance, secret measures, interception, private life, foreseeability, freedom

Conflict of interest The author declares no conflict of interest.

Financial disclosure The study had no sponsorship.

For citation Prudentov, R. V. (2020). Private life and surveillance in a digital era: Human rights in European perspective. *Digital Law Journal, 1*(2), 41–52. https://doi.org/10.38044/2686-9136-2020-1-2-41-52

Submitted: 10 Jun. 2020, accepted: 12 Jul. 2020, published: 20 Jul. 2020

СТАТЬИ

ЧАСТНАЯ ЖИЗНЬ И СЛЕЖКА В ЦИФРОВУЮ ЭПОХУ: ПРАВА ЧЕЛОВЕКА В ЕВРОПЕЙСКОЙ ПЕРСПЕКТИВЕ

Р.В. Прудентов

Фрешфилдс Брукхаус Дерингер ЛЛП
EC4Y 1HS, Великобритания, Лондон, Флит стрит, 65

Аннотация

Данная статья направлена на выявление основных юридических проблем и эволюции вопросов слежки в Европе в контексте прав человека, с акцентом на практику Европейского Суда по правам человека. Целью исследования является совершенствование и синхронизация правовой материи и правоприменительной практики в данной сфере в России и Европе. Автор проанализировал фундаментальные и самые последние решения Суда, которые могут быть применимы к рассматриваемой тематике, в том числе по аналогии, а также недавние исследования в данной сфере. Данная статья рассматривает, помимо прочего, возможность оспаривания *in abstracto* соответствующего законодательства и практики его применения, законные цели, оправдывающие вмешательство, требования к соответствующему законодательству, ограничения усмотрения властей по вопросам слежки, надлежащий характер органов надзора и объем их полномочий, а также некоторые иные гарантии. Данная статья также обсуждает взаимодействие и баланс между свободой и безопасностью, современные подходы и натянутые отношения ЕС и США по распространенным вопросам слежки. Настоящая статья показывает, что в мире COVID-19 вопросы защиты частной жизни, возникающие в связи с "track and trace" и похожими практиками, уже глубоко исследованы судами, и борьба с COVID-19 возможна через методы слежки с минимальным вмешательством в права человека. Основные проблемы, затронутые в данной статье, применимы к любым формам слежки в современном мире. Данная статья должна служить стимулом для усиления защиты прав человека с помощью судебной практики и правового поля в рассмотренной сфере с целью укрепления демократических ценностей без ущерба здоровью и безопасности.

Ключевые слова

слежка, негласные меры, перехват информации, частная жизнь, предсказуемость, свобода

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имело спонсорской поддержки.
Для цитирования	Прудентов, Р. В. (2020). Частная жизнь и слежка в цифровую эпоху: права человека в европейской перспективе. *Цифровое право, 1*(2), 41–52. https://doi.org/10.38044/2686-9136-2020-1-2-41-52

Поступила: 10.06.2020, принята в печать: 12.07.2020, опубликована: 20.07.2020

Introduction

It has become increasingly common to speak of the emergence of a surveillance society. Dataveillance, CCTV in public areas, and police officers armed with video cameras at public gatherings form an integral part of our living, with governments and various companies gathering large amounts of personal information and, to some extent, knowing us better than our friends and family.

Governments, civil society, tech companies, and cyber-criminals are constantly involved in an ongoing fight for our data, which is approached through powers, civil rights, revenues, and criminal activities, respectively. By way of mere example, in recent years all over the world, use of encryption in various forms of digital communications has exploded, with governments engaging in a public battle over access to encryption codes and contents of communications with smartphone makers and app developers. Most such battles have proven successful for governments, reinforcing serious privacy and political concerns, but also facilitating international efforts in combating terrorism, drugs, weapons, money trafficking, and other crimes.

On account of the European Convention on Human Rights and other similar pieces of law around the world on national and supranational levels, all surveillance activities, regardless of their justification, should be scrutinised in terms of their cost to personal and political freedom, as well as in maintaining democratic values. Notably, the most constant thing in life is change, whereas law (including law-making and law enforcement) is generally conservative, slow, and incremental by its very nature: it takes time to craft, and it quickly becomes outdated in the face of rapid technological and social change (Goold, 2010). These concerns prove topical in the digital area of life in general and surveillance in particular; that fact makes this paper pertinent to several new dimensions of surveillance practices addressed herein.

