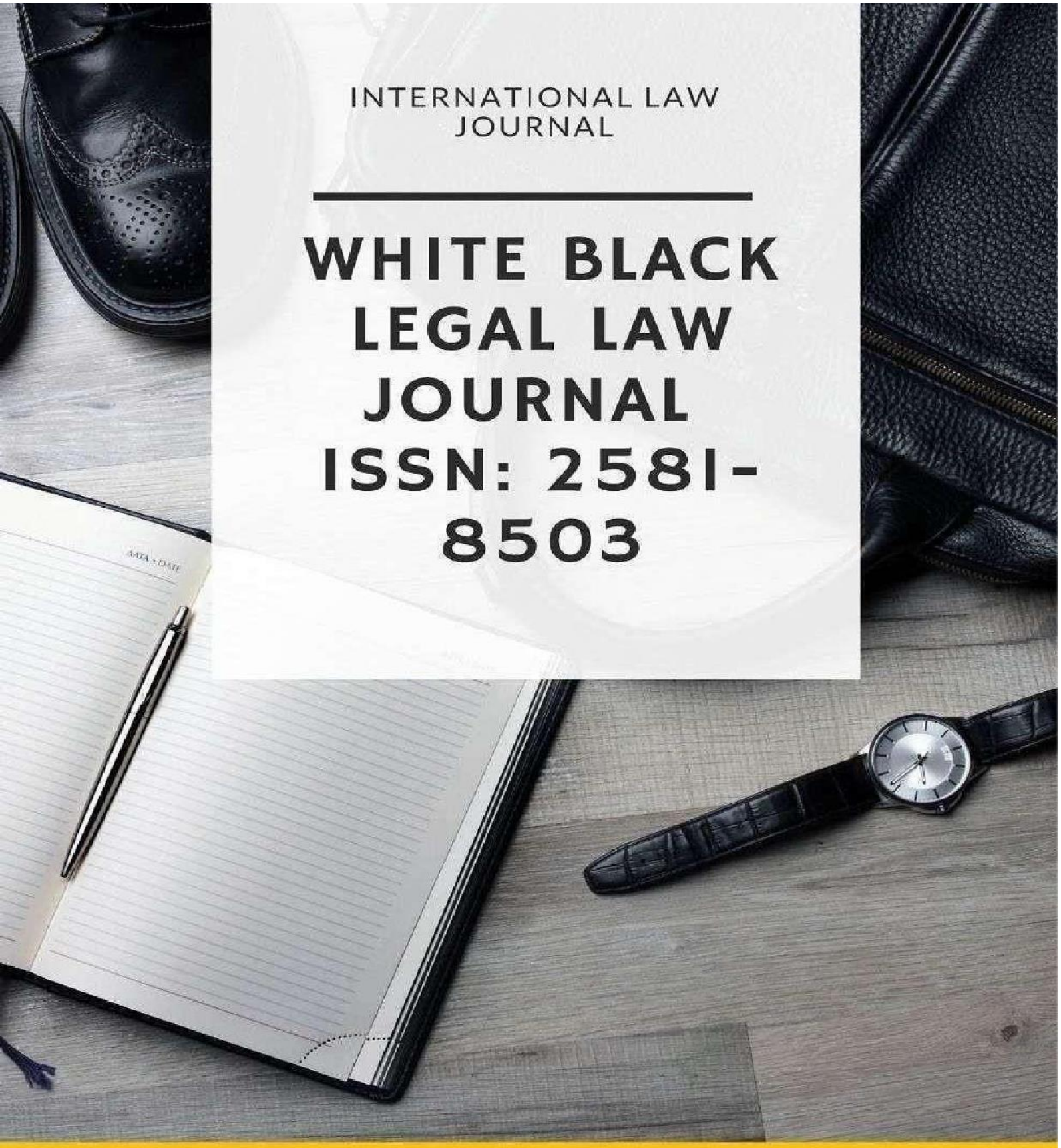


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

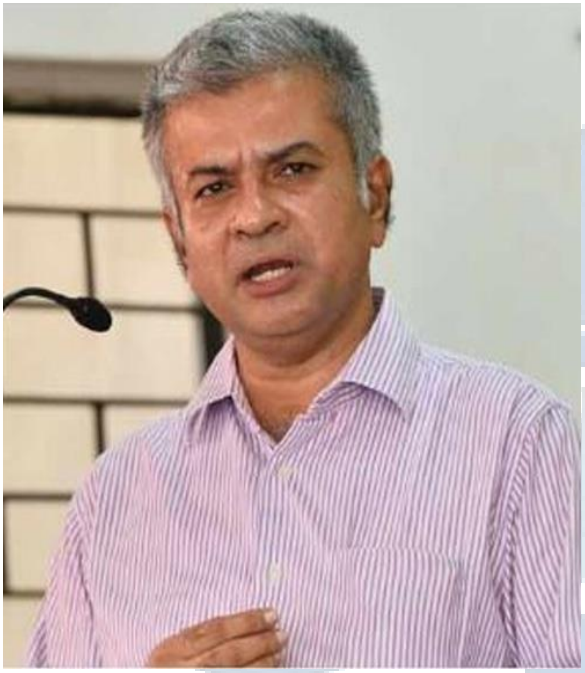
The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | March 2025 ISSN: 2581-8503

EXPLORING THE RIGHT TO PRIVACY IN THE DIGITAL AGE

AUTHORED BY - UMA K. SHINDE &
DR. PROF. KONDAIAH JONNALAGADDA
Maharashtra National Law University, Chhatrapati Sambhajinagar (Aurangabad)

Abstract

This paper aims to examine the various dimensions of privacy rights as they are challenged and transformed in the contemporary digital landscape. With the proliferation of digital technologies and data collection practices, the implications for individual privacy are profound and multifaceted. This situation raises significant questions about how personal information is gathered, stored, and utilized by both corporations and governments. Individuals are increasingly concerned about their digital footprints and the extent to which their personal data can be accessed or exploited without their consent. This growing awareness has led to a demand for greater transparency and accountability from corporations and governments regarding their data handling practices. As individuals navigate the complexities of the digital landscape, they seek assurances that their privacy rights are respected and protected. This demand for privacy is increasingly challenged by the pervasive nature of digital technologies, which often collect and store vast amounts of personal information. Consequently, individuals are compelled to reassess their understanding of privacy rights in light of new legal frameworks and ethical considerations.

