INTERNATIONAL ECONOMIC LAW

DOI: 10.24833 / 0869-0049-2019-1-18-26

Lothar DETERMANN
Baker & McKenzie LLP
660, Hansen Way, Palo Alto, USA, CA 94304
Lothar.Determann@bakermckenzie.com
ORCID: 0000-0002-5972-8309

Received 18 December 2018
Accepted 28 February 2019

PRIVACY AND DATA PROTECTION

INTRODUCTION. *This article provides an overview regarding privacy and data protection laws and principles around the world. It is based on lectures by the author on May 17, 2018 at Moscow State Institute of International Relations (MGIMO) and Lomonosov Moscow State University (MSU) on the occasion of the publication of a Russian version of the 3rd edition of Determann's Field Guide to Data Privacy Law.*
MATERIALS AND METHODS. *Materials include national and international laws and scholarly articles and books relating to privacy and data protection. Methods follow general principles of German and United States legal commentary.*
RESEARCH RESULTS. *People, societies and governments value and protect privacy quite differently around the world. Consequently, data privacy, data security and data protection laws and policies vary significantly. Particularly pronounced are differences in the approach to the protection of privacy and information freedom and data processing regulation in the United States and the European Union.*
DISCUSSION AND CONCLUSIONS. *Law and policy makers around the world must analyze and balance their people's specific needs for privacy, security, freedom of information, technical progress, economic development and other values and objectives as they decide whether to adopt European Union-style data processing regulation, enact specific individual privacy laws as the United States, or pursue alternative approaches. They need to consider the different meanings of individual privacy, data security, information self-determination and data protection, as well as the different functions of data privacy laws, data processing regulation, record retention statutes and data residency requirements.*
KEYWORDS: *privacy, data protection, data protection laws and principles, the USA, European Union, Federal Republic of Germany*

FOR CITATION: Determann L. Privacy and Data Protection. – *Moscow Journal of International Law.* 2019. No. 1. P. 18–26.
DOI: 10.24833 / 0869-0049-2019-1-18-26

МЕЖДУНАРОДНОЕ ЭКОНОМИЧЕСКОЕ ПРАВО

DOI: 10.24833 / 0869-0049-2019-1-18-26

Лотар ДЕТЕРМАНН
Baker & McKenzie LLP
660, Hansen Way, Palo Alto, USA, CA 94304
Lothar.Determann@bakermckenzie.com
ORCID: 0000-0002-5972-8309

Поступила в редакцию: 18.12.2018
Принята к публикации: 28.02.2019

КОНФИДЕНЦИАЛЬНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

ВВЕДЕНИЕ. *В статье представлен обзор правового регулирования защиты частной жизни и персональных данных во всем мире. Статья основана на лекциях автора, прочитанных 17 мая 2018 г. в Московском государственном институте международных отношений (МГИМО) и Московском государственном университете им. М.В. Ломоносова (МГУ) и приуроченных к публикации русской версии третьего издания «Путеводителя в правовом регулировании персональных данных Лотара Детерманна».*

МАТЕРИАЛЫ И МЕТОДЫ. *Материалом для данной статьи послужили национальное и международное право, научные статьи и книги, касающиеся защиты частной жизни и персональных данных. Методы следуют общим принципам юридического комментария Германии и США.*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *Во всем мире люди, общества и правительства поразному оценивают и защищают частную жизнь. Следовательно, значительно различаются законы и политика в сфере конфиденциальности, безопасности и защиты данных. Особенно разнятся подходы к правовому регулированию защиты частной жизни, свободы информации и обработки данных в Соединенных Штатах и Европейском союзе.*

ОБСУЖДЕНИЕ И ВЫВОДЫ. *Законодатели и политики во всем мире находятся перед выбором: перенять ли подход Европейского союза к регулированию обработки данных, или принять, как в Соединенных Штатах, отдельные отраслевые законы о защите частной жизни, или же искать альтернативные подходы. Однако прежде всего они должны проанализировать и найти баланс между конкретными потребностями своих граждан в защите частной жизни, безопасности, свободе информации, техническом прогрессе, экономическом развитии, а также в других ценностях и целях. Им необходимо учитывать разное понимание частной жизни, безопасности данных, информационной самостоятельности и защиты данных, а также различные задачи, поставленные перед законами о защите частной жизни, об обработке данных, о хранении записей и локализации данных.*