The European Court of Human Rights (hereinafter the "Court") has contributed greatly to the development of a legal framework for surveillance. The influence and authority of the Court is universally acknowledged, and its case law is prone to adapt (albeit sometimes belatedly) to various social and technological changes. Notwithstanding notorious political pitfalls, the Court's jurisprudence plays a remarkable role in providing the impetus for implementing best practices in a human rights context in Europe, including in the areas of respect for the private life and surveillance.

This paper focuses on identifying key legal considerations and profound human rights law developments in the area of surveillance in Europe (with emphasis on the Court's jurisprudence), with the aim to facilitate the enhancement of this regime in Russia and elsewhere in the world.

Methodology

This paper focuses on the jurisprudence of the Court on several pervasive topics that should be considered by lawmakers and practitioners in the course of applying, enforcing, challenging, or defending various surveillance measures in different circumstances. The choice of case law for analysis was based on author's experience in teaching ECHR law, numerous Court decisions, and commentaries by multiple scholars and practitioners. The format of this paper naturally circumvents detailed analyses and discussions of many topics, each of which may warrant an entire research article. By the same token, selected highlights of international legal considerations and suchlike surrounding modern surveillance human rights issues were chosen based on their timeliness and pivotal nature,

each deserving (and gaining) separate scientific discussions. The above factors contributed to the use of comparative (involving critical analysis of different bodies of law considered by the Court), empirical (involving designing and analysing key legal issues arising in the surveillance context), and doctrinal (involving analysis of the letter of the Court's case law) legal research methodology.

Results

Interference with Private Life

It goes without saying that surveillance can invade a person's private space. Whether or not surveillance interferes with "private life" depends on the circumstances. To set the scene, the Court has consistently emphasised that "private life" is a "broad concept not susceptible to exhaustive definition"[1] and interpreted this notion in various instances. The surveillance issues discussed in this paper concern two primary categories of interest within 'private life' decisions: freedom from interference with physical and psychological integrity, plus the collection and disclosure of information.

The Court acknowledged that the monitoring of an individual's actions in a public place does not, as such, give rise to any interference with that individual's private life, but the recording and subsequent use of the data (and the systematic or permanent nature of the record) may give rise to such considerations[2]. For instance, in 2003, the disclosure of the CCTV footage showing an applicant's attempted suicide to the media constituted a disproportionate and unjustified interference with the applicant's private life[3].

Importantly in the current circumstances, the Court recently recognised that non-covert surveillance in public may also constitute an interference with private life. This was in connection with video surveillance in a university amphitheatre, where professors interact with students and thus develop mutual relations and construct their social identities[4].

The Court accepted that GPS surveillance is less intrusive than other methods of visual or acoustical surveillance, but nevertheless found that GPS surveillance and the processing and use of the data obtained thereby amounts to an interference in private life[5].

Challenge *in Abstracto*

As a matter of fact, it may be difficult for a person to prove that their communications have been intercepted, or that they have been subject to surveillance, given the very secrecy of these activities. Considering this, the Court ruled that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or laws permitting such measures, without having to allege that such measures were in fact applied to them. In other words, in cases concerning secret measures, the Court has allowed individuals the right to challenge a law *in abstracto*[6].

At a later stage, the Court expanded this, claiming it applies only where there are no effective domestic remedies, and thus a widespread suspicion and concern among the general public that

1 *Peck v. the United Kingdom*, ECHR (2003)
2 *Peck*, 2003
3 *Peck*, 2003
4 *Antović and Mirković v. Montenegro*, ECHR (2017)
5 *Uzun v. Germany*, ECHR (2010)
6 *Klass and Others v. Germany*, ECHR (1978)

secret surveillance powers are being abused cannot be said to be justified[7]. In that context, the effectiveness of remedies is genuinely undermined by the absence of a requirement to notify the subject of interception, or an adequate possibility of requesting and obtaining information about secret measures from the authorities[8]. The scope of the legislation permitting secret surveillance measures should also be examined to ascertain whether the applicant could possibly be affected by it.

