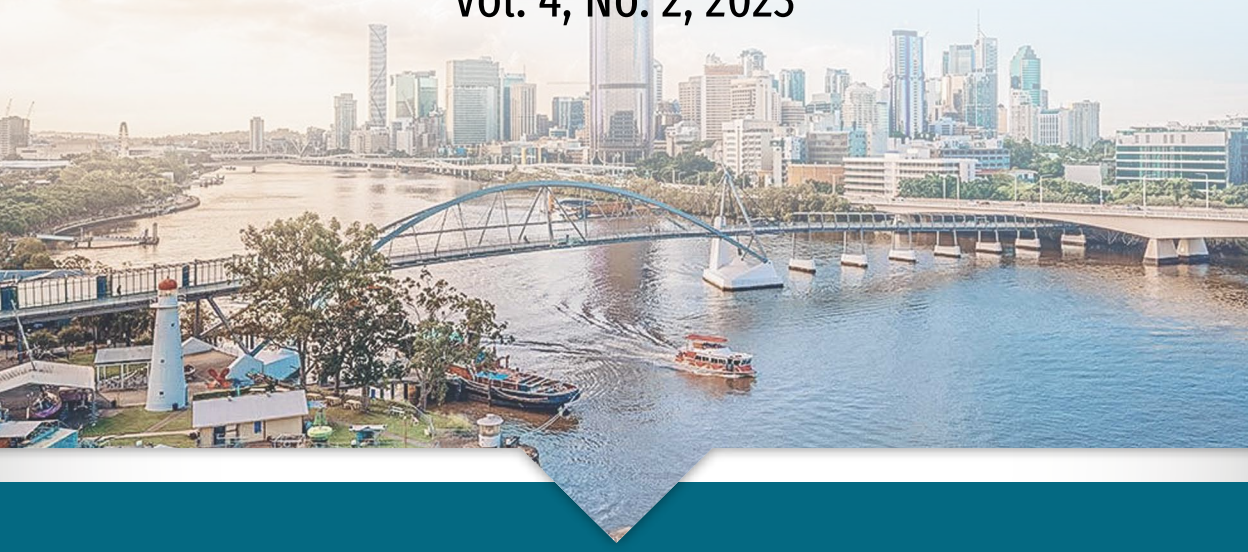
ISSN 2686-9136 (Online)

DIGITAL LAW JOURNAL

Vol. 4, No. 2, 2023



INTERVIEW

8 Whatever Technology Appears, We Remain Human
Tatiana S. Yatsenko

ARTICLES

15 Privacy in the Age of Remote Sensing During Natural Disasters in Australia and Indonesia
Temitope Lawal, Melanie Jackson, Eugenia Georgiades

40 Electronic Form of Transactions: Issues of Legal Regulation
Roman I. Shugaev

64 Biotechnologies and Patent Law: The Case of European Union
Alena I. Shcherbakova

BOOK REVIEW

73 Phenomenon of Digital Platforms and Legal Regulation
Max Gutbrod

DIGITAL LAW JOURNAL

DIGITAL LAW JOURNAL

Journal of research and practice

Published since 2020
4 issues per year

Vol. 4, No. 2, 2023

ЦИФРОВОЕ ПРАВО

Научно-практический журнал

Журнал издается с 2020 г.
4 выпуска в год

Том 4, № 2, 2023

Contents

Interview

8 Whatever Technology Appears, We Remain Human

Tatiana S. Yatsenko

Articles

15 Privacy in the Age of Remote Sensing During Natural Disasters in Australia and Indonesia

Temitope Lawal, Melanie Jackson, Eugenia Georgiades

40 Electronic Form of Transactions: Issues of Legal Regulation

Roman I. Shugaev

64 Biotechnologies and Patent Law: The Case of European Union

Alena I. Shcherbakova

Book Review

73 Phenomenon of Digital Platforms and Legal Regulation

Max Gutbrod

Содержание

Интервью

8 Какие бы технологии ни появлялись, мы остаемся людьми

Т.С. Яценко

Статьи

15 Конфиденциальность в эпоху дистанционного зондирования стихийных бедствий в Австралии и Индонезии

Т. Лаваль, М. Джексон, Е. Георгиадес

40 Электронная форма сделок: вопросы правового регулирования

Р.И. Шугаев

64 Биотехнологии и патентное право: опыт Европейского союза

А.И. Щербакова

Рецензия на книгу

73 Феномен цифровых платформ и правовое регулирование

М. Гутброд

DIGITAL LAW JOURNAL

AIMS AND SCOPE

The purpose of the Digital Law Journal is to provide a theoretical understanding of the laws that arise in Law and Economics in the digital environment, as well as to create a platform for finding the most suitable version of their legal regulation. This aim is especially vital for the Russian legal community, following the development of the digital economy in our country. The rest of the world has faced the same challenge, more or less successfully; an extensive practice of digital economy regulation has been developed, which provides good material for conducting comparative research on this issue. Theoretically, "Digital Law" is based on "Internet Law", formed in English-language scientific literature, which a number of researchers consider as a separate branch of Law.

The journal establishes the following objectives:

- Publication of research in the field of digital law and digital economy in order to intensify international scientific interaction and cooperation within the scientific community of experts.
- Meeting the information needs of professional specialists, government officials, representatives of public associations, and other citizens and organizations; this concerns assessment (scientific and legal) of modern approaches to the legal regulation of the digital economy.
- Dissemination of the achievements of current legal and economic science, and the improvement of professional relationships and scientific cooperative interaction between researchers and research groups in both Russia and foreign countries.

The journal publishes manuscripts in the following fields of developments and challenges facing legal regulation of the digital economy:

1. Legal provision of information security and the formation of a unified digital environment of trust (identification of subjects in the digital space, legally significant information exchange, etc.).
2. Regulatory support for electronic civil turnover; comprehensive legal research of data in the context of digital technology development, including personal data, public data, and "Big Data".
3. Legal support for data collection, storage, and processing.
4. Regulatory support for the introduction and use of innovative technologies in the financial market (cryptocurrencies, blockchain, etc.).
5. Regulatory incentives for the improvement of the digital economy; legal regulation of contractual relations arising in connection with the development of digital technologies; network contracts (smart contracts); legal regulation of E-Commerce.
6. The formation of legal conditions in the field of legal proceedings and notaries according to the development of the digital economy.
7. Legal provision of digital interaction between the private sector and the state; a definition of the "digital objects" of taxation and legal regime development for the taxation of business activities in the field of digital technologies; a digital budget; a comprehensive study of the legal conditions for using the results of intellectual activity in the digital economy; and digital economy and antitrust regulation.
8. Legal regulation of the digital economy in the context of integration processes.
9. Comprehensive research of legal and ethical aspects related to the development and application of artificial intelligence and robotics systems.
10. Changing approaches to training and retraining of legal personnel in the context of digital technology development; new requirements for the skills of lawyers.

The Journal has been included in the index of the Higher Attestation Commission (VAK) of the Ministry of Education and Science of the Russian Federation. The subject of the journal corresponds to the group of specialties "Legal Sciences" and "Economic Sciences".

The journal publishes manuscripts in Russian and English.

FOUNDER, PUBLISHER:

Maxim I. Inozemtsev
76, ave. Vernadsky, Moscow, Russia, 119454

Founded:	The journal has been published since 2020
Frequency:	4 issues per year
DOI Prefix:	10.38044
ISSN online:	2686-9136
Mass Media Registration Certificate:	ЭЛ № ФС 77-76948 of 9 Oct. 2019 (Roskomnadzor)
Distribution:	Content is distributed under Creative Commons Attribution 4.0 License
Editorial Office:	76, ave. Vernadsky, Moscow, Russia, 119454, +7 (495) 229-41-78, digitallawjornal.org, dlj@digitallawjournal.org
Published online:	31 July 2023
Copyright:	© Digital Law Journal, 2023
Price:	Free

REGION GROUP OF COMPANIES With support of REGION Group of Companies

ЦИФРОВОЕ ПРАВО

ЦЕЛИ И ЗАДАЧИ

Цель электронного журнала «Цифровое право» (Digital Law Journal) — создание дискуссионной площадки для осмысления в научно-практической плоскости легализации цифровых технологий, особенностей и перспектив их внедрения в нормативно-правовое поле. Особенно остро эта задача стоит перед российским сообществом правоведов в связи с развитием цифровой экономики в нашей стране. С этой же задачей сталкивается и остальной мир, решая её более или менее успешно. В мире сформировалась обширная практика нормативного регулирования цифровой экономики, она даёт хороший материал для проведения сравнительных исследований по этой проблематике. В теоретическом плане цифровое право опирается на сформировавшееся в англоязычной научной литературе академическое направление «интернет-право», которое ряд исследователей рассматривают как отдельную отрасль права.

Задачами журнала являются:

- Публикация исследований в области цифрового права и цифровой экономики с целью интенсификации международного научного взаимодействия и сотрудничества в рамках научного сообщества экспертов.
- Удовлетворение информационных потребностей специалистов-профессионалов, должностных лиц органов государственной власти, представителей общественных объединений, иных граждан и организаций в научно-правовой оценке современных подходов к правовому регулированию цифровой экономики.
- Распространение достижений актуальной юридической и экономической мысли, развитие профессиональных связей и научного кооперативного взаимодействия между исследователями и исследовательскими группами России и зарубежных государств.

В журнале публикуются рукописи по следующим направлениям развития и задачам, стоящим перед нормативным регулированием цифровой экономики.

1. Нормативное обеспечение информационной безопасности, формирование единой цифровой среды доверия (идентификация субъектов в цифровом пространстве, обмен юридически значимой информацией между ними и т. д.).
2. Нормативное обеспечение электронного гражданского оборота; комплексные правовые исследования оборота данных в условиях развития цифровых технологий, в том числе персональных данных, общедоступных данных, Big Data.
3. Нормативное обеспечение условий для сбора, хранения и обработки данных.
4. Нормативное обеспечение внедрения и использования инновационных технологий на финансовом рынке (криптовалюты, блокчейн и др.).
5. Нормативное стимулирование развития цифровой экономики; правовое регулирование договорных отношений, возникающих в связи с развитием цифровых технологий. Сетевые договоры (смарт-контракты). Правовое регулирование электронной торговли.
6. Формирование правовых условий в сфере судопроизводства и нотариата в связи с развитием цифровой экономики.
7. Обеспечение нормативного регулирования цифрового взаимодействия предпринимательского сообщества и государства; определение «цифровых объектов» налогов и разработка правового режима налогообложения предпринимательской деятельности в сфере цифровых технологий. Цифровой бюджет; комплексное исследование правовых условий использования результатов интеллектуальной деятельности в условиях цифровой экономики. Цифровая экономика и антимонопольное регулирование.
8. Нормативное регулирование цифровой экономикой в контексте интеграционных процессов.
9. Комплексные исследования правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники.
10. Изменение подходов к подготовке и переподготовке юридических кадров в условиях развития цифровых технологий. Новые требования к навыкам и квалификации юристов.