КЛЮЧЕВЫЕ СЛОВА: *конфиденциальность, защита персональных данных, правовое регулирование защиты персональных данных, принципы правового регулирования персональных данных, США, Европейский союз, Федеративная Республика Германия*

ДЛЯ ЦИТИРОВАНИЯ: Детерманн Л. 2019. Конфеденциальность и защита персональных данных. – *Московский журнал международного права.* № 1. С. 18–26.
DOI: 10.24833 / 0869-0049-2019-1-18-26

1. Privacy

Privacy is a sphere that a person controls regarding his mind, thoughts, decisions, communications, body, dignity, home and personal effects, such as papers and smart phones. The right to privacy is the right of an individual to be let alone [Warren, Brandeis 1890:193]. It is a right against other people and legal entities, including family members, neighbors, company representatives and government agents, who may invade a person's privacy by trespassing, entering a person's home without permission, accessing personal files on a computer or forcing a person to reveal sensitive personal information about herself.

One can find privacy best where no other people are, in solitude, furthest away from other humans. In civilization, one trades privacy for benefits of living and interacting with others. One lets other people into one's life to learn, communicate, collaborate, trade, socialize and seek help. One individual's right to privacy can become an intrusion into another person's rights to information, free speech or security.

With respect to information specifically, privacy means control over the dissemination of personal information, discretion regarding who may know what about one's body and mind, the choice to remain anonymous, the ability to keep thoughts and communications confidential, and the power to avoid being photographed, filmed or audiotaped.

Individuals feel different needs for data privacy depending on their personal circumstances. A child prodigy living in a large city may physically suffer from excessive invasions into privacy by journalists while a reality television star may welcome any publicity she can get. A dissident may depend on data privacy for his life while an established politician may depend on publicity for his livelihood.

Also, people in different cultures, societies and political systems feel differently about privacy. Americans in the United States care deeply about individual freedom, property and privacy in their homes and personal effects, but tend to be less concerned about data collected on public spaces or the Internet.

Germans have created the world's first and strictest regulation of data processing, but they have not coined an exact equivalent of "privacy" in the German language. In everyday language, Germans may occasionally refer to "Privatsphäre" (literally translated: "private sphere") as an abstract sphere in which the state and other persons should not interfere. Unlike the U.S. concept of "privacy", German "Privatsphäre" is not directly linked to one's home or property. German lawyers additionally use terms like "informationelle Sebstbestimmung" (information self-determination) and "Datenschutz" (data protection) with respect to the regulation of data processing, which exists separately from civil law claims pertaining to violations of one's rights to private sphere and personality.

In Russia, views and terminology regarding privacy have been evolving, particularly since the end of the Soviet Union and communism, which prioritized collective objectives over individual privacy. A direct equivalent of "privacy" has not yet evolved in the Russian language. "Приватность" is a modern borrowed term derived from the English term "private". "Конфиденциальность" means literally "confidentiality" but has been used to translate "privacy" in the past; for example, "Privacy Policy" has commonly been translated as "политика конфиденциальности". More recently, "приватность" is used to translate "privacy". The closest equivalent to "private sphere" is "неприкосновенность частной жизни", which means literally the "sanctuary of private life" and is used in literature and legislation but not in everyday language. "Информационная приватность" means "information privacy" and "data protection" means "защита персональных данных" and is commonly found in in Russian legislation. For example, the Russian Data Protection Law is called "Федеральный закон 'О персональных данных'".