Otherwise, where effective remedies pertaining to secret measures exist, applicants must meet a fairly low test of demonstrating that they are "potentially at risk of being subjected to such measures"[9].

Legitimate Aims

Surveillance — or other secret measures amounting to interfering with the right to respect for private life, home or correspondence — may be justified by reference to the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others, as per Article 8 (§ 2) of the European Convention on Human Rights. The Court has considered various legitimate aims on many occasions.

One of the illustrative cases herein involved storage of information, for some of the above purposes, on the secret police register, pertaining to the applicants' private lives. It was kept on record as bomb threats made in 1990 by the first applicant and certain other persons were relevant, and proved sufficient reasoning as regards the aim of preventing disorder or crime. By contrast, no legitimate aims described above could be validly asserted in connection with the continued storage of the information concerning (i) the second applicant's participation in a political meeting in Warsaw in 1967, (ii) the third and fourth applicants' membership of the Marxist-Leninist (Revolutionaries) Party, and (iii) an allegation that the fifth applicant had advocated violent resistance to police control during demonstrations in 1969[10].

Necessity

More than 40 years ago, when considering these matters for the first time, the Court already acknowledged that democratic societies found themselves "threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able ... to undertake the secret surveillance of subversive elements operating within its jurisdiction". On this basis, the Court accepted that "the existence of some legislation granting powers of secret surveillance ... is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime"[11].

Therefore, domestic legislature enjoys a certain (but not unlimited) discretion as concerns the fixing of the conditions and procedures under which the system of secret surveillance is to be operated. However, such a law poses a risk of "undermining or even destroying democracy on the ground of defending it", and so states may not adopt whatever measures they deem appropriate. There must be "adequate and effective guarantees against abuse" implemented, depending on the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the

7 *Kennedy v. the United Kingdom*, ECHR (2010)
8 *Roman Zakharov v. Russia*, ECHR (2015)
9 *Roman Zakharov v. Russia*, ECHR (2015)
10 *Segerstedt-Wiberg and others v. Sweden*, ECHR (2006)
11 *Klass*, 1978

authorities competent to permit, carry out, and supervise such measures, and the kind of remedy provided by national law (*Klass and Others v Germany*, 1978).

Notably, with respect to GPS surveillance, the purpose and necessity still need to be considered. Such requirements were deemed satisfied, for example, in a 2010 case, where the investigators had first attempted measures which interfered less with private life, and only then, within three months, then conducted GPS surveillance (and essentially only at weekends, and when the suspect was travelling in his accomplice's car); this was in connection with very serious crimes (attempted murders of politicians and civil servants by bomb attacks)[12].

Legality

Whereas surveillance measures were originally analysed from the perspective of necessity (see above), the issue was subsequently considered in the context of the overlapping notion of legality, i.e. that such measures should be applied "in accordance with the law", meaning, generally, a sufficiently clear and precise legal and procedural framework is in place.

First, the impugned measure should have some basis in domestic law and be compatible with the rule of law, such that the law must thus meet quality requirements: it must be accessible to the person concerned and its effects should be foreseeable[13]. These requirements are not met where, at the very least, surveillance is regulated merely by administrative practice, the details of which are not published, so that the Court is unable to say "with any reasonable certainty" what powers are incorporated in legal rules and what elements remain within the discretion of the executive[14]. It is worth mentioning here a recent (and patently outrageous) Turkish case where the judiciary failed to follow ("flagrantly failed to observe") even the basic requirements of the law when ordering the relevant interception. Such approach is obviously unacceptable[15].

The "foreseeability" element in the context of surveillance measures bears a specific connotation. A person should not be able to foresee when the authorities are likely to intercept their communications. On this basis, there should be no rule providing for advance warning in relation to surveillance, where to do so would threaten the object of such surveillance[16]. It is evident, nevertheless, that the executive's secret exercise of powers may be arbitrary. Therefore, the Court established that the law must be sufficiently clear to adequately indicate the circumstances in which, and the conditions on which, public authorities are empowered to resort to any such measures[17].