Журнал включен в перечень ВАК по следующим специальностям: 5.1.1. Теоретико-исторические правовые науки (юридические науки), 5.1.3. Частно-правовые (цивилистические) науки (юридические науки), 5.1.5. Международно-правовые науки (юридические науки), 5.2.3. Региональная и отраслевая экономика (экономические науки), 5.2.4. Финансы (экономические науки).

В журнале публикуются рукописи на русском и английском языках.

УЧРЕДИТЕЛЬ, ИЗДАТЕЛЬ:

Иноземцев Максим Игоревич
119454, Россия, Москва, просп. Вернадского, 76

История издания журнала:	Журнал издается с 2020 г.
Периодичность:	4 выпуска в год
Префикс DOI:	10.38044
ISSN online:	2686-9136
Свидетельство о регистрации средства массовой информации:	№ ФС 77-76948 от 09.10.2019 (Роскомнадзор)
Условия распространения материалов:	Контент доступен под лицензией Creative Commons Attribution 4.0 License
Редакция:	119454, Россия, Москва, просп. Вернадского, 76, +7 (495) 229-41-78, digitallawjournal.org, dlj@digitallawjournal.org
Дата публикации:	31.07.2023
Копирайт:	© Цифровое право, 2023
Цена:	Свободная

РЕГИОН ГРУППА КОМПАНИЙ При поддержке Группы компаний «РЕГИОН»

https://doi.org/10.38044/2686-9136-2023-4-2-8-14

От редакции

Цифровизация оказывает влияние на существующую систему права. В доктрине все чаще обсуждается вопрос о том, что цифровизация приведет к переосмыслению деления права на частное и публичное. Более того, слышны призывы объявить искусственный интеллект (далее — ИИ) субъектом права. «Цифровой» ревизии подверглись такие, казалось бы, неизменные отрасли, как диффамационное и наследственное право. Редакция журнала «Цифровое право» *(Digital Law Journal)* обсудила вызовы, которые ставит перед юридическим сообществом цифровизация, с Татьяной Сергеевной Яценко.

Яценко Татьяна Сергеевна — руководитель департамента частного права Национального исследовательского университета «Высшая школа экономики», доктор юридических наук, доцент. Окончила юридический факультет Ростовского государственного университета в 1999 г. В 2001 г. успешно защитила кандидатскую диссертацию на тему: «Шикана как правовая категория в гражданском праве». В 2016 г. в Диссертационном совете Московского государственного университета им. М.В. Ломоносова успешно защитила докторскую диссертацию на тему: «Гражданско-правовая охрана публичных интересов» (научный консультант доктор юридических наук, профессор, Заслуженный деятель науки Российской Федерации Е.А. Суханов). В сферу научных интересов Татьяны Сергеевны входят проблемы наследования цифровых активов; защита нематериальных благ и личных неимущественных прав в интернете; охрана прав инвесторов в краудфандинге.

ИНТЕРВЬЮ

КАКИЕ БЫ ТЕХНОЛОГИИ НИ ПОЯВЛЯЛИСЬ, МЫ ОСТАЕМСЯ ЛЮДЬМИ

Интервью с Татьяной Яценко

Т.С. Яценко

Национальный исследовательский университет
«Высшая школа экономики»
109028, Россия, Москва, Большой Трехсвятительский пер., 3

Ключевые слова

цифровое право, интернет-право, Интернет, цифровой субъект, социальные сети, правосубъектность

Для цитирования Яценко, Т.С. (2023). Какие бы технологии ни появлялись, мы остаемся людьми. *Цифровое право,* 4(2), 8–14. https://doi.org/10.38044/2686-9136-2023-4-2-8-14

INTERVIEW

WHATEVER TECHNOLOGY APPEARS, WE REMAIN HUMAN

Interview with Tatiana Yatsenko

Tatiana S. Yatsenko

Higher School of Economics (HSE University)
3, Bolshoy Trekhsvyatitelskiy Pereulok, Moscow, Russia, 109028

Keywords

Digital Law, Internet Law, Internet, digital entity, networks, legal personality

For citation Yatsenko, T.S. (2023). Whatever technology appears, we remain human. *Digital Law Journal,* 4(2), 8–14. https://doi.org/10.38044/2686-9136-2023-4-2-8-14

– Татьяна Сергеевна, в последнее время в доктрине возобновились споры относительно деления права на отрасли[1]. Не последнюю роль в этом сыграло развитие цифровых технологий. Можно ли говорить о том, что сейчас мы наблюдаем формирование новой отрасли права — цифрового права?

– Любое деление права всегда условно и преследует прежде всего научные и образовательные цели. Взять, к примеру, классическое разграничение частного и публичного права, по поводу оснований которого в науке существует множество теорий. Но даже Ульпиан, на которого в этом случае принято ссылаться, говорит лишь о структурировании учебных дисциплин, о том, что «*изучение* права распадается на два положения: публичное и частное (право)»[2], а вовсе не о фактическом разграничении права на публичное и частное. И это логично, поскольку римское частное право охраняло не только частные, но и публичные интересы.

Очевидно, современное деление права на отрасли преследует ту же цель, поскольку система национального права едина и подчиняется общим принципам. В отраслях частного права довольно много публично-правовых по своей природе норм; в публичном праве встречаются частноправовые нормы. Общественные отношения могут составлять предмет регулирования одновременно частного и публичного права.

Предвосхищая Ваш вопрос о неактуальности выделения отраслей по критериям предмета и метода, отмечу, что от него, на мой взгляд, отказаться сейчас невозможно. Использование данных критериев необходимо для понимания специфики связанных между собой норм. Сохраняют эти критерии и свое практическое значение.

Я не вижу специфики предмета и метода у цифрового права. Возможно, она появится в будущем, и мы сможем с уверенностью говорить о самостоятельном характере отрасли цифрового права. Пока же его составляют публично-правовые и частноправовые нормы, которые при их применении не утрачивают своей природы, функционального назначения и особенностей при воздействии на складывающиеся в цифровой среде отношения.

– В одной из своих статей[3] Вы затрагиваете проблему так называемой цифровой идентичности, которая обеспечивает каждому человеку истинное существование в цифровых системах. Не требуется ли, на Ваш взгляд, переосмысление традиционных категорий «правосубъектность», «правоспособность» в контексте цифровизации? Ведь в доктрине все чаще слышны призывы признать, к примеру, в качестве субъекта права искусственный интеллект?

– Когда мы говорим об идентичности человека, мы имеем в виду прежде всего разные атрибуты его личности: имя, изображение, голос и другие нематериальные блага, которые, с одной стороны, индивидуализируют человека, а с другой — могут быть объектами имущественного оборота.

---

1 См., например: Рожкова, М.А. (2020). Является ли цифровое право отраслью права и нужно ли ожидать появления Цифрового кодекса? *Хозяйство и право*, (4), 3–13; Талапина, Э.В. (2021). Сравнительное цифровое право: становление и перспективы. *Журнал российского права, 25*(9), 18–32. https://doi.org/10.12737/jrl.2021.108

2 Кофанов, Л.Л. (отв. ред., пер.) (2002). *Дигесты Юстиниана* (т. 1). Статут.

3 Яценко, Т.С. (2022). Предупреждение правонарушений в цифровой среде: гражданско-правовой аспект. *Российская юстиция*, (5), 71–74.

В цифровой (виртуальной) среде содержание идентичности человека приобретает специфику, которую современное право, к сожалению, не учитывает. Поэтому возникают проблемы, связанные, например, с установлением личности анонимных участников виртуального пространства, их идентификацией и аутентификацией, легализацией сделок с никнеймами, которые по своей природе представляют собой псевдонимы и поэтому в силу действующего регулирования являются неотчуждаемыми от их носителей объектами, с признанием правового статуса аватара как *alter ego* физического лица в Сети, и многие другие.

Решение этих проблем, в том числе на законодательном уровне, требует учета специфики цифровой среды, но не означает, что нужно пересматривать традиционные правовые категории. Изменятся ли понятия «субъект права» или «правосубъектность», если состав субъектов будет расширен, например, за счет ИИ? История с признанием правосубъектности юридических лиц позволяет дать на этот вопрос отрицательный ответ. Другое дело, что закрепление за ИИ статуса субъекта потребует такого регулирования режима его функционирования, которое отвечало бы общему назначению категории субъекта права.

В этой связи прав профессор Е.А. Суханов, который полагает, что условием признания ИИ в качестве субъекта права должно стать наделение его имуществом. Однако в этом случае ИИ, который «обитает» в цифровом пространстве, приобретет целый ряд преимуществ перед людьми, поскольку, например, торгуя на бирже, заключая разного рода сделки, он сможет использовать огромный массив информации, которая недоступна большинству других участников оборота. Разумеется, в связи с признанием правосубъектности ИИ могут возникнуть проблемы и этического толка. Поэтому, прежде чем принимать такое решение, нужно просчитать риски и создать систему их предупреждения в связи с участием ИИ в имущественном обороте.

– В литературе по теории права нередко высказывается гипотеза, согласно которой негативной чертой цифровизации является появление новых ценностных (аксиологических) установок, что приводит к формированию особого (чаще негативного) отношения к праву (формируется недоверие к закону, правовое сознание поражается правовым нигилизмом). Наиболее ярко эту проблему можно проиллюстрировать на примере коллизий позитивного закона и пользовательских соглашений. Для субъектов интернет-отношений важнейшее значение приобретают именно пользовательские соглашения, тогда как позитивное право остается в тени. Как, по Вашему мнению, можно преодолеть указанную проблему?

– Действительно, сегодня очевидным становится вмешательство крупных интернет-компаний в сферы, которые традиционно регулируются императивными нормами национального законодательства. Наиболее яркий пример — разработанный Ассоциацией интернет-компаний модельный документ о доступе к отдельным видам цифровых активов в связи со смертью их владельца — *Privacy Expectation Afterlife and Choices Act (PEAC)*[4]. Фактически этот документ регулирует наследственные отношения в виртуальной среде, поскольку устанавливает режим доступа к учетной записи умершего лица, в том числе в связи с необходимостью управления имуществом наследодателя. Еще один пример — когда в пользовательских соглашениях отдельных интернет-ресурсов в качестве условия определения юридической судьбы цифровых активов на случай смерти предусматривается составление электронного завещания, которое запрещено российским законодательством (п. 1 ст. 1124 ГК РФ). В этой связи возникает

[4] NetChoice (2015, July 20). *Privacy Expectation Afterlife and Choices Act (PEAC).* https://www.fiduciarylawblog.com/wp-content/uploads/2015/07/PEAC.pdf

парадоксальная ситуация: составление такого завещания нарушает закон, но для завещателя является единственным способом преодолеть ограничения пользовательских соглашений в сети Интернет.