Around the world, data privacy needs have changed over time and increased exponentially with the development of information technologies. In the 18th century, citizens were most concerned about physical privacy intrusions in the form of arrests, searches and seizures by government agents. In the 19th century, as photography developed, privacy invasion by the press became more noticeable. In the 20th century, computers, data bases and the Internet started to provoke fears of glass citizens, repressive surveillance states and intrusive business practices. Today, mobile phones, connected cars, planes, trains, industrial machines, toys and other devices on the Internet of Things (IoT) generate vast amounts of data and information and the total amount of stored data worldwide is expected to double every two years.

2. Privacy Law and Data Processing Regulation

As individuals have felt an increasing need for data privacy over time, states enacted laws protecting privacy. Express references to privacy can be found increasingly in constitutions, international treaties and statutes since the second half of the last century

[Koops et al. 2017:483–575; Banisar, Davies 1999:1–112; Bygrave 1998:247–284].

2.1. Constitutional Safeguards. The United States maintain the oldest written constitution. Its bill of rights dates back to 1791 and does not contain an express right to privacy, only a limited prohibition of unreasonable searches and seizures in its fourth amendment. The citizens of the State of California added an express right to privacy to the California Constitution in 1972 by way of a ballot measure in a general election, but there has not been enough consensus in the United States to add such a right to the federal constitution.

Germany enacted its current constitution in 1949 as its "basic law" without expressly referring to "privacy", but protecting human dignity in Art. 1(1), a right to "unfold one's personality" in Art. 2(1), the confidentiality of mail and telecommunications in Art. 10(1) and the sanctity of one's home in Art. 13(1). In December 1983, weeks before the turn to the year for which George Orwell had predicted grave intrusions on individual privacy in his novel "1984", the German Constitutional Court (*Census Act Case 1983*) recognized an implied right to information self-determination emanating from the express rights to dignity and personality in Art. 1(1) and 2(1) when German citizens challenged an expansive federal census measure.

Newer constitutions tend to expressly protect a right to privacy, including, for example, the constitutions of Russia (Articles 23, 24 and 25) and South Africa (Section 14).

2.2. International Treaties. The Universal Declaration of Human Rights of 1948 refers to privacy expressly in Article 12, as do the subsequently adopted International Covenant on Civil and Political Rights (Article 17), UN Convention on Migrant Workers (Article 14), UN Convention of the Rights of the Child (Article 16), European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8) and the American Convention on Human Rights (Article 11). The Charter of Fundamental Rights of the European Union does not refer to privacy, but protects a right to "private life" in Art. 7 and the "protection of personal data" in Art. 8.

2.3 Statutes. National statutes protecting privacy have become more common since in 1970 the state Hessen in Germany enacted the first data protection law worldwide. When governor Oswald signed the Hessian data protection law into force, he referred to George Orwell's novel "1984" and declared that the Hessian data protection law was intended to prevent the surveillance state forecasted by Orwell. Other countries in Europe followed. The European Community then harmonized national data protection laws in Directive 95/46/EC (the "Data Protection Directive"), which the European Union replaced effective 2018 by a General Data Protection Regulation (GDPR).

More and more countries have followed Europe and also regulated the processing of personal data with general data protection regulations. In August 2018, Brazil enacted a GDPR-like data protection law and India published a GDPR-like bill which is expected to pass soon [Determann, Gupta 2018].

The United States, on the other hand, have so far opted against broad omnibus data processing regulation. Since the early 1970s, Congress and state legislatures have been enacting hundreds of sector-, situation- and harm-specific data privacy laws.

3. Policy Reasons for Privacy Protections and Limitations

Governments typically protect privacy to safeguard individual human dignity and freedom. Under the shield of data privacy protection, citizens are more empowered to exercise civil rights, such as the freedom of speech, religion and assembly. This in turn helps secure the functioning of the democratic process. Also, citizens need protection from psychological, economic and other privacy harms that states, businesses, criminals and others cause, for example by identity theft; blackmail; bullying; stalking; revelation of secret location or identities of spies, domestic abuse victims or persons in witness protection programs; stigmatization based on addictions, diseases, political opinions, religion, race or sexual preferences; computer hacking; irritating direct marketing methods; unfair business practices based on surreptitious data collection; and discrimination by employers, banks and insurance companies based on information about pre-existing health conditions [Citron 2019; Solove 2002:1087–1156; Solove, Citron 2017; Calo 2018:361–364; Hu 2016:1735–1809; Hurley, Adebayo 2016:148,151; Datta, Tschantz, Datta 2015:92–112; Citron, Pasquale 2014:15].