Discretion and Supervision

Given that the implementation of secret surveillance measures is not open to scrutiny by the individuals concerned nor the public at large, the competent authorities (i.e., the executive or a judge) should not enjoy unfettered powers, and the law should indicate the scope of their discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference[18]. Those provisions of the law should have a binding force circumscribing discretion in the application of such measures (*Valenzuela Contreras v Spain*, 1998).

---

12 *Uzun*, 2010

13 *Malone v. the United Kingdom*, ECHR (1984); *Rotaru v. Romania*, ECHR (2000); *Kennedy*, 2010

14 *Malone*, 1984

15 *Mustafa Sezgin Tanrikulu v. Turkey*, ECHR (2017)

16 *Mersch and Others v. Luxembourg*, ECHR (1985)

17 *Malone*, 1984; *Leander*, 1987; *Rotaru*, 2000

18 *Malone*, 1984; *Leander*, 1987

The rule of law also implies that any interference by the executive authorities should be subject to effective control by democratic and/or independent institutions, which should normally be assured by the judiciary (at least at the last resort), with judicial control offering the best guarantees of independence, impartiality, and proper procedure. Supervision by non-judicial bodies may be acceptable where such bodies are independent and are vested with sufficient powers and competence[19].

Supervision of the English RIPA regime[20] was considered satisfactory, and it may be treated as an example of acceptable supervision arrangements that are worth highlighting here for reference. First, intercepting agencies were required to keep detailed records of interception warrants that were periodically reviewed by them and, where appropriate, by the Secretary of State. Second, an independent (of the executive and the legislature) office of the Interception of Communications Commissioner was established for overseeing the general functioning of the surveillance regime and the authorization of interception warrants in specific cases. The Commissioner reported annually to the Prime Minister, and his report was laid before Parliament. In addition, any person who suspected interception of their communications could apply to the Investigatory Powers Tribunal (hereinafter "IPT"), with it also being an independent and impartial body that has adopted its own rules of procedure. Both the Commissioner and the IPT had access to all relevant (including closed) documents and material, and each of them comprised of persons who hold or have held high judicial office (or, in the case of the IPT, have been experienced lawyers). The IPT also had powers to quash any interception order, to require the destruction of intercepted material, or to order compensation to be paid. Both the Commissioner's report and the IPT's legal rulings were available to the public, and thus open to public scrutiny[21].

By contrast, the Court found that no meaningful supervision regime existed in Russia. Logging or recording interceptions was prohibited, which made it impossible for any supervising authority to discover unlawful interceptions. At the same time, the law enforcement authorities were technically able to directly intercept all communications. Moreover, judicial supervision was limited to the initial authorization stage, with subsequent supervision being entrusted to the President, Parliament, the Government, the Prosecutor General, and competent lower-level prosecutors. For the first three bodies, there were no regulations or instructions describing the scope, procedures, and conditions for their review, or for remedying the breaches. In theory, there was a legal framework for some supervision by prosecutors of secret surveillance measures; however, prosecutors lacked independence, given that they were appointed and dismissed by the Prosecutor General after consultation with the regional executive authorities, and noting that they also gave approval to requests for interceptions. Moreover, the scope of their supervision was limited; information about the security services' undercover agents, and about the tactics, methods, and means used by them, was outside the scope of prosecutors' supervision. Interceptions performed by the FSB in the sphere of counter-intelligence could be inspected only following an individual complaint that was unlikely to ever be lodged (given that individuals were not notified of interceptions). Supervisory activities were not open to public

[19] *Klass*, 1978

[20] This was the regime established under the Regulation of Investigatory Powers Act 2000. Note that this regime has been substantially modified over time; notably, an office of the Interception of Communications Commissioner was repealed by the Investigatory Powers Act 2016, s 240(1)(a) and (2)(a), with effect from 1 September 2017. The relevant review powers now lie with the Investigatory Powers Commissioner. Investigatory Powers Act, Part 8 (2016).