Keywords: Privacy, Data protection, Digital surveillance, Technology and Privacy, Freedom of Expression

1. Introduction

The history of surveillance is as old as human conflict, for the central paradox of security is that, to be secured, people must sacrifice the very qualities that make them human: in the embrace of total security, they become something less than fully human. In this sense, surveillance necessarily diminishes the humanity of both watched and watcher.[1] The right to privacy seeks to pose a counterbalance to this diminishment, framing privacy as a necessary shield against the ever-watchful eye of state authority. In cases in which the ordinary protections of privacy have been defeated or impaired, the right offers antecedent substantive protections to shield behavior that might otherwise be considered suspect or even felonious, thus ensuring that all people—even the most violent or despicable—remain fully human.

Unlike more totalizing conceptions of authority, democracy is both nurtured by and in need of these peculiarly human aspects of privacy. In close votes in national parliaments, mathematical models have determined the likelihood that a given MP will follow up the anonymity of the secret ballot by voting against her official party line is 93%. But privacy doesn't just provide the shelter for unconstrained action, it furnishes the crucible in which dissenting opinions form.[2] The right to privacy is properly understood, then, as a safeguard of the democratic ethos. But the invigilation of the state remains only part of the story. If privacy is a fundamental aspect of liberty, it translates also into a franchise over the norms that govern the competitive arenas of everyday social life.

1.1. Background and Significance

The right to privacy has always been a part of human freedom. With the advances of the digital age, the gaps between the public and private spheres may well be thrown into a state that will require constant redefinition. The universalization of digitized information and communication may lead to a transformation of individual privacy and perhaps even the notion of the private self as it is currently understood. Claims of privacy have a long history and they can be found in political, moral, and religious discourses, starting from the understanding of governance of the self. As much as governments express the need for security and the states and nations pretend to protect their borders and identities, the private citizen has the right to express and defend their intimate-self against any interference.

[1] M. Blanke, J., 2018. Privacy and Outrage.
[2] B. Serwin, A., 2009. Privacy 3.0-The Principle of Proportionality.

The private self has the right to remain undisclosed with the knowledge of the subject person for the public sphere. Such an understanding of respectfulness towards a human, intimate and non-shareable part of the self is fundamentally a recent apprehension raised as a reactionary effort towards the shifts in lifestyles, mentality and habitus during the 20th century. Protection of the private communication sphere against unreasonable interference is a core example of the realization of this commitment. Developments of communication technologies have influenced societal understanding of what may be defined as a private communication and to what extent it may be kept as private. Given the catastrophic potential of electronic communication technologies, within the surveillance context, E-mails are considered as the most intimate and private due to their highly personal nature; therefore surveillance is viewed as having more chilling effect on E-mail communication than it does on other forms of digital communication. SMS and telephone calls are regarded as slightly less private than E-mails while social media and interaction in the cyberspace are at the bottom. Several national and European legal frameworks also acknowledge the exceptional protection as granted to the communication media.

1.2. Scope and Objectives

The proposed Drafting Project on developing a resolution (or a set of resolutions) on 'Exploring the right to privacy in the digital age' by fostering a global dialogue on the right to privacy and its interrelation with and promotion of other human rights in the context of the digital age focuses, in an initial phase, on the scope, objectives and expected results, and on the structure.

The proposed Drafting Project seeks to explore the right to privacy and the rise of the digital age by fostering a global dialogue on the right to privacy and its interrelation with and promotion of other human rights in the context of the digital age, including the right to freedom of expression.

The ultimate objective of this initiative is to identify intents and efforts by state authorities in the creation, pervasiveness and maintenance of social, political, and cultural environments in which individual rights can thrive and be protected. Efforts must be made towards protecting the concept of privacy. However, privacy does not exist in a vacuum, and the protection (or lack thereof) of other rights integrally contributes to its existence and vitality, especially to the growth and maintenance of more profound and valuable realms of privacy. Hence, this initiative aims at highlighting, through the lens of privacy, the precarious state of other rights,

the overall chilling effects on human rights environments and instances of the profound and universal consequences of human rights violations.

2. Historical Development of the Right to Privacy

This article discusses the right to privacy, developing a definition of privacy that includes consideration of privacy harms, and considers how the right to privacy can be practically designed for increasing privacy concerns in new Information and Communication Technologies (ICTs). A history of the right to privacy is presented as background.

Privacy is an evolving concept; new technology generates new privacy concerns and renders certain older concerns less relevant. An effective analysis of privacy must adopt a dynamic approach, taking account of variations in privacy expectations across time and individuals, and recognizing that claims for privacy may be based on a wide variety of potential harms and interests.[3] In the analysis of this article, a key illuminating moment in privacy will be connected to the otherwise unrelated concern of wide press freedom, so defining a general framework in which the right to privacy has developed in Western legal systems. Thus, a legal framework is laid out which helps identify the types of privacy harms that might be taken more account in privacy analysis and protection in ICTs. Methods are discussed for keeping the right and expectations of privacy roughly in proportion using a Principle of Proportionality of Privacy.