Но приводит ли коллизия позитивного права и пользовательских соглашений к формированию негативного отношения к праву, недоверия к нему? Думаю, что нет.

В большинстве случаев люди не осознают подобные коллизии. Проблема заключается в другом. Люди не всегда знают содержание норм национального законодательства, но вынуждены знакомиться с пользовательскими соглашениями, поскольку без соответствующей отметки об ознакомлении невозможно получить доступ к интернет-ресурсам.

Кроме того, поскольку существенная часть жизни человека проходит в цифровой среде, он вынужден подчиняться тем правилам, которые устанавливаются пользовательскими соглашениями (просто потому, что от этого зачастую зависят его заработок, общение и досуг). Несоблюдение этих правил легко контролировать с помощью технических средств, а потом применять к нарушителю санкции, вплоть до отлучения его от доступа к ресурсу. Обеспечить подобный тотальный контроль за соблюдением своего законодательства не способно сегодня ни одно государство.

Очевидно, для любого государства является проблемой приоритет, который субъект отдает пользовательскому соглашению перед законом. Я думаю, что если интернет-компания желает действовать на определенной территории, она должна неукоснительно соблюдать национальное законодательство. И это требование должно быть закреплено в законе. Кроме того, выработка разными странами унифицированных правил в отношении интернет-компаний позволит обеспечить соответствие их пользовательских соглашений действующему законодательству.

– Кажется, Вы были одной из первых, кто указал на трудности, которые испытывает российское наследственное право в связи с появлением цифровых прав[5]. Какие проблемы на сегодня так и не решены в этой сфере? И что бы Вы могли посоветовать для их преодоления?

– Прежде всего отсутствует определенность в составе прав, включаемых в наследственную массу, поскольку согласно ст. 128 и 141.1 ГК РФ цифровыми признаются названные в таком качестве в законе обязательственные и иные имущественные права, однако эти права не конкретизированы. Очевидно, их состав должен быть уточнен.

Кроме того, не решена проблема обеспечения доступа наследников к коду (логину, паролю, криптокошельку и т.п.), если наследодатель не оставил никакой информации. В этой ситуации получить цифровые права по наследству практически невозможно.

За рубежом предпринимаются некоторые попытки решить эту проблему. Например, в США разработан Единообразный закон о доступе фидуциаров к электронным активам *(Uniform Fiduciary Access to Digital Assets Act (FADA)),* который предусматривает право владельцев цифровых активов передавать их хранителям информацию о лицах, которые вправе получать допуск к данным активам. Правда, речь пока идет лишь об аккаунтах в социальных сетях, платежных системах и службах электронной почты. Схожим образом в Нидерландах Ассоциация нотариусов поддержала разработку цифрового хранилища, в котором клиенты смогут хранить свои цифровые данные, включая коды доступа.

[5] Яценко, Т.С. (2019). Наследование цифровых прав. *Наследственное право*, (2), 11–14.

Возможно, Федеральная нотариальная палата могла бы в будущем создать подобное хранилище, в котором можно было бы по желанию наследодателя размещать информацию о цифровых активах и кодах доступа к ним. Пока же система оборота цифровых прав такова, что мы не можем установить принадлежность цифрового права гражданину, если такая информация отсутствует.

Не решена и проблема наследования аккаунтов. Это связано с тем, что их правовая природа пока не определена. И в этой связи возникает закономерный вопрос: если интернет-аккаунт ассоциируется с личностью его владельца, обладает имущественной ценностью как для самого владельца, так и для его наследников, то почему бы не разрешить оборот аккаунтов, в том числе их наследование? В зарубежных странах оно разрешено. Наследники зарабатывают большие суммы на использовании аккаунтов умерших знаменитостей: певцов, актеров, музыкантов. Например, по данным *Forbes,* на использовании аккаунтов Майкла Джексона в социальных сетях в 2020 г. его наследники заработали более 40 млн долл.[6] Очевидно, нет никаких препятствий к тому, чтобы легализовать аккаунты в социальных сетях в качестве объектов гражданских прав и в России, разрешить сделки с ними и их наследование.

– Анонимность в Интернете создает плодородную почву для всевозможных нарушений, в том числе посягающих на честь и достоинство личности. Для России эта проблема наиболее актуальна, так как система мер защиты граждан, пострадавших от диффамации в Сети, недостаточно эффективна. Существует ли, на Ваш взгляд, наиболее оптимальный механизм борьбы с диффамацией анонимных пользователей?

– Действительно, используемые в России подходы к борьбе с диффамацией в Интернете недостаточно эффективны. Если личность анонимного нарушителя, который распространил в сети порочащую честь, достоинство или деловую репутацию гражданина информацию, установить невозможно, то наказывать никого не будут. Как пояснил Конституционный Суд РФ в Постановлении от 9 июля 2013 г. № 18-П «По делу о проверке конституционности положений пунктов 1, 5 и 6 статьи 152 Гражданского кодекса Российской Федерации в связи с жалобой гражданина Е.В. Крылова», интернет-провайдеры, владельцы доменных имен и другие субъекты в случае, если порочащие сведения были распространены на принадлежащем им ресурсе, ответственности не несут, кроме случаев, когда такой ресурс зарегистрирован в качестве средства массовой информации. Конституционный Суд РФ объяснил исключение ответственности указанных лиц за диффамационный контент, размещенный анонимными пользователями, общим принципом юридической ответственности за вину. Думается, что подобное положение весьма неоднозначно, поскольку зачастую владельцы сайтов размещают рекламу на принадлежащих им ресурсах, что может свидетельствовать об осуществлении предпринимательской деятельности, следовательно, об ответственности без вины.

Как мне кажется, в некоторых странах существует оптимальный механизм борьбы с диффамацией анонимных пользователей. К примеру, в Великобритании, если анонимный пользователь, который распространил порочащие сведения в сети Интернет, не обнаружен, к ответственности будет привлечен информационный посредник. Считается, что такой подход обеспечивает реальную защиту интересов потерпевшего, поскольку, кроме всего прочего, это побуждает владельцев сайтов помогать суду в идентификации анонимных пользователей.

---

[6] Богатырев, Т. (2020, ноябрь 13). *Forbes назвал умерших знаменитостей с самыми высокими доходами.* Forbes. https://www.forbes.ru/newsroom/biznes/413747-forbes-nazval-umershih-znamenitostey-s-samymi-vysokimi-dohodami

Кроме того, государствам важно договориться и унифицировать ответственность за диффамационное поведение анонимных пользователей в сети Интернет, что позволит создать действенный механизм предупреждения нарушения, независимо от места его совершения или страны проживания потерпевшего и правонарушителя.

– В заключение хотелось бы задать вопрос, обращенный в будущее: каков Ваш прогноз по поводу места и значения права в XXII в.?

Как мне кажется, мир развивается, а психология человека остается неизменной и требует от этого мира упорядоченности и стабильности. Обеспечить данную потребность может только право, функциональное назначение которого по этой причине останется неизменным и в XXII в. Чтобы ни менялось, какие бы новые технологии ни появлялись, мы остаемся людьми, для которых важен порядок!

Сведения об авторе:

Яценко Т.С. — доктор юридических наук, доцент, руководитель департамента частного права факультета права Национального исследовательского университета «Высшая школа экономики», Москва, Россия.
tyatsenko@hse.ru
ORCID: https://orcid.org/0000-0002-0876-2224

Information about the author:

Tatiana S. Yatsenko — Doctor of Law, Associate Professor, Head of the Department of Private Law, Faculty of Law, HSE University, Moscow, Russia.
tyatsenko@hse.ru
ORCID: https://orcid.org/0000-0002-0876-2224

https://doi.org/10.38044/2686-9136-2023-4-2-15-39

ARTICLES

PRIVACY IN THE AGE OF REMOTE SENSING DURING NATURAL DISASTERS IN AUSTRALIA AND INDONESIA

Temitope Lawal*, Melanie Jackson, Eugenia Georgiades

Bond University
14, University Drive, Robina, Queensland, Australia, 4226

Abstract

Satellites are increasingly used for remote sensing, aiding in disaster management, however they also raise privacy concerns. Despite the existence of international instruments such as the *Outer Space Treaty, Principles Relating to Remote Sensing of the Earth from Outer Space* and *International Charter Space and Major Disasters*, there are no specific rules addressing satellite misuse leading to privacy breaches during natural disasters. This article examines the existing legal frameworks for satellite regulation and privacy in Australia and Indonesia, two disaster-prone countries, with the aim of determining their adequacy for addressing privacy concerns arising from satellite use during natural disasters. By conducting a comparative analysis of both legal frameworks vis-à-vis relevant international law, this article highlights the gaps that affect their applicability and effectiveness. It finds that international rules on the use of satellites for remote sensing activities generally lack binding force, and do not address the issue of privacy breaches resulting from satellite misuse. Both countries also lack specific legal frameworks addressing privacy breaches caused by satellite misuse during disasters. It recommends that in the absence of unequivocal and specific provisions under international law, both countries could review and rely on their national legal frameworks to address potential privacy issues due to advancing remote sensing capabilities. The provision of Article VI of the *Outer Space Treaty* requires states to authorise and ensure continued supervision of activities of non-governmental entities in outer space. This provision could be relied on to impose, through the instrumentality of domestic laws, restrictions, or conditions on space activities, including privacy provisions. Existing space legislation requiring liability insurance could also be extended to include privacy provisions.