[21] *Kennedy*, 2010

scrutiny in Russia, as prosecutors' biannual reports were confidential documents that were submitted to the Prosecutor General only and contained statistical information only[22].

On a similar prominent case related to members of a non-governmental 'watchdog' organisation voicing criticism of the Hungarian government, the system of supervision (that was eminently political, and carried out by the Minister of Justice) was found inadequate. Although this Minister was formally independent of both the police force and of the Minister of Home Affairs, he was "inherently incapable of ensuring the requisite assessment of strict necessity"[23].

In short, the level of scrutiny over the surveillance control systems would depend on the scope, manner, and origins of surveillance; furthermore, however, generally speaking, the independence of the oversight body, its jurisdiction, its power to access data, and its power to effective reactions are pivotal in ensuring the rule of law, and hence the compatibility of surveillance with the principles of human rights (Malgieri & De Hert, 2017).

Other Safeguards

More specifically, a few minimum safeguards should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception or another surveillance order; a definition of the categories of people subject to surveillance; a limit on the duration of surveillance; the mandatory procedure for examining, using, sharing, storing, or destroying the data obtained; the precautions to be taken when communicating the data to others; and the circumstances in which recordings may or must be destroyed or otherwise extinguished[24].

In addition to all of the above, appropriate safeguards may also involve "provisions designed to reduce the effects" of any interference "to an unavoidable minimum", and certain limits on the use of information (such as public prosecution and obtaining of citizenship)[25].

The approach taken by Western democracies proves that the publication of information concerning rules and procedures for dealing with intercepted material and other surveillance projects is essential in a democratic society, and should not be viewed as damaging the efficacy of the intelligence-gathering system or otherwise giving rise to a security risk. The German Law of 13 August 1968 on restrictions on the secrecy of mail, post, and telecommunications (hereinafter the "G10 Act") is a widely cited example of democratic enactments in this area. In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order, and which search terms had to be listed in the monitoring order. Moreover, the rules on storing and destroying data obtained through strategic monitoring were set out in detail: the authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them, and if that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked, with the destruction having to be recorded in minutes and, in certain cases, having to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions governing the transmission, retention, and use of data obtained through the interception of external communications[26].

---

22 *Roman Zakharov*, 2015

23 *Szabó and Vissy v. Hungary*, ECHR (2016)

24 *Huvig v. France*, ECHR (1990); *Liberty and Others v. United Kingdom*, ECHR (2008); *Roman Zakharov*, 2015

25 *Leander v. Sweden*, ECHR (1987)

26 *Weber and Saravia v. Germany*, ECHR (2006); *Liberty*, 2008

Discussion

Freedom and Security

It is important to recognise the political value of privacy. Reagan argued that privacy is essential to the maintenance of democracy, primarily because it ensures that citizens are able to hold elected governments to account and place limits on the expansion of the state. Unfettered mass surveillance may have a chilling effect on political discourse, creating fears of reprisal. At all times, various forms of surveillance (starting from the census) can be justified on the grounds of safety and security, or as a means to improve public service. These justifications are sometimes treated as mere excuses for an expansion in state power (Goold, 2010).

It is not only governments and secret agencies with the capabilities to possess and produce profoundly pervasive and complicated data mining and information collection, storage, and shaping of surveillance information, but also (and perhaps to a larger extent) the big tech companies, constituting a quarter of the entire US stock market: Amazon, Apple, Google, Facebook, and Microsoft. The desire for security is driving the rampant expansion of government powers of colossal surveillance activity. It is hard to ascertain whether it is possible to say certain things on a cell phone without running afoul of the surveillance systems. The fine balance between freedom and security is uncertain and possibly eventually unsustainable, given rapid changes in the modern world. However, the question is whether this emanates into the concept of a "post democratic" state or not (Barnhizer, 2013).