2.1. Origins of Privacy as a Concept

"THE RIGHT TO BE LET ALONE" was the headline chosen for an article on privacy in the digital age. As a concept, privacy has attracted much attention in the media and popular culture, and has a salient place on the policy agendas of governments in many countries. However, the protection of privacy as a legal right is a relatively recent development and is not as widespread or as consistently acknowledged as the various lamentations over the decline of privacy might suggest. The concern with privacy is as universal as the right to privacy as a widely recognized right is of recent date.[4] Although not mentioned explicitly in the European Convention on Human Rights, privacy has been recognized as a fundamental right of human beings and has thus become a general principle of international law. As such, it is directly protected by a number of regional agreements. In particular, privacy rights are dealt with in Article 12 of the

[3] B. Serwin, A., 2009. Privacy 3.0-The Principle of Proportionality.
[4] J. Gstrein, O. & Beaulieu, A., 2022. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. ncbi.nlm.nih.gov

United Nations Declaration of Human Rights adopted by the General Assembly on December 10th, 1948, and in the International Covenant on Civil and Political Rights signed in 1966. At the international level, the highest protection of privacy rights is therefore achieved by the judiciary bodies considering these agreements. These include the European Court of Human Rights, with competence under Article 32 of the European Convention on Human Rights, the Human Rights Committee of the United Nations Economic and Social Council, and the tribunal referred to in Annex 6 to the General Framework Agreement for Peace in Bosnia and Herzegovina, which has required the European Court of Human Rights to make referrals to this entity. At the regional level, there is a fundamental right to privacy by virtue of its recognition in other general principles of international law, in particular in the constitutions of the member states, as regional understandings relying on it have been concluded since the adoption of the Universal Declaration of Human Rights and Covenant. At its 80th Session, the European Committee of Social Rights found that Article 9 of the European Social Charter implicitly recognizes the right to privacy and has monitored information on legislation on data protection in the State parties to it since 2011. The right to respect for private and family life, as well as to secrecy of correspondence, is constitutionally and even explicitly protected in the Czech Republic. This is why the quasi-universal right to respect for private and family life, as well as to secrecy of correspondence, must also be guaranteed by the Convention.

2.2. Landmark Legal Cases

New technology brings new privacy concerns and renders certain older privacy concerns less relevant. By way of example, the advent of handheld devices, such as smartphones and PDAs, within the past decade has exponentially increased the storage capacity and inherent privacy breaches. One estimate indicates that millions of people are walking around with videocameras on their belts, in their purses, or stitched to their clothing. While handheld devices can infringe on traditional privacy rights and interests, the idea that surveillance can only occur from a stationary viewpoint is a quaint concept by today's standards. Conversely, surveillance cameras are almost as abundant as gas stations. Cameras are perched on traffic light poles, public shopping mall ceilings, in taxis, buses, and public businesses, capturing unsuspecting pedestrians with little forewarning. Cell tower triangulation, a requisite technology for cellular phones, interacts with a central server, issuing a date and time-stamped record for each call. Synchronized timestamps and receipt printouts from a merchant can concretely place a debit cardholder with a pattern of purchases. Similarly, these tracking mechanisms can determine habitual associations with an alarming degree of precision.

The principle of proportionality is an important one in the consideration of privacy. Proportionality permeates the statutes and case law of many countries and sets the standards for much conduct. In discussing, consideration is given to Technology's displacement of the common-law principles in the context of the Privacy 3.0. In this new age of privacy concerns due to rapid technological advances, it is argued that technology now bears upon the privacy quanta. A justification for preventing trivial privacy claims is the incompatibility of old tort principles in the face of Technology's evasion. Ultimately, a centuries-old jigsaw puzzle that, when pieced together, nobly attempted to erect a new privacy "right anklet," broad enough to encompass heretofore unprotected territory.

3. The Digital Revolution and Privacy

The concept of privacy has been examined for centuries, developing into a multifaceted principle along the way. As technology evolves, so does the perception of privacy. These changes can clearly be seen as society enters the digital age. New tools and gadgets that utilize data collection have the public questioning what types of information are secure. Countless instances of data breach have accumulated, including large corporations and the government. Moreover, there are whistleblowers who claim espionage, creating further concern for personal privacy. Lawmakers are confronted with the task of maintaining a balance between a variety of interests. The importance of privacy is tempered by the need for security, but also economic advancement. Legislators are in the age-old position of changing laws to regulate new technologies.[5] There have been a number of proposed solutions on how to balance liberty and security. It is worth looking at some historical instances concerning the right to communication privacy. How the concept of privacy has evolved, in what ways it is resistant to change, and what the future may hold are also themes considered.[6]

Technology has completely modified most facets of daily life. Currently, society is in the realm of the Internet of Things, Smart Cities, and Big Data. From dialing 411 to obtain an address, a Sextant to determine longitude or latitude, or to find a Pin Mill, the ability to hold a dataset has empowered people. As devices have become "smarter", the capabilities of data collection have expanded. Society has entered an age where most items can have an IP address. As objects go online, each one generates a digital footprint. These footprints create a digital copy that documents daily activities. In 2014, people may stop the local Radio Shack, purchase a drone

[5] B. Serwin, A., 2009. Privacy 3.0-The Principle of Proportionality. [PDF]
[6] M. Blanke, J., 2018. Privacy and Outrage. [PDF]

and camera, fly it over a house, and capture footage. Now, near real-time satellite footage is viewable. A plethora of people are engaging in Touch-toPay systems. Many new vehicles may immediately extricate GPS evidence. Surveillance through systems becomes everyday such as doorbells, microwaves, and refrigerators. Very recently, an agreement was signed to provide information of vape use to investigate drug crimes. Already, many may be in Smart Homes. As more of life becomes connected, each element creates a digital account posed permanently in the cloud of this era's technological revolution.

3.1. Emergence of Digital Technologies

The last decades have witnessed the alarming apparent erosion of privacy. The rise of digital technologies, the increasing deployment of webcams and biometrics, the development of e-surveillance and databasing, the recent efforts to monitor the Internet and to enforce digital copyright, have constituted potent vehicles for expanded control. Each individual movement generates increasing quantities of data, some gathered voluntarily, some captured unobtrusively. Most digital transactions are almost immediately recorded, and computerized systems employing different sorts of sensors can observe and control many aspects of people's everyday activities.[7]

The November 2009 report of the EUs Fundamental Rights Agency on privacy and data protection indicates that privacy tops the list of concerns of European citizens. According to the Pew Research Center survey on the future of the Internet, about 70% of consultants believed that the greatest, probably negative impact will concern ethics and privacy, whereas 85% said that leading firms will contribute in taking further steps to revolutionize online data collection.