There are also reasons why – and situations when – governments do not protect, but rather invade privacy. The executive branch of governments fulfills many functions, most importantly law enforcement, that necessitate data processing and tend to collide with privacy protection agendas. Additionally, legislatures and courts also safeguard interests and policy objectives that conflict with data privacy, such as freedom of information and commercial

enterprise. One person's right to gather and share information on another person can intrude on the other person's interest in data privacy. Different jurisdictions balance these conflicting policy goals differently.

The U.S., for example, tends to hold freedom of speech, information and commercial enterprise in relatively high regard and therefore decided against enacting the kind of omnibus data protection laws that are prevalent in Europe. Also, after the terrorist attacks of September 11, 2001, the United States has been very focused on national security and ramping up government surveillance programs. In Europe, on the other hand, people still remember what surveillance by totalitarian regimes has done to them. European lawmakers have decisively acted to limit the automated processing of personal data and carved out narrowly defined exceptions for press, media and non-commercial activities. Anyone trying to understand, interpret and apply data privacy laws has to consider the various conflicting interests and their relative status in the applicable legal system.

Without security, there can be no privacy; criminals, companies and foreign governments will invade individual privacy if security is not safeguarded. There can be security without any privacy, though. A totalitarian state focused on absolute security will monitor all individuals at the expense of their privacy. There cannot be free speech and democracy without privacy or security. Societies have to strike a balance with respect to privacy and security.

4. Legislative Approaches

The terms "data privacy" and "data protection" are often used interchangeably, in particular in the context of comparisons of Anglo-Saxon data privacy laws and continental European data protection laws. Also, data security, data residency, data retention, data ownership and trade secret requirements are often thrown into the mix. But, the approaches, purposes and effects are quite different.

4.1. Privacy Protection. The individual person and her autonomy is the central focus of privacy laws. Data privacy laws are intended to protect individuals from intrusion into reasonable privacy expectations, interception of confidential communications and other specific privacy harms.

Data privacy laws typically contain requirements regarding notice, choice, data security and sanctions. Individuals must be notified about how their data is handled so they can decide how much information they share, with whom and for what consideration. If they have access to sufficient information in privacy policies and other notices, they can adjust their conduct or privacy expectations. In particularly sensitive scenarios, companies may need to obtain express and informed consent. If companies fail to live up to their commitments in privacy policies or apply reasonable security safeguards and cause harm, then individuals can assert claims in private lawsuits including class actions. Regulators and law enforcement authorities can also sanction offenders in particularly egregious privacy law violations.

4.2. Data Protection. The processing of personal data is the central focus of data protection laws. European legislatures have taken George Orwell's warnings to heart and view automated data processing as an inherently dangerous activity warranting strict regulation.

The GDPR, like previous EU data protection regulation, builds restrictions and limited exceptions around a fundamental prohibition of any processing of personal data in Art. 6(1) GDPR. European data protection laws are first and foremost intended to restrict and reduce automated processing of personal data. Individual privacy expectations, harm potential, choice or consent are not predominantly relevant. Accordingly, broad definitions of "personal data" and "processing" prevail and even publicly available data is covered. Companies are required to minimize the amount of data they collect, the instances of processing, the people who have access and the time periods for which they retain data.

Besides basic prohibitions and minimization principles, data protection regulations typically establish data protection authorities, impose registration and approval requirements, prescribe filing fees, mandate the designation of local representatives and internal data protection officers, restrict international data transfers, mandate data protection impact assessments and require that companies maintain data inventories and accountability documentation that data protection authorities can routinely audit. Data protection authorities are also primarily tasked with enforcing data protection laws.