Keywords

data privacy, legal frameworks, natural disasters, remote sensing, satellite misuse

Conflict of interest	The authors declare no conflict of interest.
Financial disclosure	The study was funded by the APNIC Foundation, Grant ID: F-202206-01436 — Bond University Internet Law Research Clinic: Enhancing the Efficacy of Internet Connectivity Legal Frameworks in the Asia-Pacific Region.
For citation	Lawal, T., Jackson, M, & Georgiades, E. (2023). Privacy in the age of remote sensing during natural disasters in Australia and Indonesia. *Digital Law Journal*, 4(2), 15–39. https://doi.org/10.38044/2686-9136-2023-4-2-15-39

* Corresponding author

Submitted: 9 June 2023, accepted: 27 June 2023, published: 31 July 2023

СТАТЬИ

КОНФИДЕНЦИАЛЬНОСТЬ В ЭПОХУ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ СТИХИЙНЫХ БЕДСТВИЙ В АВСТРАЛИИ И ИНДОНЕЗИИ

Т. Лаваль*, М. Джексон, Е. Георгиадес

Университет Бонд
4226, Австралия, Квинсленд, Робина, Юниверсити Драйв, 14

Аннотация

Спутники все чаще используются для дистанционного зондирования Земли во время стихийных бедствий, что вызывает тревогу в отношении нарушения конфиденциальности данных частных лиц. Несмотря на существование международных документов, таких как *Договор о космосе*, *Принципы, касающиеся дистанционного зондирования Земли из космического пространства,* и *Международная хартия по космосу и крупным катастрофам*, не существует конкретных правил, касающихся неправомерного использования спутников, ведущего к нарушению конфиденциальности. В настоящей статье рассматривается существующее правовое регулирование использования спутников и конфиденциальности данных в Австралии и Индонезии, странах, часто подвергаемых стихийным бедствиям, с целью определения готовности правопорядка разрешать вопросы конфиденциальности данных. Посредством проведения сравнительного анализа обоих правопорядков и международного права в статье подчеркиваются существующие правовые пробелы, которые влияют на применимость и эффективность действия норм. Авторы полагают, что нормы международного права по использованию спутников для дистанционного зондирования, как правило, не имеют обязательной силы и не касаются проблемы нарушения конфиденциальности. В обеих странах также отсутствуют конкретные правовые нормы для устранения нарушений конфиденциальности, вызванных неправильным использованием спутников во время стихийных бедствий. В условиях отсутствия недвусмысленных и конкретных норм международного права авторы считают, что страны могли бы полагаться на национальное право, возможно, частично пересмотрев некоторые его нормы, для решения потенциальных проблем конфиденциальности в связи с развитием возможностей дистанционного зондирования. Установление национальных условий и ограничений на осуществление космической деятельности, включая положения о конфиденциальности, можно было бы обосновать применением статьи VI Договора о космосе, требующей от государств санкционировать и обеспечивать непрерывный надзор за деятельностью неправительственных организаций в космическом пространстве. Существующее космическое законодательство о страховании ответственности также можно было бы расширить, включив в него положения о неприкосновенности частной жизни.

Ключевые слова

конфиденциальность данных, правовой режим, стихийные бедствия, дистанционное зондирование, неправомерное использование спутников

Конфликт интересов Авторы сообщают об отсутствии конфликта интересов.

Финансирование	Исследование финансировалось APNIC Foundation, номер гранта: F-202206-01436 — Bond University Internet Law Research Clinic: Enhancing the Efficacy of Internet Connectivity Legal Frameworks in the Asia-Pacific Region.
Для цитирования	Лаваль, Т., Джексон, М., Георгиадес, Е. (2023). Конфиденциальность в эпоху дистанционного зондирования стихийных бедствий в Австралии и Индонезии. *Цифровое право, 4*(2), 15–39. https://doi.org/10.38044/2686-9136-2023-4-2-15-39

* Автор, ответственный за переписку

Поступила: 09.06.2023, принята в печать: 27.06.2023, опубликована: 31.07.2023

Introduction

In November 2022, an earthquake hit Cianjur, West Java, Indonesia, resulting in the death of at least 600 people and causing extensive damage.[1] In a similar vein, several parts of South Australia were affected by a devastating flooding of the River Murray between December 2022 and January 2023, leading to human displacements and significant damage to properties and infrastructure.[2]

Indonesia is located within the ring of fire, a path along the Pacific Ocean that experiences frequent seismic activities leading to earthquakes, volcanic eruptions, and tsunamis (Hakim & Lee, 2020). Consequently, the country is prone to natural disasters, with over 2000 occurrences reported yearly since 2016.[3] Australia on the other hand, has a diverse climate marked by temperature and rainfall variations throughout the year. Significant parts of the country transition between dry and hot conditions characterised by droughts and heatwaves to moist and cooler conditions that often result in flooding.[4] This climate variability is linked to several natural disasters such as bushfires, floods, and heatwaves (Boon, 2013).

During natural disasters, satellites[5] play a vital role in providing essential data and services.[6] They are used in search and rescue efforts to locate individuals who may be stranded or missing,

1 Statista Research Department. (2023, January 17). Number of fatalities due to natural disasters in Indonesia 2016–2022. Statista. https://www.statista.com/statistics/954214/indonesia-fatalities-natural-disasters/#:~:text=In%202022%2C%20there%20were%20around,%2C%20on%20November%2021%2C%202022

2 Some have suggested that this might be the most significant natural disaster in the history of South Australia. See Richards, S. (2023, January 16). *River Murray flood "most significant" natural disaster in SA history. InDaily.* https://indaily.com.au/news/2023/01/16/river-murray-flood-most-significant-natural-disaster-in-sa-history/

3 Statista Research Department. (2023, January 24). *Natural disasters in Indonesia—statistics & facts.* Statista. https://www.statista.com/topics/8305/natural-disasters-in-indonesia/#topicOverview

4 Royal Commission into National Natural Disaster Arrangements. (2020). Royal Commission into National Natural Disaster Arrangements — report. https://naturaldisaster.royalcommission.gov.au/system/files/2020-11/Royal%20Commission%20into%20National%20Natural%20Disaster%20Arrangements%20-%20Report%20%20%5Baccessible%5D.pdf

5 The earthquakes that occurred in certain areas of Turkey and Syria on 6 February 2023 serve as a clear indication of the crucial role of satellites during natural disasters. The activation of the International Charter on Space and Major Disasters facilitated the provision of satellite data (such as images and maps of the impacted areas) to assist in the rescue and recovery operations. *See* Office for Outer Space Affairs UN-SPIDER. (2023, February 7). *Earthquake in Turkey and Syria—International Charter and Copernicus active.* United Nations. https://www.un-spider.org/news-and-events/news/earthquake-turkey-and-syria-international-charter-and-copernicus-active

6 Bronner, E. (2023, February 7). Earthquake in Turkey and Syria: How satellites can help rescue efforts. *The Conversation*. https://theconversation.com/earthquake-in-turkey-and-syria-how-satellites-can-help-rescue-efforts-199357

thereby minimising the disaster's impact.[7] Recently, satellite IoT (Internet of Things), in the form of hundreds or thousands of sensors placed on satellites launched into orbit, is being used as early warning systems to monitor natural disasters such as hurricanes, tornadoes, and earthquakes, and providing critical information to communities at risk.[8] Governments often process the data collected through remote sensing to take necessary actions to detect and mitigate the effects of these natural disasters.[9]

According to Moran (2017)[10], remote sensing involves 'identifying, observing, and measuring an object without coming into direct contact with it.' In other words, it is a means of observing the Earth's surface from space (Nafis et al., 2021). Earth observation satellites launched into orbit carry remote sensors capable of detecting, observing, and collecting information about the Earth's surface and other planetary bodies using various means including satellite imaging (Tronchetti, 2015). This is particularly important as terrestrial communication limitations during natural disasters make the use of satellite technology for emergency communications critical (Page & Besco, 2021). Both private entities and governments are increasingly building or planning to build constellations of Earth observation satellites to conduct remote sensing activities.[11] In 2008, there were only 150 Earth observation satellites in orbit (Tatem et al., 2008). As of 2022, there are over 1,000 Earth observation satellites occupying different orbits.[12] The cost of launching imaging satellites as well as procuring high-resolution satellite images capable of remote sensing is constantly decreasing.[13]

Historically, Earth observation satellites were placed in the geosynchronous equatorial orbit (GEO), which is about 36,000 km above Earth's surface.[14] Due to the distance from Earth, images captured from GEO were of low quality (Emery & Camps, 2017). However, with the continuous advancements in technology, Earth observation satellites are now being placed in the low Earth orbit (LEO), which is much closer to Earth's surface (Emery & Camps, 2017). This allows for higher spatial resolution images to be captured, as the closer a satellite is to Earth's surface, the better the resolution of the images that can be captured (Emery & Camps, 2017). This has led to diverge opinions as to how different countries view remote sensing activities. Countries that actively engage in remote sensing believe that collection and dissemination of satellite data have significant international benefits (Mosteshar, 2016). Others, especially developing countries, hold the view that the use of satellites

7 Fair Tech Institute. (2020). *The Role of Satellite Communications in Disaster Management.* https://accesspartnership.com/wp-content/uploads/2022/03/The-Role-of-Satellite-Communications-in-Disaster-Management.pdf

8 Inmarsat. (2021, April 22). *Satellite-based monitoring to reduce impact of natural disasters.* [Press Release]. https://www.inmarsat.com/en/news/latest-news/government/2021/satellite-monitoring-impact-natural-disasters.html

9 Fair Tech Institute. (2020). *The Role of Satellite Communications in Disaster Management.* https://accesspartnership.com/wp-content/uploads/2022/03/The-Role-of-Satellite-Communications-in-Disaster-Management.pdf

10 Moran A. (2017, August 16). Remotely Sensing Our Planet. NASA. https://svs.gsfc.nasa.gov/30892

11 These satellites are equipped with advanced high precision sensors capable of capturing and processing high-definition images of the Earth's surface. *See* Beam, C. (2019, June 26). Soon, satellites will be able to watch you everywhere all the time: Can privacy survive? *MIT Technology Review.* https://www.technologyreview.com/2019/06/26/102931/satellites-threaten-privacy/

12 Thorpe, E. (2022, March 5). *Earth Observation Satellites Imagery: Types, Application, And Future Trends*. Orbital Today. https://orbitaltoday.com/2022/03/05/earth-observation-satellites-imagery-types-application-and-future-trends/

13 Chow, D. (2022, April 9). To cheaply go: How falling launch costs fueled a thriving economy in orbit. *NBC News*. https://www.nbcnews.com/science/space/space-launch-costs-growing-business-industry-rcna23488

14 Jagula, D. (2022, February 19). *Satellite imagery for everyone.* IEEE Spectrum. https://spectrum.ieee.org/commercial-satellite-imagery

by sensing countries which extends to obtaining data about the territory and natural resources of another State violates their sovereignty, and such activities should require the prior consent of the Sensed state (Mosteshar, 2016).