EU and US: Modern Approaches and Tensions

In the early 21st century, much debate and controversy arose from the terror attacks and the subsequently increased counter-terrorism powers. In Europe, the Data Retention Directive was rapidly adopted; from this, metadata derived from the communications of every individual or legal entity within the EU must be retained and made available for the purpose of "the investigation, detection and prosecution of serious crime", as defined by each Member State (by way of background, "metadata" concerns the context (as opposed to the content) of communication, revealing the 'who', the 'when', the 'what' (type of communication), the 'how' (the device used), and the 'where', combined with results from the aggregation and analysis of this). The revelations made by Edward Snowden in 2013 prompted a global debate concerning the rapid pace of technological developments in the area of communications surveillance and the related privacy implications. Ultimately, in 2014, the Court of Justice of the European Union quashed the aforementioned Data Retention Directive, based on its disproportionate scope (applying to all persons and all means of communication), the length of the retention period, and a lack of provisions ensuring the 'irreversible destruction' of the data or control by an independent authority (Ni Loideain, 2015).

In the US, public privacy discussions in the area of surveillance focus on the need to demonstrate probable cause (or solid grounds and articulable suspicion) before acting, and on whether surveillance constitutes a "search" or "seizure" in the context of the Fourth Amendment (Slobogin, 2002). At the same time, US authorities are notorious for using personal data arbitrarily.

To this end, privacy concerns more and more often are becoming the subject of substantive tensions amongst these countries, and are creating problems for both businesses and government security. For instance, the latest Judgement of the Court of Justice of the European Union quashed the core basis of data transfers from the EU to the US, on the grounds that the limitations on the protection of personal data arising from the US domestic law on the access and use by US public

authorities of such data are not circumscribed by the principle of proportionality, as the surveillance programmes are not limited to what is strictly necessary. In addition, data subjects do not enjoy actionable rights before the courts against the US authorities[27].

Role of Regulators

It has generally been established that private-sector surveillance shapes individuals' reasonable expectations of privacy, and hence regulation of the private sector has effects on the government as a surveillant. On this basis, regulators dealing with private-sector surveillance also affect the stance on civil liberties of the state. Such regulators should make companies more responsible for their surveillance technologies, increase the quality of consent necessary to engage in surveillance, and make companies liable for using certain surveillance techniques and systems (Hoofnagle, 2017).

Lifelogging

Many ideas emerge around the subject of this paper. One worth noting relates to the idea of "lifelogging", referring to a comprehensive archive of an individual's quotidian existence, created with the help of pervasive computing technologies. This is a sort of "time capsule" containing digital archives of a person's lifetime as a means to remember, digest, and possibly use for the best. The emerging interest in this concept obviously stems from the growing capacity to store and retrieve traces of one's own life via digital devices. It is characterized as a combination of personal "sousveillance" (to the extent that it captures data from the perspective of oneself) and surveillance (to the extent it captures data about others that interact with the first person). The resulting memory (in general and in its physical sense) can be a very good thing used for entertainment, sharing, or improving health or personal insight. It may also generate substantive privacy concerns as discussed in this paper (which may be eliminated by ethical limitations and design parameters), not to mention other troubling implications, such as mental and moral health hazards (Allen, 2008).

COVID-19 Considerations

Most recently, digital technologies are being innovatively adopted to combat COVID-19, with various forms of surveillance being exploited (including CCTV, cellular data, and special apps), allegedly for the public good. Any related disclosures of personal information may help to better identify infections and track the spread of the decease.

At the same time, current digital solutions have implications for privacy and data protection. Governments are collaborating with telecom providers to access geolocation data; new mobile applications are also being launched with different degrees of privacy and data protection. Leveraging biometric data has both benefits and challenges. The OECD recommends that governments consider the legal basis of the use of these technologies, which should vary depending on the type of data collected, the requirements of proportionality, transparency, and accountability, and limited time periods for collecting and retaining personal data[28].

The Court's legal positions, outlined above, are vital in considering privacy concerns around anti-COVID-19 digital measures.