Data protection laws can indirectly benefit individual privacy if they cause companies and governments to process less personal data. But, protecting individual privacy is not the direct focus of the GDPR or other EU data protection laws. Individual privacy expectations, needs or harms can factor into data protection impact assessments, determinations whether security breaches have to be notified under Art. 33 or 34 GDPR, and the application of Art. 6(1)(f) GDPR, the "legitimate interest exception"

to the general prohibition of automated data processing. But, many other requirements and restrictions apply regardless of individual privacy considerations.

4.3. Data Security Laws. Legislatures around the world have started to supplement data privacy laws with increasingly specific data security laws that aim to protect individuals from specific harms resulting from unauthorized access to personal information, in particular identity theft. Examples include data security breach notification laws: California passed the first law in 2002, with most U.S. states and many countries following suit thereafter. Also, more and more laws prescribe encryption or other technical and organizational measures, also known as "TOMs". In 2018, California added a duty on manufacturers of connected devices to design products with reasonable security measures and refrain from delivering products with default passwords, for example. Data security measures limit unauthorized access to information and thus protect data and individual privacy.

4.4. Trade Secret Laws. Businesses use contracts and tort laws to protect confidential information from misappropriation by unauthorized persons. As a condition to trade secret claims, companies have to prove that they used reasonable efforts to keep their information secret, which often includes similar measures as required by data security laws with respect to personal data. Where confidential business information pertains to persons (as opposed to technologies or manufacturing processes, for example), trade secret law can also indirectly protect individual privacy. But, the primary purpose of trade secret laws is to protect business integrity and competition from unfair misappropriation of valuable confidential information.

4.5. Data Ownership. With property laws, states allocate real estate, chattels, intangibles or other items to individuals with an entitlement to exclude others in the interest of incentivizing innovation, creation, maintenance and investment regarding the allocated items. Legislatures typically exclude information as such from the scope of property laws, to preserve maximum public access. Also, it seems hardly necessary or in the public interest to incentivize the creation of information. Even without rewards in the form of property rights, companies and governments hoard enough data at the expense of individual privacy.

If individuals owned personal data about themselves, they could theoretically gain additional rights to defend their privacy. In practice, however, many individuals would likely be induced or compelled to sell their personal data property rights, with the undesirable effect that the buyers could exclude the data subjects from personal information about themselves. Others could use property rights to withhold information about themselves that governments, companies or individuals legitimately need for public safety, security or other purposes. Therefore, no own owns or should own data [Determan 2018b].

4.6. Freedom of Speech and Information. Individuals and their right to communicate and inform themselves is the core function of constitutional freedoms of communication and information. Privacy rights can directly conflict with rights to free speech and information. For example, defamation claims, censorship measures and "rights to be forgotten" can be based on privacy laws and restrict the dissemination of information or access to data. Privacy rights can also complement rights to free speech and information, because people can speak more freely when they can remain anonymous or at least hide or obscure their identities from government or private prosecution. But, freedoms of speech and information do not typically protect privacy and rather intrude.

4.7. Data Residency and Retention Requirements. Governments mandate that companies and citizens maintain certain documentation, records and information locally for minimum time periods, to be available for tax audits, law enforcement investigations and national security monitoring. Russia, Kazakhstan, Indonesia and the People's Republic of China have enacted particularly broad data residency requirements that are not limited to particular types of records but all personal data. Data residency and retention laws are not intended to protect privacy. To the contrary, such laws limit individual privacy. European Union laws requiring companies to store Internet meta data for minimum time periods have been successfully challenged and invalidated based on constitutional safeguards for data privacy[1].

[1] See Judgment of the Court (Grand Chamber) dated April 8, 2014 (requests for a preliminary ruling from the High Court of Ireland (Ireland) and the Verfassungsgerichtshof (Austria)) — *Digital Rights Ireland Ltd. (C-293/12) v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12)*. Joined Cases C-293/12 and C-594/12. URL: http://curia.europa.eu/juris/documents.jsf?num=c-293/12 (accessed date: 12.12.2018).