Thus, despite the immense benefits of remote sensing activities carried out using satellites, they are also prone to misuse, particularly during natural disasters. With the constant advancements in remote sensing capabilities (Ito, 2011; Sitanggang, 2018), the potential for the misuse of satellites resulting in privacy breaches have increased. Misuse can occur when monitoring places, objects, or people without prior notification or authorisation. Any information collected through satellite imaging can be misused through the improper dissemination of data or reaching false conclusions based on wrong data interpretation.[15]

Consequently, satellites' misuse can result in privacy breaches when collecting data through remote sensing activities. Singh et al. (2012) highlight concerns about the commercialisation of remote sensing using satellite imagery and the potential for abuse. Santos and Rapp (2019) argue that as low-cost commercial satellite systems become operational, high-resolution imagery will become a regular part of end-user products and information services. Accordingly, advancements in the resolution capacity of remote satellite technology will inevitably raise debates on the infringement of citizens' privacy, as monitoring can now be done from continents away without the need for installed cameras.[16] Singh et al. (2012) further suggest that 'the rapidly improving resolution capacity coupled with the growth in nanotechnology could enable live recording instead of imagery in the near future and we are left to imagination to perceive the threat posed by unfettered usage of remote sensing satellites.'

Although there are international frameworks such as the *Remote Sensing Principles*[17] and *Disasters Charter*,[18] as discussed later, they are generally not legally binding and do not provide specific rules for addressing privacy breaches that occur during satellite-based remote sensing activities, particularly in natural disasters situations (de Beer, 2020; Sitanggang, 2018).

Consequently, this article, which consists of two parts, focuses on the intersection of privacy protection and satellite use during natural disasters. The first part clarifies the specificity of collecting and processing personal data during natural disasters by distinguishing it from general electronic surveillance. It discusses the unique challenges posed by disaster situations such as the urgency and necessity of data collection, the potential for large scale data breaches, and the increased vulnerability of affected individuals. An analysis of how the circumstances of natural disasters can impact privacy rights, including issues of consent, data security, data retention, and the potential for re-identification of anonymised data is also undertaken.

The second part provides a comparative analysis of the relevant provisions of Australian and Indonesian law pertaining to use of satellite, particularly for remote sensing, and privacy

---

15 Beam, C. (2019, June 26). Soon, satellites will be able to watch you everywhere all the time: Can privacy survive? *MIT Technology Review*. https://www.technologyreview.com/2019/06/26/102931/satellites-threaten-privacy/

16 Between 2007 and 2017, India launched CARTOSAT-2, a series of remote sensing satellites with spatial resolution of less than a meter. To illustrate the extent of these sort of resolution capabilities, the satellite imagery collected by these satellites are capable of being used to detect the model and make of a car on Earth. *See* (Singh, 2012).

17 *The Principles Relating to Remote Sensing of the Earth from Outer Space*, UN GA Res 41/65 — adopted on 3 December 1986. See generally the different principles, especially Principle I that defines raw data, processed data and analysed data, Principle XI that envisages that 'Remote sensing shall promote the protection of mankind from natural disasters.'

18 *Charter on Cooperation to Achieve the Coordinated Use of Space Facilities in the Event of Natural or Technological Disasters*, opened for signature 20 October 2000.

considerations during natural disasters.[19] It also analyses relevant international instruments related to remote sensing, natural disasters, and privacy, evaluating their applicability and effectiveness in addressing privacy issues arising from the use of satellites for remote sensing during natural disasters. Through this, gaps are identified in the existing legal frameworks and suggestions proffered for potential improvements that can be explored to address the specific privacy issues arising from advancing remote sensing capabilities.

Part I — Handling of personal data during natural disasters

Contrasting personal data collection during natural disaster and surveillance

To better understand the focus of this article on privacy implications arising from collection and processing of personal data using remote sensing capabilities during natural disasters, an appropriate starting point would be to distinguish this process from general electronic surveillance.

The first differentiating factor pertains to the purpose of data collection. During natural disasters, data is typically collected for emergency management, disaster relief, and recovery activities (Yu et al., 2018). In contrast, electronic surveillance is often carried out for national security, economic stability, or other social benefits.[20] Consequently, the legal implications and law governing both activities differ considerably. Where they exist, legal frameworks relating to data collection and processing during natural disasters are generally designed to ensure the safety and well-being of individuals.[21] These frameworks, such as the provision of Part VIA of the Privacy Act (Cth) discussed later, may specify the types of data that can be collected, the purposes for which it can be used, and the specific safeguards required to protect privacy and data security. They may also include provisions for securing and preventing unauthorised access and misuse of the collected data. On the other hand, electronic surveillance is often governed by wiretapping statutes that regulate the interception of electronic communications for law enforcement or national security purposes (National Research Council, 1996). These laws, such as the Telecommunications (Interception and Access) Act 1979 (Cth), are typically employed for intercepting and retaining communications data, especially during intelligence operations.

Another important distinction between data collection during natural disasters and surveillance is the impact on privacy. During natural disasters, data collection and processing may involve accessing social media posts, health records, and other personal information (Kuner & Marelli, 2020). As earlier alluded to, this is primarily done to provide emergency services and support, rather than for surveillance purposes. However, general electronic surveillance can significantly impact a broad spectrum of rights, including privacy. Some argue that surveillance is inherently harmful, as Quentin Skinner explains: "I think it is very important that the mere fact of there being surveillance takes away liberty… it is true that my privacy has been violated if someone is reading my emails without my knowledge… my liberty is also being violated, not merely by

[19] While the emphasis for potential misuse of satellites in this article pertain to privacy breaches in the context of natural disasters, it should be noted that the misuse of satellites also applies in other contexts.

[20] Lee, N.T., & Chin, C. (2022). *Police surveillance and facial recognition: Why data privacy is imperative for communities of color.* Brooklings. https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

[21] United Nations Office for Disaster Risk Reduction. (2015). Sendai Framework for Disaster Risk Reduction 2015-2030. United Nations. https://www.undrr.org/quick/11409

the fact that someone is reading my emails but also by the fact that someone has the power to do so should they choose".[22]

Challenges of data collection in relation to privacy during natural disasters

Despite the primarily beneficial nature of data collection during natural disasters, there are unique challenges and considerations related to privacy.

One such challenge is the urgency and necessity of data collection. During natural disasters, there is often an urgent need to gather data to support emergency management, particularly in order to deliver health services, relief materials, and carry out recovery activities (Kuner & Marelli, 2020). For example, the activation of the Disaster Charter is available year-round, and activations typically occur within 10 days of a disaster.[23] Member agencies prioritise providing satellite data to requesting countries as quickly as possible to aid in disaster management and recovery. Therefore, obtaining informed consent from disaster victims becomes impractical in many cases. This impacts one of the salient principles of data protection — consent as a lawful basis for processing personal data. In distressing situations, it is questionable to consider any 'consent' given by someone in need of humanitarian assistance as truly 'freely' given (Kuner & Marelli, 2020). Moreover, during natural disasters, individuals are more likely to share personal information in exchange for emergency support (Sheinidashtegol et al., 2019), which increases their vulnerability and the risk of privacy breaches. Individuals affected by natural disasters may be unaware of how their personal data is collected, processed, or used, potentially breaching the provisions of some data privacy legislation (*Privacy Act* 1988 (Cth), APPs 3, 6, 11).

Another challenge relates to data retention. A common requirement during data collection and processing is the obligation to delete or anonymise data once the purpose for which it was collected has been served. However, during a natural disaster event, there might be a need for data to be retained longer than would be necessary in a non-emergency situation (Sanfilippo et al., 2020). The risk of privacy breaches, therefore, heightens especially if the data is not securely stored and is subsequently accessed by unauthorised persons. While data minimisation, which involves collecting only the minimum amount of personal data necessary for a specific purpose, is considered a useful strategy (Qu et al., 2019), it does not completely eliminate the risk associated with privacy breaches.

Furthermore, there remains an associated risk of data breaches, including cyber-attacks on data collected during natural disasters. Anonymisation is often proposed as a preventive measure to protect individuals' privacy by removing personally identifiable information from datasets (Nishara & Pandey, 2015). In the context of natural disasters, the expectation is that once data is anonymised, the personal information of individuals is safeguarded while allowing for data collection and analysis. However, the risk of re-identifying anonymised data is not completely eliminated, especially when such data is combined with other datasets.[24]

---

[22] Marshall, R., & Skinner, Q. (2013, July 26). Liberty, liberalism and surveillance: A historic overview. *OpenDemocracy*. https://www.opendemocracy.net/en/opendemocracyuk/liberty-liberalism-and-surveillance-historic-overview/

[23] Office of Outer Space Affairs. (n.d.). *International Charter Space and Major Disasters.* United Nations. Retrieved June 7, 2023. https://www.un-spider.org/international-charter-space-and-major-disasters

[24] Tyrrell, J. (2023, February 2). *Re-identification risks: Can data ever be fully anonymized?* T_HQ: Technology and business. https://techhq.com/2023/02/re-identification-risks-can-data-ever-be-fully-anonymized/

Part II — National and International legal regime on remote sensing, natural disasters and privacy

Resulting from the analysis in the previous part, it becomes important to probe the question of whether there exist adequate provisions, generally under international law, and specifically under Australian and Indonesian law to address the potential for privacy breaches that may arise when carrying out remote sensing activities during natural disasters.

Landscape of national Legal framework for the regulation of LEO satellites

The advancement in satellite technology is facilitating the deployment of constellations of satellites in the low earth orbit (LEO). These satellites are used for various purposes, including for remote sensing. It therefore becomes important to commence the discussion in this section with an overview of the current legal framework in Australia and Indonesia which relates to the regulation of LEO satellites.

Australia

In Australia, space activities are primarily regulated pursuant to the *Space Act,*[25] and the *Telecommunications Act*.[26] It is a State Party to all the major international treaties governing space, including the *Outer Space* Treaty.[27] The Australian Space Agency (ASA) regulates Australian space activities, while the Australian Communications and Media Authority (ACMA) regulates communications and media services. ACMA also serves as the Australian administration for the International Telecommunications Union's international process of managing frequencies for satellite communications.[28]

Under Section 42 of the *Telecommunications Act*, a carrier license is required for any person who uses a network unit to supply a carriage service to the public. A network unit includes a designated radiocommunications facility that uses different means, including satellites, to supply carriage services between different points in Australia. If such operator requires the use of radio frequency spectrum, a radiocommunications licence must be granted,[29] as well as other necessary authorisations to set up and operate a satellite network.[30]

Section 18 of the *Space Act* contains regulatory and licensing provisions relating to launch facilities, launching, and returning of space objects (which encompasses satellites),[31] as well as liability for damage by space objects. By virtue of Sections 11, 12, 15, 18 and 28 of the *Space Act*, a licence is

25 Space (Launches and Returns) Act, 2018 (Cth).

26 Telecommunications Act, 1997 (Cth).

27 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (GA Res 2222 (XXI), annex) — adopted on 19 December 1966, opened for signature on 27 January 1967, entered into force on 10 October 1967.