3.2. Challenges to Privacy in the Digital Age

Privacy is a protected human right which can be understood as the right to freedom from interference. Mostly, this privilege is defined as information privacy. It comes from the various countries in the form of the right to informational self-determination. However, the right to privacy should not be underestimated only as a question of unlawful data protection, but should be considered on a normative level as a right linked to the respect of fundamental individual freedoms such as, for instance, personal identity or freedom of association. We are living in a new age, and it is rather clear that new age is a digital one. However, while some scholars

[7] J. Gstrein, O. & Beaulieu, A., 2022. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. ncbi.nlm.nih.gov

denounce this contemporary phenomenon as lacking dignity and respect, it is nonetheless possible, even useful, to reconsider and examine the idea of privacy not only because of the great changes the digital era often brings, but as a protection of freedom and democratic values. The principles of protection of privacy still have their security. However, especially since the data protection movement, they are not as solid. Permissions are no longer copyrighted, or else attempts have been made to do so and have been met by heavy outcry. With the evolution of the digital age regarding respect for privacy, this right comes under increasing pressure in the digital age, which led to new challenges for additional research.

4. International Legal Framework

Privacy is a universal human right, enshrined in Article 12 of the United Nations Universal Declaration of Human Rights.[8] Internet legislation is dominated by data protection, which can unintentionally decouple data protection and privacy, leading to a blind eye being turned to the restriction of privacy negations. As the party responsible for governments and related infrastructure, the state must also have a data collection and surveillance function, cannot account for the full scope of privacy and the ways in which it differs. Article 17 of the International Covenant on Civil and Political Rights provides legally binding human rights standards for nation states to respect, protect, and fulfil individual rights, including privacy. This performativity is performative in that it coincides with long-standing European attempts to position privacy as a trade obstruction in order to "make a Europe fit for the Internet's explosion of data flows". The focus on privacy negations in Internet governance processes, those of golden European or US interest. Overall, it suffices to illustrate the theoretical and political complexity at the interface of privacy as a human right and data protection as a question of Internet governance. Some bilateral agreements also threaten the full enjoyment of privacy if data can be freely transferred, used and stored without guarantees of due process regarding this information. These rules might help jurisdictions to build entries for shortcomings in their respective legal orders on the basis of international instruments. Like universal standards set in international human rights treaty law, it includes some basic guarantees for all people in the world. Europe has informal and formal guarantees through regional and union treaties such as the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. Similarly, robust standards exist in all regions

[8] J. Gstrein, O. & Beaulieu, A., 2022. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. ncbi.nlm.nih.gov

of the world. Some of the internationally compiled, high-security standards are already the result of widespread human rights discussions on privacy, aiming to establish a solid set of public guarantees for the protection of citizens. In fact, privacy or something closely related to it is a formally guaranteed civil right in national constitutions, such as in the Bill of Rights of the USA. Among the ten amendments ratified in 1791, the fourth amendment is one of the most cited in the history of privacy.

4.1. Universal Declaration of Human Rights

Privacy is a universal human right, enshrined in Article 12 of the United Nations Universal Declaration of Human Rights from 1948,[9] as well as Article 17 of the International Covenant on Civil and Political Rights from 1966. Although the wording and structure of both provisions are very similar, only the latter document was drafted from inception to become legally binding for states to protect the rights of individuals.

Privacy is a formally guaranteed civil right in national constitutions such as the Bill of Rights of the USA. Following its ratification in 1791, the 4th amendment became highly contested or is interpreted in a wide variety of ways. By prohibition of unreasonable searches and seizures, this provision is of particular interest due to the wide-spread and continuous control of information and communication artifacts by different state and corporate agencies about individuals. With Moore's law of exponential growth, both the significance and the actual ambit of these tenets had exploded in the digital age.

4.2. European Convention on Human Rights

The concept of private life involves moral values and privacy. To be able to respect these values, privacy as a dimension of the fundamental right has become important. The right to privacy states that individuals have the right of privacy and the claim to protect their own private lives. The protection of the individual and his private life and the confidentiality of private information is one of the most important aspects of freedom. This right is one of the requirements of democratic societies. It consists of the same and equivalent legal norms in democratic legal countries.

The protection of private life has also been guaranteed by law in these countries. This right is

[9] J. Gstrein, O. & Beaulieu, A., 2022. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. ncbi.nlm.nih.gov

also safeguarded in international law. Article 8 of the European Convention on Human Rights states: everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[10] In accordance with the interpretation of the European Human Rights Court, this freedom also protects family life, the home and the confidentiality of correspondence in addition to individual private life. This right also includes respecting the goods, bodies and moral and emotional life of individuals in the broadest sense. This is an absolute right and is not subject to any first limitation. It is open to a wide range of protective measures from states.

4.3. General Data Protection Regulation (GDPR)

There is more power in the laws and regulations over data. To succeed in support of the protection of individuals with regard to processing of personal data, universally applied good practices rely on having the right content at the right time, with supporting privacy information safeguards, so that the data is protected from any kind of privacy risks. The law is a basic component in setting out general principles and requirements for the transfer and processing of personal data. In the case there is a dispute in relation to the handling of personal data, this law is a source of information in order to make determinations as to whether there has been any violation of privacy. Europe is the first region to be so comprehensive in addressing and shaping one of the most critical issues arising from the digital age. The data protection policy is simply the most robust and powerful that can benefit from the application of good practices that are essential to companies, nonprofits, bureaucracies, anywhere that relies on the transfer and/or the processing of personal data. As digital tools quickly exploit, allow for the unobstructed use, transfer, and storage of vast volumes of personal data, the existence of this regulation would give strength, power, and legitimacy (often lacking) to the protection of personal data. All actors connected to the healthcare system and the related IT system need to be aware that the current practices regarding health data which are collected, handled, transferred and structured are not up to compliance with the regulation resorting the design of new tools, mechanisms and data mountains. Paradoxically, ‘big data’ is needed to cope with

[10] H. Çinar, Özgür, 2019. The right to privacy in international human rights law.

the bigger data protection that is now imperative.