5. International Privacy Law at Crossroads

More and more countries are enacting or updating privacy laws based on one or more of the approaches described in the preceding Part 4 of this Article. Many jurisdictions enact European-style data processing legislation and few follow the United States. In fact, United States itself is currently reconsidering its own approach. International privacy laws are at crossroads.

5.1. Privacy v. Data Protection. When Hessen and then other German states and European countries started enacting data protection laws in the 1970s, the United States also considered this option, but decided against comprehensive regulation of data processing. Congress felt it was too early to appropriately identify and address potential privacy harms and balance privacy interests with freedom of information, innovation and economic freedoms [Schwartz 2008:902, 910–916]. Therefore the United States resolved to pass sector-, situation- and harm-specific privacy laws as the need arises, at the state and federal level. This allowed information technology companies in the Silicon Valley to grow and become industry leaders in semiconductor technologies, software, e-commerce, cloud computing, social media, big data and other data intensive products and services [Chander 2014:639–694]. But, this also resulted in hundreds of diverging and constantly evolving privacy laws across the United States. Companies and government agencies find it increasingly difficult to navigate the maze of U.S. privacy laws. Businesses are particularly concerned about the California Consumer Privacy Act of 2018, which adds extensive new disclosure requirements and individual rights to existing laws in order to reign in perceived risks emanating from data selling [Determann 2018a:312–316].

Calls have become louder for uniform federal privacy laws in the United States. Politicians, government authorities, activists, businesses and consumers agree in principle that broad federal legislation is warranted. Disagreements prevail, however, over important questions of detail, including whether a new federal law should preempt (that is: invalidate) or merely supplement existing state laws, and whether the United States should adopt European-style data processing regulations or continue the U.S. tradition of individual privacy protections.

5.2. Adequacy of EU Regulations of Data Processing. The EU hails its GDPR as the most modern data protection law worldwide and claims authority in Art. 45 GDPR to formally decide whether the level of data protection in other countries is adequate. At the same time, critics, including in the German government, are questioning whether the GDPR itself is truly adequate [Veil 2018:686–696]. The European approach from the 1970s to broadly prohibit processing of personal data, subject to a limited number of exceptions, seems even more unrealistic and impractical today where information technologies are so developed and omnipresent. European calls to elevate privacy to a fundamental human right may be merely "rights talk" [Schwartz, Peifer 2017:138].

The genie is out of the bottle. Data processing technologies are here to stay. Data collection, usage and sharing will increase, in fact: must increase, to better research and cure diseases; treat patients with personalized, precision medicine; develop artificial intelligence; enable autonomous cars to recognize and protect people; support global communications; create reliable block-chains; and protect national and international security. EU-style data minimization and prohibitive regulation is counter-productive to pursuing the many opportunities of data-driven innovation. Also, vast amounts of sensitive personal data on most people is already stored in numerous legitimate and illegal data bases around the world[2].

European companies and governments are using – and will continue to use – very similar technologies, products and services as their U.S. counterparts. Today, most information technologies, products and services are developed by industry leaders outside of Europe, but individual data subjects in Europe are exposed to the same privacy harms and concerns in the EU as elsewhere. Also, omnibus data protection laws that try to regulate everything are unreasonably vague and difficult to update. It took the European Union more than 20 years to replace the Data Protection Directive with the GDPR effective 2018. Moreover, the Data Protection Directive of 1995 merely constituted a harmonized version of national data protection laws from the 1970s, before private television, the Internet, mobile phones, big data, cloud computing and other technologies arrived on the scene.

5.3. Why Then Follow Europe? Despite the obvious shortcomings of European data protection laws,

[2] See McMillan R. Thieves Can Now Nab Your Data in a Few Minutes for a Few Bucks. – *The Wall Street Journal.* December 9, 2018. URL: https://www.wsj.com/articles/what-happens-to-your-data-after-a-hack-1544367600 (accessed date: 12.12.2018).

more and more countries outside Europe have enacted similar laws. One reason are benefits for cross-border trade if the EU finds data protection laws of another country "adequate". The procedure contemplated by the Data Protection Directive and also in the GDPR has yielded somewhat surprising results: Since 1995, only Argentina, Canada, Israel, Japan, New Zealand, Uruguay and a few smaller countries have been found to have "adequate levels of data protection".