28 Australian Communications and Media Authority. (2012). *Australian procedures for the coordination and notification of satellite systems.* Australian Government. https://www.acma.gov.au/sites/default/files/2019-11/aust_procedures-coordination_notification_of_satellite_systems%20pdf.pdf

29 *See generally* Chapter 3 of the Radiocommunications Act, 1992 (Cth).

30 Australian Communications and Media Authority. (n.d.). *Set up and operate a new satellite network*. Retrieved June 7, 2023. https://www.acma.gov.au/set-and-operate-new-satellite-network

31 Although satellites are not explicitly mentioned under the *Space Act,* Section 8 defines 'space objects' to mean 'any object the whole or a part of which is to go into or come back from an area beyond the distance of 100 km above mean sea level.' This definition captures satellites within its scope.

generally required to operate a launch facility in Australia, and a launch permit is required to launch and return a space object from and to a facility or area in Australia. Australian nationals require an overseas payload permit and return authorisation to launch and return space objects respectively from and to a place outside Australia pursuant to Sections 14, 15A, 46B, and 46L of the *Space Act*. Since satellites fall under the definition of space objects, the regulatory and licensing provisions under the *Space Act* also apply.

As part of the licensing process, Section 22, 56, and 102 of the *Space (Launches and Returns) (General) Rules* requires an applicant to submit a technology security plan that includes procedures for preventing unauthorised access to the technology and ensuring cybersecurity. However, while the plan requires that the cybersecurity of the technology used in relation to the launch and return of a space object be safeguarded, it does not stipulate any standards for safeguarding these space objects against cyberattacks during launch and return. This is particularly concerning since remote sensing satellites launched into orbit can capture high-resolution images of Earth's surface, including information that can be used to identify individuals (Singh et al., 2012). As would be discussed in the later part of this article, the *Privacy Act*[32] requires personal information to be safeguarded against potential unauthorised use, loss, disclosure, alteration, or access.

Although the above provisions of the *Space (Launches and Returns) (General) Rules* relate to safeguards during launch and return of satellites, it is nonetheless useful to highlight the connection with the *Privacy Act* as explained above. To put in context, there have been instances when sensitive satellite infrastructure of the Australian government or private entities have been subject to sophisticated cyber-attacks (Verco, 2021). For instance, between 2015 and 2016, the systems of the Australian Bureau of Meteorology were subjected to cyber-attacks.[33] Besser & Sturmer (2016) suggest that the true targets for this attack may have been the defence assets linked to the Bureau of Meteorology and its 'vast data collection capabilities.'[34] It is evident that satellites are becoming increasingly susceptible to cyberattacks that can lead to privacy breaches, and with the increasing participation of governments, private entities, and individuals in space activities, it becomes important that these satellites are adequately protected from cyber-attacks (Housen-Couriel, 2016).

Indonesia

Indonesia, as a State Party to the *Outer Space Treaty*, has an obligation to regulate space activities within its territory (von der Dunk, 2002). To meet this obligation, Indonesia has specific frameworks for regulating space activities and the use of satellites for communications services. The primary laws in this regard are the *Law on Telecommunication*[35] and the *Space Law*.[36]

Telecommunications is defined under Article 8 of the *Law on Telecommunication* as 'any emission, transmission, and/or reception of information in the forms of signs, signals, writings, images, voice and sound through wire, optic, radio, or other electromagnetic systems.' This definition is broad

[32] Privacy Act 1988 (Cth).

[33] Uhlmann, C. (2015, December 2). *China blamed for "massive" cyber attack on Bureau of Meteorology computer.* ABC News. https://www.abc.net.au/news/2015-12-02/china-blamed-for-cyber-attack-on-bureau-of-meteorology/6993278

[34] Besser, L., & Sturmer, J. (2016, August 29). *Government computer networks breached in cyber attacks as experts warn of espionage threat.* ABC News. https://www.abc.net.au/news/2016-08-29/chinese-hackers-behind-defence-australe-security-breaches/7790166; 1. BBC News. (2016, October 12). *Australia weather bureau hacked by foreign spies, says report*. https://www.bbc.com/news/world-australia-37615645

[35] Law No. 36 of 1999 on Telecommunication.

[36] Law No 21 of 2013 Concerning Space Activities.

enough to cover different mediums of transmission, including satellites and the different uses they can be put to.

Due to its unique geography (Nafis et al., 2021), Indonesia's telecommunications system relies heavily on communications satellites (Sastrawidjaja & Suryanegara, 2018), which transmit and receive information through radio frequencies (Sitanggang, 2018). Communications satellites are essential to many services including remote sensing activities, mobile communication services, broadcasting, disaster management, and weather forecasting (Supancana, 2006). Whilst Indonesia uses foreign satellites, it also has its own system of communications satellites (Nafis et al., 2021) currently made up of nine (9) satellites.[37] Pursuant to Article 33 of the *Law on Telecommunication*, the use of radio frequency spectrum and satellite orbit is a licensable telecommunication undertaking.

Furthermore, Article 6 of the *Law on Telecommunication* empowers the Minister of Communications and Informatics to regulate telecommunications in Indonesia, including the use of satellites for communications services. While the National Institute of Aeronautics and Space (LAPAN) has been carrying out supervisory functions over all space activities in Indonesia pursuant to Article 38(4) of the *Space Law*. Despite not being specifically mentioned under the *Space Law*, LAPAN has been undertaking that responsibility as the existing national space agency since its establishment in 1963.[38] However, with the creation of the National Research and Innovation Agency (BRIN), LAPAN's role as the country's space agency is being transferred to BRIN (Nugraha et al., 2022). A thorough reading of Article 1 and 5 reflects that the *Space Law* applies to all space activities occurring within the territory or jurisdiction of Indonesia, all space activities occurring on behalf of or otherwise attributable to Indonesia, or space activities conducted by Indonesian citizens or Indonesian legal entities with a license to undertake space activities.

To regulate space activities, Article 41 and 42 of the *Space Law* requires entities to obtain a license before engaging in space activities. Additionally, Article 71 of the *Space Law* mandates that all space objects, including satellites, must be registered with the Indonesian government, providing sufficient information on their orbital parameters, function, purpose, and launching entity. It clarifies that registration is necessary to ensure open information and must be published and easily accessible. Operators of space activities are prohibited from placing, orbiting, or operating nuclear weapons or other weapons of mass destruction (Supancana, 2015). Furthermore, operators must ensure the protection and preservation of the environment, including any activities that may contaminate Earth's environment (Froehlich & Seffinga, 2018). Indonesia recognises the involvement of private entities in the space segment, and the *Space Law* aims to ensure that all space activities, including commercialisation, are carried out in an orderly manner and for the benefit of humankind (Froehlich & Seffinga, 2018).

International Legal framework related to use of LEO satellites for remote sensing during natural disasters

The use of outer space for various activities, including remote sensing using satellites, increased significantly after the end of the Cold War (Zunnuraeni et al., 2020). To guide the carrying out of these

[37] Mulyadi. (2016, September 6). *Indonesian Satellite Service Regulatory Framework*. ITU International Satellite Symposium 2016, Bali. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/Sep-ISS2016/Presentation/ITU%20International%20Satellite%20Symposium%202016%20-%20Indonesia.pdf

[38] Mardianis. (2014, March 24). *The Indonesian Space Act NO. 21/2013*. Fifty-third session of UNCOPUOS Legal Subcommittee, Vienna. https://www.unoosa.org/pdf/pres/lsc2014/tech-02E.pdf

activities, the *Remote Sensing Principles*[39] were passed in 1986 as a resolution of the United Nations General Assembly (Gummadi & Gupta, 2022). The Principles were adopted as a compromise between the conflicting views of sensed States and sensing States (Mosteshar, 2016). While sensing States believe that the data collected during remote sensing are of immense international benefits, most sensed States believe that such activities impede on their territorial sovereignty (Mosteshar, 2016).

In relation to natural disasters, Principle XI of the *Remote Sensing Principles* provides that 'remote sensing shall promote the protection of mankind from natural disasters.' According to Dodge (2014), this Principle is the 'clearest statement in international law that space-based Earth observation is to be used to protect human life from the effects of natural disasters.' However, its provisions only serve as principles and are not legally binding on States, even if those States voted in favour of them and agreed to them (von der Dunk, 2002). Furthermore, it failed to clearly address issues such as liability and privacy considerations when conducting remote sensing. It also falls short in ensuring satellite data obtained during remote sensing comply with privacy laws under national and international laws (Gummadi & Gupta, 2022), which is relevant in the context of remote sensing during natural disasters.

The *Disaster Charter* is another framework established to provide guidelines for use of remote sensing technology during natural disasters. The *Disaster Charter* was created in 1999 by the Centre National D'Etudes Spatiales[40] and the European Space Agency during the Unispace III conference held in Austria, but officially came into operation on 20 October 2000 after the Canadian Space Agency joined.[41] Currently, it consists of 17-member space agencies who jointly provide free satellite imagery over the disaster areas as soon as the charter is activated.[42] It serves as a framework through which its members collaborate to respond to major natural disasters around the world using satellites. These member space agencies provide fast access to satellite data to aid disaster management as soon as it is triggered by any of the authorised users.[43]

One main distinction between the *Remote Sensing Principles* and the *Disaster Charter* is that while parties to the former are States, members of the latter are space agencies and space systems operators which include private entities (Mosteshar, 2016). Accordingly, it fosters collaboration among space agencies, to share their space facilities in managing major natural or man-made disasters (Mosteshar, 2016). This cooperation ensures that necessary assistance, through the provision of

[39] The Remote Sensing Principles comprise 15 non-binding but politically relevant principles that guide how UN member states conduct remote sensing activities. It defines what remote sensing is and attempts to establish a legal framework prescribing how collection and dissemination of remote sensing data should be carried out while also restating general principles of international law contained under the Outer Space Treaty. *See* (Gummadi & Gupta, 2022).

[40] The French national space agency.

[41] Bally, P., Boubila, F., Viel, M., Jutz, S., Cheli, S., & Briggs, S. (2010). *In Action Around the World: The International Charter 'Space and Major Disasters' (Bulletin No. 143).* European Space Agency. https://earth.esa.int/eogateway/documents/20142/37627/In-action-around-the-world-the-International-Charter-Space-and-Major-Disasters.pdf

[42] Bronner, E. (2023, February 7). Earthquake in Turkey and Syria: How satellites can help rescue efforts. *The Conversation*. https://theconversation.com/earthquake-in-turkey-and-syria-how-satellites-can-help-rescue-efforts-199357

[43] Registration to become an authorised user is open to the disaster management authorities of all countries in the world, provided they meet the prescribed criteria stipulated under the Charter. As of February 2022, national users from 67 countries have been designated authorised users. In addition, 15 international organisations, including the United Nations Office of Outer Space Affairs (UNOOSA), can trigger the Charter system, thereby ensuring all countries of the world can benefit from the Charter, regardless of their registration status. See The International Charter Space and Major Disasters Executive Secretariat. (n.d.). *How to become an authorised user.* Retrieved June 7, 2023. https://disasterscharter.org/web/guest/how-to-register-as-a-user

satellite data collected, is extended to countries or communities that are exposed to an imminent risk, or that have already been affected by such disasters (Mosteshar, 2016).