---

[27] *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, ECLI, CJEU (2020)

[28] Organization for Security and Co-operation in Europe (OECD). (2020, April 23). *Tracking and TRACING COVID: Protecting privacy and data while using apps and biometrics*. https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-pro- tecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/

Scholars also note that the most privacy-protective app design should be used which meets the public health goal, and the benefits of meeting such a goal outweigh its deleterious effects on privacy. When balancing constitutional values, it is also important to consider the extent by which the app usage reduces the need for restrictions in the form of self-isolation (thus promoting freedom of movement and work) (Austin et al., 2020).

Developed democracies have created solid legal frameworks related to the COVID apps. One example worth noting is Australia, although issues related to the possibility of obtaining this app information by law enforcement agencies and courts remain largely open[29].

Conclusion

Surveys published in several media reveal that many people are concerned about how companies or the government are using their personal data, believing that most of what they do online or while using a cell phone is being tracked by the government, advertisers, and technology firms. Few understand what is being done with their information. When it comes to data collection, people tend to see more risks than benefits.

This paper was meant to outline key human rights considerations arising in the legal area related to surveillance in the modern world. The Court's rulings and international legal framework should hopefully enhance democratic values without compromising health and safety concerns. They should also become the basis for further positive development of laws, case law, and research in this area.

References:

1. Allen, A. L. (2008). Dredging up the past: Lifelogging, memory, and surveillance. *University of Chicago Law Review*, *75*(1), 47–74.
2. Tanguay-Renaud, F., Austin, L. M., Chiao, V., Coleman, B., Lie, D., Shaffer, M., & Slane, A. (2020). Test, trace, and isolate: Covid-19 and the Canadian constitution. *Articles & Book Chapters*, 2797. https://digitalcommons.osgoode.yorku.ca/scholarly_works/2797
3. Barnhizer, D. R. (2013). Through a PRISM darkly: Surveillance and speech suppression in the "post-democracy electronic state" [Unpublished paper]. Cleveland State University. http://works.bepress.com/david_barnhizer/77/
4. Goold, B. J. (2010). How much surveillance is too much? Some thoughts on surveillance, democracy, and the political value of privacy. In D. W. Schartum (Ed.), *Overvåkning i en Rettsstat – Surveillance in a Constitutional Government* (pp. 38–48). Fagbokforlaget. Allard Research Commons. https://commons.allard.ubc.ca/cgi/viewcontent.cgi?article=1149&context=fac_pubs
5. Hoofnagle, C. J. (2017). FTC regulation of cybersecurity and surveillance. In D. Gray & S. E. Henderson (Eds.), *The Cambridge handbook of surveillance law*. (pp. 708–726). Cambridge University Press. https://doi.org/10.1017/9781316481127.031
6. Malgieri, G. & De Hert, P. (2017). European human rights, criminal surveillance, and intelligence surveillance: Towards "good enough" oversight, preferably but not necessarily by judges. In D. Gray & S. Henderson

[29] Watts, D. (2020, May 2). *COVIDSafe, Australia's digital contact tracing app: The legal issues*. SSRN Electronic Journal. https://dx.doi.org/10.2139/ssrn.3591622

(Eds.), *The Cambridge Handbook of Surveillance Law* (pp. 509-532). Cambridge University Press. https://doi.org/10.1017/9781316481127.023
7. Moreham, N. A. (2008). The Right to respect for private life in the European Convention on Human Rights: A re-examination. *European Human Rights Law Review*, (1), 44–79.
8. Ni Loideain, N. (2015). EU Law and mass Internet metadata surveillance in the post-Snowden era. *Media and Communication*, *3*(2), 53–62. http://dx.doi.org/10.17645/mac.v3i2.297
9. Slobogin, C. (2002). Public privacy: Camera surveillance of public places and the right to anonymity. *Mississippi Law Journal*, *72*, 213-315.

Information about the author:

Roman V. Prudentov — Ph.D. in Law, Solicitor of the Senior Courts of England and Wales, Associate, Freshfields Bruckhaus Deringer LLP, London, UK.
romanprudentov@rambler.ru

Сведения об авторе:

Прудентов Р.В. — кандидат юридических наук, солиситор Высших судов Англии и Уэльса, юрист международной юридической фирмы Freshfields Bruckhaus Deringer LLP, Лондон, Великобритания.
romanprudentov@rambler.ru