Another reason is that the United States approach has become unmanageable in practice. In the 1970s, the United States shied away from enacting European-style general data protection laws for fear such laws could suffocate innovation and become too difficult to update and supplement as privacy threats evolve. Since then, the United States enacted and updated hundreds of threat- or sector-specific privacy laws, each narrowly crafted, but cumulatively suffocating in their own way. The California Consumer Privacy Act of 2018 (CCPA) imposes overly complex and detailed obligations on companies that are not compatible with requirements of other jurisdictions. Businesses can no longer navigate the maze. The United States need a reform centered around federal legislation.

But, perhaps the most important reason is that crafting tailored and balanced privacy laws is very difficult. Lawmakers find it relatively easy to craft data security and data protection legislation. Anyone can agree on what good security looks like: unauthorized person do not have access to confidential information. Also, if one accepts with EU lawmakers that the processing of personal data is predominantly harmful and dangerous, then one can easily agree on data minimization and the various procedural and administrative requirements contained in the GDPR.

Crafting balanced and proportionate privacy laws focused on preventing harm while protecting free speech, information and innovation, however, is much more difficult. We do not all agree on what good *privacy* looks like. A defendant who demands that the police stay out of his home or computer obstructs criminal investigations or national security measures. A patient who objects to clinical trials or research prevents medical progress and cures. An employee who objects to workplace monitoring makes it harder for employers to prevent harassment and theft of trade secrets. A politician who demands a "right to be forgotten" intrudes on freedoms of speech and information rights of other citizens.

Data subjects are not harmed by the processing of personal data as such. Concerns pertain to particular abuses of data processing, such as discrimination by employers, health insurance companies and law enforcement. But, it is difficult for policymakers to agree on the dividing lines between legitimate use and abuses. For example, some believe that insurance companies should be permitted to consider how healthy policy holders (people) live and offer discounts to non-smokers or based on exercise and eating habits to encourage lower risk behaviors. Others see an unfair penalty for smokers or overweight people and feel violated in their privacy if insurance companies monitor their exercise levels and consumption habits.

Moreover, it is difficult to enforce laws that are narrowly focused on prohibiting certain abuses. It is much easier to just prohibit the collection of personal data in the first place, so the data cannot be abused. But, this seems like overkill. States do not prohibit cars to reduce car accidents either and instead enact differentiated traffic rules, even if they are harder to craft and enforce than a complete prohibition of cars. Similarly, we need differentiated rules focused on privacy harms, which need to be constantly updated as technologies and threats evolve.

Policymakers should focus on particular privacy harms and craft legislation that balances privacy and other interests proportionally. Legislatures should not continue with the European approach of broadly prohibiting or regulating the processing of personal data, because this has not lead to effective privacy protections in Europe in the past and only prevented scientific and commercial progress in the information technology sector, which is now globally dominated by non-European companies. Data processing as such is not harmful to individuals, but necessary and largely beneficial. Lawmakers should encourage and enable secure data sharing and direct their efforts to enforce existing laws to prevent and pursue abuses such as cybercrime, fraud and harmful discrimination. If lawmakers enact broadly applicable general privacy laws to define baselines, they must be careful to prevent ossification and leave room for updates and upgrades as technologies and business practices evolve and new threats emerge.

6. Conclusion and Outlook

The United States and other countries find themselves at crossroads with respect to data privacy legislation. The rigid regulatory and prohibitive approach in Europe has been largely ineffective and hindered the development of information technologies in Europe. The GDPR repeats and doubles down

on regulatory concepts of the 1970s and does not have answers for today's or tomorrow's challenges. Technology companies have fared better in the United States under narrowly crafted privacy laws, but evolving technologies and privacy threats have triggered so many specific laws that the legal environment has become unmanageably complex. Data privacy law reform should focus on actual harms and remain flexible to allow frequent updates and adjustments as technologies and threats evolve.