Since 2000, the *Disaster Charter* has been activated 798 times in 131 countries (Mosteshar, 2016)[44]. However, it is a voluntary agreement among its members and is not legally binding (Zollner, 2018). Like the *Remote Sensing Principles*, it does not create any obligations but serves as a mechanism to provide information and other assistance (Mosteshar, 2016). While the *Disaster Charter* aims to facilitate the exchange of satellite data between space agencies and disaster management organisations to support response and recovery efforts (Zollner, 2018), it does not address issues regarding the use of satellites that may result in privacy breaches. Arising from the shortcomings of these international frameworks, the next section will examine the international law regime concerning privacy, after which an evaluation of the national legislation in Australia and Indonesia that deal with data privacy will be carried out.

Legal framework on data privacy

As noted previously, satellites play a vital role in supporting rescue and recovery efforts during natural disasters. Nevertheless, it is also important to ensure privacy rights are protected while using satellites to collect data, especially when the data collected can potentially be used to identify individuals. Satellite technologies gather different types of data, and as technology advances, it is not far-fetched that information capable of being used to identify individuals can be obtained during remote sensing activities. User identity has been identified as one of the important areas of concerns while discussing different countries approaches to remote sensing regulation (Mosteshar, 2016). In light of this, it is essential to ensure that privacy considerations are not overlooked when examining issues of satellite sensed data under national legislation.[45] Therefore, it is important, in this context, to assess the existing legal frameworks pertaining to data privacy first under international law, and then under Australian and Indonesian law.

International law regime related to data privacy

The characteristics of remote sensing make it probable that technologies used to carry out these activities would have privacy ramifications. The applicability of privacy law in this context stems from the understanding that while the sensing activity itself takes place in space through Earth observation satellites, the information gathered by these satellites relate to activities and information on Earth (Freeland & Ireland-Piper, 2022). Thus, an Earth observation satellite used in obtaining satellite imagery of areas where a natural disaster has occurred would essentially be capturing data relating to the disaster areas, and not 'space' data. This presents an opportunity to examine these activities within the framework of existing international law to assess how effectively they address privacy concerns during remote sensing.

In this respect, the Universal Declaration of Human Rights (UDHR),[46] International Covenant on Civil and Political Rights (ICCPR)[47] and the International Covenant on Economic Social and Cultural

[44] *See also* The International Charter Space and Major Disasters Executive Secretariat. (n.d.). *How to become an authorised user.* Retrieved June 7, 2023. https://disasterscharter.org/web/guest/how-to-register-as-a-user

[45] Williams, M. (2006). *Legal aspects of the privatization and commercialization of space activities, remote sensing, and national space legislation.* International Law Association. https://ila.vettoreweb.com/Storage/Download.aspx?DbStorageId=1044&StorageFileGuid=2dc0ec9c-0fb5-4b9d-b12d-20f82ec3e4ae

[46] Universal Declaration of Human Rights, GA Res 217A (III), UN Doc A/RES/217(III) (10 December 1948)

[47] International Covenant on Civil and Political Rights, UN GA Res 2200A (XXI) — adopted 16 December 1966, opened for signature 19 December 1966, entered into force 23 March 1976.

Rights (ICESCR)[48] are three key international covenants that form the basis of human rights provisions in various international, regional, and national legal frameworks.

Interestingly, the proximity in the dates the ICCPR and ICESCR were adopted (16 December 1966) and when the first major international treaty governing space — *Outer Space Treaty* — was adopted (19 December 1966) cannot be seen as a mere coincidence. Reflecting on the provisions of Article III of the *Outer Space Treaty* shows that its intention is to be read in consonance with other international law. Specifically, it provides that 'State Parties to the Treaty shall carry on activities in the exploration and use of outer space... in accordance with international law...in the interest of maintaining international peace and security and promoting international co-operation and understanding.' The inclusion of the phrase 'in accordance with international law' in this provision, as well as in Article I, can be interpreted as a deliberate consideration of existing international law such as UDHR as well as concurrent negotiations that were being carried out in respect of other international legal framework, such as the ICCPR, at that time.

Furthermore, the provision of Article III of the *Outer Space Treaty*, when read in conjunction with Articles I and II, establishes a dual concept. Firstly, it guarantees the freedom of every country to engage in exploration activities in outer space. Secondly, it prohibits any nation from asserting territorial sovereignty over any part of outer space. As remote sensing is an activity conducted from outer space, it falls within the scope of the aforementioned freedom (von der Dunk, 2013: 2). This is further buttressed by the right to freedom to seek, receive, and impart information through any media or frontier, pursuant to the provisions of the UDHR and ICCPR.[49] Since remote sensing is used to seek and receive information about activities taking place on the Earth's surface, it aligns with these rights.

The right to privacy, guaranteed under the UDHR and ICCPR, is a competing right that should be considered in the context of remote sensing. Article 12 of the UDHR states that 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour or reputation.' A similar provision is found in Article 17 of the ICCPR. However, these privacy provisions are drafted in broad terms and do not specifically address the privacy concerns that may arise from remote sensing activities. Additionally, while Greenwood et al. (2017)[50] argues that data privacy during humanitarian crises should align with international human rights and humanitarian law and standards, there is no established internationally recognised humanitarian standard for data privacy in such situations.[51] Consequently, these instruments do not sufficiently accommodate or regulate data privacy issues in the context of remote sensing during natural disasters.

On one hand, the *Outer Space Treaty* grants each nation the freedom to conduct activities in outer space, a freedom extended to the freedom to seek, receive, and impact information through any frontier (in this case, remote sensing) under Article 19 of both the UDHR and ICCPR. This freedom is not subject to territorial jurisdiction in outer space. On the other hand, the UDHR and ICCPR guarantee individuals' right to privacy. These two perspectives create a potential conflict that requires a balancing act, one that is not clearly addressed under international human rights law.

---

48 International Covenant on Economic, Social and Cultural Rights, UN GA Res 2200A (XXI) — adopted 16 December 1966, opened for signature 19 December 1966, entered into force 3 January 1976.

49 Article 19 UDHR and Article 19 ICCPR.

50 Greenwood, F., Howarth, C., Poole, D. E., Raymond, N. A., & Scarnecchia, D. P. (2017). *The signal code: A human rights approach to information during crisis*. Harvard Humanitarian Initiative. https://hhi.harvard.edu/sites/hwpi.harvard.edu/files/humanitarianinitiative/files/signalcode_final.pdf?m=1607469621

51 Halle, E. (2018). International human rights framework to disaster management. https://dx.doi.org/10.2139/ssrn.3287849

It is worth noting that the *Outer Space Treaty* lacks specific rules or guidance on how the freedom to conduct activities in outer space may be limited, particularly regarding potential privacy concerns that may arise during remote sensing. Some argue that this lack of specificity could be attributed to the fact that privacy concerns resulting from remote sensing were not prominent when the *Outer Space Treaty* was adopted, as high-resolution remote sensing technology did not exist at that time (von der Dunk, 2013: 7). Moreover, the primary focus of the United Nations at that time was to create guiding rules for the exploration of outer space for peaceful purposes, and for the benefit of every nation, in an era when the two major space faring nations — US and USSR — were increasingly developing their space technology capabilities (Freeland and Pacujlic, 2018).

As a result, von der Dunk (2013) suggests that in the absence of any general international law agreements or customary international law addressing privacy concerns, which could be incorporated into the scope of the *Outer Space Treaty* under Article III, it is the responsibility of individual countries to establish safeguards within their national laws to limit the seemingly unfettered freedom to conduct remote sensing activities that the *Outer Space Treaty* or any other international law has not limited, in light of privacy concerns. This is so as Article VI of the *Outer Space Treaty* imposes international responsibility on individual countries for their own outer space activities, as well as those of non-governmental entities under their jurisdiction. Accordingly, countries have the authority to regulate private space activities, including the power to prohibit them altogether or require compliance with specific national laws protecting privacy of individuals and entities (von der Dunk, 2013).

With this in mind, the next section examines the legal framework on data privacy in Australia and Indonesia to assess the adequacy of these laws in addressing privacy concerns arising from remote sensing activities.

Legal framework on data privacy in Australia and Indonesia

Australia

The main data privacy framework in Australia is the *Privacy Act*.[52] One of its objects under Section 2A is 'to provide the basis for nationally consistent regulation of privacy and the handling of personal information.' Personal information is defined in Section 6 as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.' Georgiades (2020) opines that the scope of the *Privacy Act* applies to personal information recorded and captured digitally.

As has been previously discussed, during a natural disaster, personal information collected by satellites can result in misuse. For example, satellites can capture very high-resolution images when used for remote sensing (Kaku, 2019). The capturing of such images has potential ramifications for people's privacy because such images can include information that can identify an individual. Consequently, the processing of the information captured would need to comply with the *Privacy Act* as it falls within the scope of collecting, storing, and monitoring of data. Although the Act does not explicitly mention satellites, it applies to data collected by various means, which includes satellites.

[52] Privacy Act, 1988 (Cth). Australia currently lacks a legal framework specifically regulating the use of remote sensing technology to prevent data privacy breaches. Nonetheless, it is important to examine the existing data privacy framework, to determine if they are adequate in preventing misuse during natural disasters. *See* The University of Adelaide. (2019). *Laws applicable to remote sensing*. Australian navigational guide explaining laws for space. https://spacelaws.com/articles/laws-applicable-to-remote-sensing-activities/

Therefore, compliance with the provisions of the *Privacy Act* is required when collecting personal information.

The *Privacy Act* is applicable to and imposes obligations on APP entities. Section 6 defines an APP entity to be an agency or an organisation. An agency includes *inter alia,* a Minister, a Department, a body, or tribunal established for a public purpose under a Commonwealth, State, or Territory law. An organisation is defined under Section 6C to include an individual, body corporate, partnership, unincorporated association, or trust. However, State or Territory authorities, political parties, and small business operators are not considered organisations.[53]

An important provision of the *Privacy Act* is Section 5B that deals with extra-territorial applicability of the *Privacy Act*. Section 5B(2) and (3) extends the applicability of the *Privacy Act* to organisations or small business operators with an 'Australian link'. Examples of Australian link under Section 5B(2) include where an organisation is incorporated or forms a partnership in Australia. By virtue of Section 5B(3), even where an organisation or small business operator does not fall under any of the above listed entities, it would still be considered to have an Australian link if it carries on business in Australia. The term 'carries on business in Australia' has generally been viewed as two elements that are connected; however, they can be considered separately (*Luckins v Highway Motel (Carnavon) Pty Ltd*, 1975; *Bray v F Hoffman-La Roche Ltd*, 2002; *ASIC v Active Super (No 1)*, 2012).