5. National Approaches to Privacy Protection

Human right levels and the right to privacy. This section approaches the right to privacy on four levels: international, regional, national and personal.[11] The right to privacy is a universal human right – it is enshrined in Article 12 of the United Nations Universal Declaration of Human Rights from 1948, just 1 year after the UN Charter. The UN Charter, as the constitution of the United Nations, formalised respect for human rights by member states. Accordingly, the UN General Assembly adopted the Universal Declaration of Human Rights to establish normative standards of behaviour for the treatment of individuals by governments. The right to privacy was therefore one of the first human rights to be codified globally. However, it is not legally binding for states due to the non-obligatory nature of declarations. More importantly, the phrasing of the Universal Declaration of Human Rights in this regard is only a recommendation to states – it recognises privacy as a right which deserves protection but full consideration needs to be taken that national protection may be provided in form of guarantees.

Both the phrasing and the structure of Article 12 reveal connections to another important binding document of the United Nations – Article 17 of the International Covenant on Civil and Political Rights. This kinship is due to the fact that the right to be free from interference with privacy, family, home or correspondence is the same in both provisions. Hence, Article 17 of the International Covenant on Civil and Political Rights is the starting point for exploring the right to privacy on a global level. Europe has its formal guarantees regarding privacy protection, such as the European Convention on Human Rights from 1950, supplemented by the case law of the European Court of Human Rights. The most recent example is the right to be forgotten, which rethinks the right to respect for private life in the digital era and transforms the landscape of other rights, such as freedom of expression. Moreover, privacy is also cherished in the Charter of Fundamental Rights of the European Union and is rather expansive. Although the Charter of Fundamental Rights of the European Union is binding on EU institutions and bodies, it only matters in relation to the member states of the Union when they implement EU law. Additionally, similar standards on privacy protection exist in all regions of the world. In Africa, the right to privacy is specifically protected by Article 27 of the African

[11] J. Gstrein, O. & Beaulieu, A., 2022. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. ncbi.nlm.nih.gov

Charter on Human and Peoples' Rights. The American Declaration of the Rights and Duties of Man from 1948 proclaims in Article IV that "everyone has the right to liberty and security of person", which in turn includes privacy. Similarly, many states of the American hemisphere have designated privacy as a civil freedom in their national constitutions, including the first and the most influential one – the Bill of Rights of the USA. The passage of the fourth amendment in 1790 was a result of the hostility of the American colonists towards the Writs of Assistance, authorising the British customs officials to conduct searches and seizures in order to control smuggling and to enforce the tax regulations of the Seven Years' War. At the same time, the British government endeavoured to deal with its enormous war debt by establishing administrative policies aimed at increasing direct and indirect taxes on the American colonies. In this context, John Adams, future President of the USA, defended to great extent the opposition of the American Merchants against Britain's policies. As a retaliation, the authorities of the British colonies introduced a systematic non-importation agreement. In 1768, British officials seized a vessel owned by the Merchant John Hancock, which led to further anti-British sentiments. Hancock's personal space and autonomy was hence substantially affected. Prior to the American independence, the Massachusetts colony had already declared the Writs of Assistance unconstitutional. This can be considered as the first legal act against the fundamental issues of the fourth amendment. The discord between the Crown representatives and the American colonists led to the normalization of the practice of issuing general search warrants, which allowed the British authorities to conduct searches and seizures virtually anywhere at any time, for any object. This warrants had a lasting and adverse effect on the personal qualities of individuals living in the colonies. The above-mentioned situation resulted in the prominent legal case known as Entick v. Carrington, which firmly established two principles. First, it was rendered that the common law provides general protection to the privacy of individuals. Second, it was judged that governmental search and seizure was possible only after a normal warrant had been issued with precise legal definitions. The issued warrant had to specify the location and the items to be searched or seized. Moreover, the warrant had to be executed willingly by the item listed in it. The refusal to cooperate rendered all the gathered evidence as inadmissible in court. In light of this adverse precedent, a safeguard against governmental search and seizure was included in the Bill of Rights. Paradoxically, after the American independence, the American merchants established entirely pirate trade policies in New England, which prompted the introduction of the Sugar Act of 1764 imposing a substantial tax on sugar bought from the French colonies. To enforce this Act, the British authorities increased customs regulations on the ports in the American colonies.

5.1. United States

A reasonable expectation of privacy extends to individuals in the United States; this expectation of privacy is not lost in the digital age.[12] Answers may depend on the measurement of a reasonable expectation of privacy and the form the perceived invasion takes. Privacy is one of the least understood phenomena of the modern information era.[13] Privacy is not one of the rights explicitly listed in the constitution.

However according to the U.S. Supreme Court, privacy is protected by the U.S. Constitution, namely in the 1st, 4th, 5th, 9th, and 14th Amendments. In terms of digital privacy, the 4th Amendment is the one most often cited. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. Reading all of the tests together it is possible to determine if a reasonable expectation of privacy extends to the use of digital technologies. At the heart of the privacy concerns is the consumer, but companies can be consumers too. However recently as digital technology has greatly expanded and has viewable to anyone with a computer or smart phone, privacy has been thrown out nearly completely. Government and Corporations oftentimes promise personal information will not be shared.

5.2. China

This section is a work of eight scholars from eight countries. Their focus is on the right to privacy as viewed by people in these nations as well as public opinion on the current law protecting individual privacy in respective countries. For China, a recent survey on public perception of and attitude toward personal data protection will be introduced first. Then, recent discussions over the right to privacy as well as related laws and rules in China will be summed up. Although fright to privacy is constitutionally guaranteed in China, recent surveys find few in this country view the right. In a Chinese survey study by,[14] currently about 10% of urban Chinese have heard about the right to privacy, and a similar percentage state clearly they love and cherish the right to privacy. On top of that, China receives the lowest score among 38 countries in a survey question concerning whether the current national law can protect the right

[12] Shelton, A., 2014. A Reasonable Expectation of Privacy Online: Do Not Track Legislation.
[13] Green, D., 2018. Big Brother is Listening to You: Digital Eavesdropping in the Advertising Industry.
[14] Han, D., 2017. The Market Value of Who We Are: The Flow of Personal Data and Its Regulation in China. [PDF]

to privacy effectively.