References

1. Banisar D., Davies S. Global Trends in Privacy Protection. – *Journal of Computer and Information Law.* 1999. Vol. XVIII. Issue 1. P. 1–112.
2. Bygrave L.A. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. – *International Journal of Law and Information Technology.* 1998. Vol. 6. P. 247–284.
3. Calo R. Privacy Harm Exceptionalism. – *Colorado Technology Law Journal.* 2018. Vol. 12. Issue 2. P. 361–364.
4. Chander A. How Law Made Silicon Valley. – *Emory Law Journal.* 2014. Vol. 63. Issue 3. P. 639–694.
5. Citron D.K. Sexual Privacy. – University of Maryland Legal Studies Research Paper. 2018. No. 2018-25. 83 p.
6. Citron D.K., Pasquale F. The Scored Society: Due Process for Automated Predictions. – *Washington Law Review.* 2016. Vol. 89. Issue 1. P. 1–33.
7. Datta A., Tschantz M.C., Datta An. Automated Experiments on Ad Privacy Settings. – *Proceedings on Privacy Enhancing Technologies.* 2015. Issue 1. P. 92–112. DOI: https://doi.org/10.1515/popets-2015-0007
8. Determann L. *California Privacy Law. Practical Guide and Commentary U.S. Federal and California Law.* 3rd ed. Portsmouth: International Association of Privacy Professionals. 2018a. 600 p.
9. Determann L. No One Owns Data. – *UC Hastings Research Paper.* 2018b. No. 265. 44 p.
10. Determann L., Gupta Ch. Indian Personal Data Protection Act, 2018: Draft Bill and Its History, Compared to EU GDPR and California Privacy Law (September 3, 2018). – *UC Berkeley Public Law Research Paper.* 2018. 27 p. DOI: http://dx.doi.org/10.2139/ssrn.3244203
11. Hu M. Big Data Blacklisting. – *Florida Law Review.* 2016. Vol. 67. Issue 5. P. 1735–1809.
12. Hurley M., Adebayo J. Credit Scoring in the Era of Big Data. – *Yale Journal of Law and Technology.* 2016. Vol. 18. Issue 1. P. 148–216.
13. Koops B.-J. et al. A Typology of Privacy. – *University of Pennsylvania Journal of International Law.* 2017. Vol. 38. Issue. 2. P. 483–575.
14. Schwartz P.M. Preemption and Privacy. – *Yale Law Journal.* 2008. Vol. 118. P. 902–947.
15. Schwartz P.M., Peife K.M. Transatlantic Data Privacy Law. – *The Georgetown Law Journal.* 2017. Vol. 106. P. 115–179.
16. Solove D.J. Conceptualizing Privacy. – *California Law Review.* 2002. Vol. 90. Issue 4. P. 1087–1156. DOI: https://doi.org/10.15779/Z382H8Q
17. Solove D.J., Citron D.K. Risk and Anxiety: A Theory of Data-Breach Harms. – *GWU Law School Public Law Research Paper.* 2017. No. 2017-2. 42 p. URL: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2499&context=faculty_publications (accessed date: 12.12.2018).
18. Veil W. The GDPR: The Emperor's New Clothes – On the Structural Shortcomings of Both the Old and the New Data Protection Law. – *Neue Zeitschrift für Verwaltungsrecht.* 2018. Vol. 10. P. 686–696.
19. Warren S.D., Brandeis L.D. The Right to Privacy. – *Harvard Law Review.* 1890. Vol. 4. Issue 5. P. 193–220.

About the Author

Lothar Determann,
partner, Baker & McKenzie LLP

660, Hansen Way, Palo Alto, USA, CA 94304

Lothar.Determann@bakermckenzie.com
ORCID: 0000-0002-5972-8309

Информация об авторе

Лотар Детерманн,
партнер, Baker & McKenzie LLP

660, Hansen Way, Palo Alto, USA, CA 94304

Lothar.Determann@bakermckenzie.com
ORCID: 0000-0002-5972-8309