5.3. India

India has been greatly influenced by the US Supreme Court in its development of jurisprudence to give effect to the right to privacy in a digital age.[15] India has adopted a privacy law in 2011, in contrast to China; therefore, the perspective on the evolving right to privacy is reviewed. The concept of the right to privacy in India has recently received wider attention in view of the incremental liberalization of the Indian economy which has led to an enormous influx of foreign capital and concomitant transfer of technology, heralding a proliferation of the use of computers. This trend was also exacerbated by the outsourcing of data processing work to India by multinational companies abroad. It does not therefore come as a surprise that computer-related data processing gave rise to a substantial body of Indian judicial decisions in recent years. The locus classicus of the right to privacy in India was recognized for the first time as a fundamental right as one of the component right to personal liberty enshrined in Article 21 of the Indian Constitution, 1950, in the landmark decision of the Supreme Court in Kharak Singh v State of UP. The Court held that criminal domiciliary visits by the police under the UP Police Regulations amounted to an invasion of privacy of liberty and freedom of the person and home within the meaning of Article 21. But that was the end of the road in privacy protection in a Tale of Two Cultures. The enforcement of the right to privacy under the Indian constitutional scheme can only be made against State instrumentalities and not against private persons. Of course, state action extends to state regulation of private transaction. In this respect, although privacy protection in India, as in the USA, would appear to have been founded primarily on the control of state power tradition, the Indian courts have a much more limited role in overseeing state behaviour in relation to privacy matters than their American counterpart.

6. Surveillance Technologies and Privacy

Recent advances in the technology used by surveillance devices threaten individual privacy. Camera lenses, for example, need no longer be inserted close to the producing device to capture images in good resolution. Cameras can now be made small enough to escape the human eye's attention, yet so sensitive to light that being close to the captured body is not necessary to capture a representation. Impinging on different sound frequencies and refining techniques used to see through objects are not the only technological developments threatening to break

[15] Basu, S., 2012. Privacy Protection: A Tale of Two Cultures. [PDF]

down the barriers of "private" locations and their wrapped privacy expectations.[16] This way, if we choose to leave our house, seeking anonymity by not revealing our identities to others is an option we can exercise. This decision does not affect the anonymity provided by the public space: we are no less subject to surveillance in the street, but we are among others in our condition. In our homes, on the other hand, solitude gives us reason to assume that no one is watching. The logic above indicates that surveillance devices can be blind to individuals, it is grounded on the circumstances of surveillance activity. Throughout human history, being away from the sight of others could offer a barrier to the tracking of agents. Considering this requirement for the occurrence of a space-time event, assuming others are not able to see could fulfill nominal purposes of anonymity.

7. Data Breaches and Cybersecurity

High-profile government data breaches have acted as a catalyst for discourse on data security as analysts, news outlets, and the public have demanded answers about the security of government systems and databases in the wake of these leaks (L. Mills & Harclerode, 2018). Recognizing the leak's dramatic effect on public dialogue about government intrusion, however, does not prevent an equally important discussion about the disclosure's intrusiveness to individuals. In response, activists, litigators, and legislators have all seized the momentum to advocate changes in consumer privacy law and cyber defense strategies. However, the focus of these efforts has entirely been on privacy in the context of corporate data insecurity. Adding to this is the fact that in the midst of media outcry for increased NSA transparency, the very same mass leak revealed metadata for the communications of a great number of innocent individuals. Data can take on many different meanings. For example, the body of an email is the content and the subject line, origin, and destination of the email is metadata. Both forms are vulnerable to a breach, and the information itself carries varying levels of intimacy, which may be intensified when aggregated. Furthermore, the value or sensitivity of data can be sector-specific. Labels such as "confidential" or "for internal use only" provide a veneer of security that transcends the information itself. To add to the complexity, the legal standards for protecting health data are different from the standards for protecting education data. However, regardless of the sector, metadata is often less protected than content under current legal doctrine. Different legal standards do not adequately recognize the fungibility and character of data itself. Additional consideration must be given to potential protective measures and the

[16] W. Luk, J., 2002. Identifying Terrorists: Privacy Rights in the United States and the United Kingdom. [PDF]

implications that such protections carry.

8. Ethical Considerations in Privacy

The photograph is significant. A runner without a bra is running. She is focused, confident, and powerful. She feels good. This image depicts a contrasting scenario. It was taken unknowingly. The young woman was originally posing for another photograph. She was distracted, easily controlled and vulnerable. The difference is clear: the more positive image was taken with her willing participation; the more negative was taken without her consent. The former photograph was taken on the marathon course. The runner is wearing a pink sports bra. She is proud to represent a charity. Well in the back is the latter photograph. It is unflattering. It depicts a tired young woman in a yellow bra. There are fat rolls on her back. Her facial expression falls far short of confident. This photograph was obtained by including photos taken during the marathon in a search. This search brought up an astonishing number of images. After I ran the marathon, I read the information on the race website. It stated that the marathon would be photographing all runners both at the start line and finish line. I was not aware that pictures would be taken during the run. So, I was naturally quite surprised to find a young female runner who likely did not know photographs would be taken in this setting. The search returned images of runners with race numbers. From the available information, it would seem many of the finish line photos were taken unknowingly. The majority of these images do not depict positive scenarios. This woman was not the only runner without a sports bra. In total, there are seventy-seven image results when the search is performed with the runner's information. Twenty-eight of these images are of women. Six show women not wearing a sports bra. Given the emotion evoked by the photograph, this last statistic is disconcerting. Runners form a close-knit community. This community is one that holds the athlete in the highest regard. Athletes at any level are cognizant of the extreme difficulty of running such a distance. Runners feel a shared camaraderie in the accomplishment of running a marathon. Add in the intention of raising money for charity and the positive social norm increases. Strong emotional reactions are evoked when the runner enters the park where the majority of the crowd is. This strong emotional response is typically very positive, adding to a memory of the run as something proud and joyful. Inconsistent with this strong social norm are actions taken by this woman. In the other photographs she is not running. Are there expectations of privacy in a public race? This question was augmented by a posting on a running website, which linked to a photo weblog of the marathon. This weblog invites people to post comments on photographs taken at

the marathon, and by simply including the image number, run number, or description of what the runner was wearing, the person posting makes viewers feel, "like that's the way we should see them." Evidently, many did. There are many negative posts. However, the user can request that a picture be removed if it is of them. A few users made this request. One commented, "Post a picture of a headquarters on their homepage?" In the same way that athletes are held in high regard, so are those who work for and support charities. so the thirty-seven-year-old female sixth-grade school teacher who has raised over $2700 isn't deserving of respect? Many of the women who are making negative comments also wrote run times for the race. From the visible belly ring and the halo taped to the mouth, it's pretty easy to find a finish line photo of your idol. At the very least, many finish line pictures were almost identical. It should also be noted that the photo host deleted all images connected to comments that they were profiting on. Being ridiculed anonymously is one thing, but relinquishing the right to choose exactly what can be remotely linked with one's name is another matter entirely. There are too many possible consequences of this image, both personally and professionally.

8.1. Informed Consent and Transparency

Eight ideas for the protection of privacy in a datafied society using different methods and for different stakeholders. The right of each individual to decide autonomously on the disclosure of information about herself, especially in an increasingly surveilled, observed, and analyzed world, in which many personal decisions are taken by application programs and algorithms. One participant in a population-based cohort study submits a data access request to the research institute and wants to know which of her records are stored in research databases and were provided for research projects. In the clinical routine, many more data are collected and stored than are common in cohorts, however, the hospital procedure steps and their medical necessity are usually not recorded in the EHR, so it is hardly possible to answer. Regardless, the transparent data handling, which is part of the consent procedure, ensures that all data used for establishing her disease status, risk factor values or event dates can be tracked back to the original records together with a justification (J. Gstrein & Beaulieu, 2022). Transparent data handling also ensures that this request can be treated efficiently and in compliance with data protection regulations.

9. Definition and Scope

Discussions about the right to privacy take different shapes in each society and moment. The digital revolution and its algorithms and powers of prediction encroach on the private sphere

as understood since Warren and Brandeis. More data is generated in less time, and this use and reuse of data is contributing to a dystopian data moment, where privacy is only for the elites or the offline persons, who can afford to be private.[17]

At this point, multiple arguably opaque algorithmic systems decide on the fate of individuals. Once data is streamed or posted, there is no way to take it back, as the case of Kathy Sierra, the blogger who fearing rape and murder threats had to go into hiding, exemplifies. More recent cases are the Facebook emotional contagion experiment, the ill-fated Google Glass live recording spectacles or indeed the right to be forgotten conflict in Europe. One response to the blackmail economy the Internet seems to be fostering is to become net invisible, to encrypt identities with PGP keys, browse through Tor's deep web browser, always-on-top-disable-WebRTC, and install an operating system with full-disk encryption and an ever-changing MAC address. That is to be part of the encrypted, decentralized, peer-to-peer, pirate browser crowd nowadays reshaping the digital underground.

10. Privacy and Freedom of Expression

Theoretical formulations of privacy and data protection rights are often premised on the notions of similar private and public spheres, proposing these as spaces where individuals can be protected from intrusion, speech controls, as well as inappropriate processing of personal data. Because of the central role of the internet and the pervasive nature of digital communication technologies, these basic assumptions require close scrutiny in policy forums, in theory, and in practice. Private and public spaces are no longer physical, tangible, or offline. Graphic-interactive technologies and narratives published in the internet space, including social media, can record each and every move, preference, and choice of data subjects, including their social and political behavior. Accordingly, considerable discussion accompanies the nature and scope of the respective rights in bringing these into balance with one another. The sanction of a lawyer supported by an NGO in various lawsuits against social media that defame him seriously infringes the freedom of artistic expression of the parties creating the material. At the same time, search engines process data undermining the lawyer's dignity in an excessive way. Personal data collected are inaccurate or irrelevant, having regard to the purpose of the processing.

[17] Green, D., 2018. Big Brother is Listening to You: Digital Eavesdropping in the Advertising Industry.

11. Balancing Rights in the Digital Sphere

Digital technology has spread over all the spheres of life of people and society's activities, profoundly changing familiar living conditions, and environment human consciousness and behavior. In digital age, private life is becoming most vulnerable to arbitrary interference. After the expiration of the first digital age with mankind starting in computer technology booming development, the effects of the global digital revolution began to have significant social and individual consequences. One of them was intensification and massive spread of digital and computer technology over all various areas of society, life activity, and everyday life. It has changed life at the workplace, home leisure and entertainment, shopping, traffic, human communications, personal lives and habits, entertainment behavior, and etc. Microprocessor advance and advent of microelectronics infinitesimally small in its size and unique in its characteristics, have created new convenient and comfortable for use microelectronic devices, among which there became compact portable computers (such as notebooks, laptops, handhelds, UMPC), mobile phones, smart boxes PDAs, digital cameras, and camcorders with cellular phones, world receiver, dictaphones, blackberries, etc.[18]

12. Future Trends and Technologies

Regarding surveillance, the draft regulations provide for a reduced authorisation threshold but broadened scope. Regulation 8(4) involves significantly amending the current authorisation regime and is concerned primarily with crime, bijural child welfare and the legal profession. The thrust is to permit intelligence to be gathered for the prevention, detection, investigation or prosecution of any of more than 20 crimes, the investigation of serious child abuse or any representative's actions and the provision of legal representation for certain categories of individuals. This is proposed alongside a reduced threshold for authorisation from "serious" criminal offences to just "criminal offences" for factors such as damage to property, the penalty for which resides under £2,000. As with the peaceful protest authorisation, the list of crimes has been expanded and the term "serious" removed, yet this decision appears less arbitrary in the context of crime, which is already defined in law. The rationale surrounding a greater focus on criminality is nevertheless notable, as legal professional privilege has historically lent itself to the gathering of intelligence for lesser offences than the "serious crime" upon which RIPA is premised.[19] Defense of the Draft Regulations maintains there has been a lack of such

[18] Anatolyevna Kuznetsova, O. & Bondarenko, N., 2017. Private Life Safety Provision in Digital Age.
[19] Michael Froomkin, A., 2000. The Death of Privacy?.

proactive investigation in this context to date, and that without access to financial intelligence or legal privileged material it may be difficult to disrupt criminal networks at an earlier stage. Potential concerns may be that, although these provisions would respectively alienate financial institutions and deter suitable legal representation, there does not appear to have been an analysis of the qualitative or socio-economic effect that widening intelligence-gathering powers in this area may have. With this in mind, the draft Code of Practice indicates the Data can only be retained where it is for the purpose of investigations or prosecutions arising from Part 1 Conduct; this must further be reviewed at 90 days and may only proceed for an extended 180 days where the relevant offence has been discovered. It is a concern, therefore, that for enquiries into serious crime the relevant offence may remain elusive.[20]

13. Conclusion

This Article frames a unique approach to the study of mobile phones and privacy. Surveying the existing literature, it is argued that scholarship on the right to privacy has become outdated and ineffective, particularly in a fast-evolving digital world. This Article aims at proposing a new, comprehensive framework to better understand the right to privacy in today's world of smartphones, sensors, and apps. It is argued that the right to privacy should be conceived as a network of capabilities, which empowers an individual to control the boundary between herself and others regarding personal data generated by the use of mobile phones, thereby enhancing the technological self-sovereignty of the data subject. The key capabilities consist of a set of instrumental freedoms, which allow individuals to effectively control personal data through a multi-layered architecture, while avoiding abusive practices such as exploitation and discrimination. New governance features substantiate these spatiotemporal dimensions of the right to privacy. These common rules are aimed at regulating the bundle of capabilities, the infrastructures, and the stakeholders involved in the generation and processing of personal data, enabling individuals to enjoy a privacy umbrella, not just in one's home or homeland, but ubiquitously and at all times, when using mobile phones.

14. Key Findings and Recommendations

The United Nations expert on privacy stated that the proper realization of the right to privacy in the digital age requires much greater effort. The right to privacy is necessary not just to maintain a free and open space for people and their thoughts, but also to ensure a pluralistic

[20] M. Blanke, J., 2018. Privacy and Outrage.

landscape of diverse-from-society viewpoints. Thus, the right to privacy is crucial to the exercise of the right to freedom of expression. Mapping violations on privacy and freedom of expression rights and developing an analysis of the trends involved, the report suggests some critical issues needing to be addressed in the future. Finally, the report provides a set of recommendations aimed at a better protection of rights to freedom of expression and privacy.[21]

The right to privacy has been regarded as a fundamental human right since the 1948 Universal Declaration of Human Rights was adopted by the United Nations General Assembly. Much has been said about the necessity of the protection of privacy in the digital age. In the 21st century, Internet and mobile penetration expanded almost exponentially, with the number of mobile-broadband subscriptions worldwide now almost equaling the global population. Given that individuals are communicating, sharing and disseminating information more than ever with such devices, the volume of personal data generated and stored is now vast and unprecedented. At the same time, many governments have been found to adopt unjustified data protection practices, regulating public communication and with little regard to privacy protection. Given a concern for the right to privacy, together with the right to freedom of expression, it is important to assess the impact of digital communication practices on the deployment of these rights.

References:

M. Blanke, J., 2018. Privacy and Outrage. [PDF]

B. Serwin, A., 2009. Privacy 3.0-The Principle of Proportionality. [PDF]

J. Gstrein, O. & Beaulieu, A., 2022. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. ncbi.nlm.nih.gov

A. Tsoukalas, I. & D. Siozos, P., 2011. Privacy and Anonymity in the Information Society – Challenges for the European Union. ncbi.nlm.nih.gov

Levin, A., 2017. Has the Era of Privacy Come to an End?. [PDF]

H. Çinar, Özgür, 2019. The right to privacy in international human rights law. [PDF]

Shelton, A., 2014. A Reasonable Expectation of Privacy Online: Do Not Track Legislation. [PDF]

Green, D., 2018. Big Brother is Listening to You: Digital Eavesdropping in the Advertising Industry. [PDF]

Han, D., 2017. The Market Value of Who We Are: The Flow of Personal Data and Its

[21] Ebrahim Dorraji, S. & Barčys, M., 2015. Privacy in digital age: dead or alive?! Regarding the new EU data protection regulations.

Regulation in China. [PDF]

Basu, S., 2012. Privacy Protection: A Tale of Two Cultures. [PDF]

W. Luk, J., 2002. Identifying Terrorists: Privacy Rights in the United States and the United Kingdom. [PDF]

Hum, M., 2013. Biometric ID Cybersurveillance. [PDF]

Burkhardt, B., Borradaile, G., & Gelvin, B., 2023. Racial Equity in Police Use of Social Media Monitoring Software. osf.io

Cover, A., 2015. Corporate Avatars and the Erosion of the Populist Fourth Amendment. [PDF]

L. Mills, J. & Harclerode, K., 2018. Privacy, Mass Intrusion and the Modern Data Breach. [PDF]

Celiktutan, B., Cadario, R., & K. Morewedge, C., 2024. People see more of their biases in algorithms. ncbi.nlm.nih.gov

Wang, X., Cheng Wu, Y., Ji, X., & Fu, H., 2024. Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices. ncbi.nlm.nih.gov

Stewart, K., 2017. Looking Backward, Moving Forward: What Must be Remembered When Resolving the Right to be Forgotten. [PDF]

Rivkin-Haas, E., 2011. Electronic Medical Records and the Challenge to Privacy: How the United States and Canada are Responding. [PDF]

Zeide, E., 2017. The Limits of Education Purpose Limitations. [PDF]

Nottingham, E., Stockman, C., & Burke, M., 2022. Education in a datafied world: Balancing children's rights and school's responsibilities in the age of Covid 19. ncbi.nlm.nih.gov

Anatolyevna Kuznetsova, O. & Bondarenko, N., 2017. Private Life Safety Provision in Digital Age. [PDF]

Michael Froomkin, A., 2000. The Death of Privacy?. [PDF]

V. Jr. Posadas, D., 2017. After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy. [PDF]

Humerick, M., 2018. Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence. [PDF]

Ebrahim Dorraji, S. & Barčys, M., 2015. Privacy in digital age: dead or alive?! Regarding the new EU data protection regulations. [PDF]