In a recent ruling, the full bench of the Federal Court interpreted 'carries on business in Australia' to encompass foreign organisations that collect or hold personal information of persons located in Australia, notwithstanding that such entities do not have physical assets in Australia (*Facebook v. AIC*, 2022). Thus, merely collecting or handling personal information of any person located in Australia will suffice to make an entity subject to the provisions of the *Privacy Act* (Svantesson, 2014, 2015)[54]. This means that as long as satellites are used to carry on business which involves collection, holding or storing of personal information of any person located in Australia, the *Privacy Act* will apply.

The *Privacy Act* also protects biometric information which is categorised under Section 6 as sensitive information. While Section 6 does not include a list of information that could be considered biometric information, the Office of the Australian Information Commissioner lists attributes such as an individual's face, iris, fingerprint, palm, voice, and signature, as constituting biometric information.[55] This information can be collected with the relevant individual's consent, except when authorised by law or to prevent a serious threat to life, health, or safety (*Privacy Act 1988* (Cth) APPs 3.3, 3.4). In this regard, Maniadaki et al. (2021) argues that 'the application of facial recognition or big data analytical software in data collected by remote sensing technology puts in danger the protection of personal data when it constitutes the process of personal data.'

Whilst satellite imagery is useful for weather monitoring and defence intelligence, in the event of natural disasters, the use of high-resolution satellite imagery create challenges for data protection (Coffer, 2020). In addition to geographical locations and interactive maps, there are now facial recognition technologies causing more concern for personal data collection (Maniadaki et al., 2021). Since satellites can capture higher resolution images, it is crucial to comply with the requirements set

---

[53] Office of the Australian Information Commissioner. (n.d.). State and territory privacy legislation. Retrieved June 7, 2023. https://www.oaic.gov.au/privacy/privacy-in-your-state#:~:text=Queensland%2C%20the%20Northern%20Territory%20and,public%20sector%20health%20service%20providers

[54] *See also* Ganko, M. (2022, December 15). Privacy is not dead in Australia; it's diffusing. *Iapp*. https://iapp.org/news/a/privacy-is-not-dead-in-australia-its-diffusing

[55] Office of the Australian Information Commissioner. (n.d.). *Biometric scanning.* https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/biometric-scanning

out in the *Privacy Act* if satellite imagery includes biometric information. Of importance is Schedule 1 of the *Privacy Act* which contains 13 Australian Privacy Principles (APPs) that govern the utilisation, exposure, and safeguarding of gathered data (Alazab et al., 2021; Daly, 2018; Sainty & Rowe, 2020). Among these principles, APP 4, 6, 8, and 11 may be applicable to the collection, use, and disclosure of data gathered by satellites in different contexts including remote sensing activities. The relevant APPs are examined subsequently.

APP 4 provides the way in which an entity is to handle unsolicited personal information. Unsolicited personal information is described under Schedule 1 to mean personal information received by an APP entity without it taking active steps to collect such information. This APP is relevant to satellites since they can often inadvertently collect data about an individual. This could also lead to unauthorised surveillance or uncontrolled data generation and use (Caron et al., 2016). If unsolicited data is obtained in the process of carrying out remote sensing activities, the APP entity must ascertain whether this type of data can be collected under APP3. According to APP 3, data can only be collected by an agency or organisation if it is reasonably necessary or directly related to the agency or organisation's functions and activities. If the APP entity determines that it can collect the type of data under APP 3 or data collected is contained in a Commonwealth Record, then the APP entity is not mandated to destroy or de-identify the information. However, Schedule 1, Part 2, Section 4.4 of the *Privacy Act* provides that the entity must comply with APPs 5-13.

APP 6 outlines the framework governing the circumstances under which an APP entity can use or disclose personal information. An APP entity can use or disclose personal information if it is relevant to the 'primary purpose' of collecting that information. In 2020, the Australian Information Commissioner sued Facebook (now Meta) for inter alia disclosing the personal and sensitive information of Australian Facebook users for a purpose other than that for which it was collected between 2014 and 2015, thereby contravening APP 6.[56] According to Perram J, 'APP 6 prevents an organisation which has collected information for a particular purpose to use it for another, except in limited circumstances' (*Facebook v AIC*, 2022). As noted by the Court in this case, personal information can still be used and disclosed for a secondary purpose under certain circumstances. These exceptions, contained under Schedule 1 of the *Privacy Act*, include situations where the APP entity is an organisation and a permitted health scenario exists, or when the secondary use or disclosure is mandated by an Australian law or an order of a court or tribunal. This APP is relevant in the context of satellites and natural disasters because any personal information collected via satellite during a natural disaster could be used and disclosed for the primary purpose of collecting data to ensure safety. More importantly, breach of this APP could lead to unauthorised surveillance or uncontrolled data generation and use (Caron et al., 2016: 10). Part VIA of the *Privacy Act* is closely related to the provisions of APP 6 and contains special provisions that apply to emergency situations or disasters (which by necessary implication includes natural disasters). It specifies how personal information obtained during a declared[57] emergency or disaster should be handled by entities that obtain such information. The entities permitted to handle this information are agencies, organisations, and persons (*Privacy Act 1988* (Cth) s. 80P(7)). While agencies can disclose information to other agencies, State or Territory authorities, organisations, entities involved in disaster management, or even a person responsible to an affected individual (*Privacy Act 1988* (Cth) s. 80P(1)(c)), organisations or any other person can only disclose such information to

[56] Byrne, E. (2023, March 7). *High Court to decide if Facebook is liable for the possible breach of 300,000 Australians' personal data.* ABC News. https://www.abc.net.au/news/2023-03-07/facebook-in-australian-high-court-over-data-breach/102061004

[57] The Prime Minister is empowered under Section 80J to make a declaration of emergency.

agencies, entities providing services to affected individuals, and entities prescribed by regulation or the Minister (*Privacy Act 1988* (Cth) s. 80P(1)(d)). This allows for flexibility in expanding the categories of entities that can access personal information of individuals affected by natural disasters as needed. However, the practical applicability of this provision to instances where personal data is collected through remote sensing during natural disasters remains uncertain, especially when entities are operating from outside Australia's territorial borders.

APP 8 allows for cross-border disclosure of data collected and works in conjunction with Section 16C of the *Privacy Act*. APP 8 stipulates that if data is to be disclosed cross-border, the APP entity responsible for the disclosure must take reasonable steps to ensure that the recipient overseas does not violate any of the APP principles (*Privacy Act 1988* (Cth) APP 8.1). The APP entity disclosing the information is accountable for any failure of the overseas entity to comply with the APPs. In the event that an APP entity wishes to disclose data collected from a natural disaster to an overseas entity, it is required to ensure that the recipient adheres to these principles. Breach of this APP could lead to uncontrolled generation and use, and information security risks (Caron et al., 2016).

APP 11 governs the security of personal information collected by an APP entity. Breach of this APP could lead to uncontrolled generation and use, inadequate authentication, and information security risks (Caron et al., 2016). The Court in *Facebook v AIC* (2022) held that Facebook was in breach of APP 11 as it failed to implement measures to obtain consent directly from the affected Australian users before disclosing their personal information. It is mandatory for any APP entity collecting personal information to safeguard it against potential unauthorised use, loss, disclosure, alteration, or access. Additionally, once the personal information is no longer required by the APP entity, it must either be destroyed, or de-identified to prevent identification of the relevant individual (*Privacy Act 1988* (Cth) APP 11.2).

It is important to note that a person's data privacy may potentially be breached when their image is captured by remote sensing technologies when such technologies are used for monitoring purposes (Maniadaki et al., 2021). Privacy breaches may still occur even if the use is for ostensibly beneficial reasons such as search and rescue efforts during natural disasters. Non-disclosure of the purpose for data collection, details of the entity collecting such data, may exacerbate the unease and leave data subjects feeling that their right to control the use of their personal information has been unjustly compromised (Maniadaki et al., 2021). This may be the case where the person has not consented to the use of their image. The issue of consent highlights some limitations for the scope of the *Privacy Act* because if a person consents to their image being held, collected, or used by an APP entity, the *Privacy Act* will not apply. This is because consent has two purposes under the *Privacy Act*.[58] The first is that it acts as an exception when an APP entity collects and uses personal images. The second is that consent authorises the use of personal data. This therefore underscores the importance of having in place a legal framework that addresses privacy concerns of those individuals whose personal data might be included in satellite imagery collected during natural disaster management operations.

Indonesia

Similar to Australia, Indonesia also has a responsibility to ensure that its remote sensing activities do not violate international laws, including the right to privacy. However, there is no specific framework in place for regulating remote sensing activities or for addressing key issues relating to data access and international cooperation (Zunnuraeni et al., 2020). The *Space Law* and

[58] Sch 1, APPs 3.3 (a), 6.1 (a) of the *Privacy Act*.

the *Government Regulation No. 11 of 2018 Concerning Remote Sensing (GR 11/2018)* cover technical aspects of remote sensing, but not regulations for private entities engaged in remote sensing activities (Sitanggang, 2018).

The *Space Law* requires all government remote sensing activities to be conducted by the National Research and Innovation Agency, and only for specific purposes (Sitanggang, 2018). Prior to the passing of the *Personal Data Protection Law (PDP Law)*[59] in 2022, the regulation of private entities with regards to data privacy was not covered by specific laws but was part of Indonesia's broader privacy laws such as *Government Regulation No. 71 of 2019 Regarding Implementation of Electronic Systems and Transactions* and the *Minister of Communication and Informatics Regulation No. 20 of 2016 Regarding Personal Data Protection in Electronic Systems*. It was generally accepted under these earlier regulations that the collection and use of personal data required express consent from the data owner. However, these regulations were not comprehensive and only applied to specific electronic systems, instead of all telecommunication systems.[60]

The *PDP Law* now provides comprehensive rules for processing personal data, which can also apply to personal data collected during remote sensing activities.[61] Article 2 of the *PDP Law* applies to any individual, corporation, public agency, or international organisation that carries out activities within Indonesia, or outside Indonesia that may have legal consequences within Indonesia or affect Indonesian citizens. The *PDP Law* defines personal data as any data concerning a person, whether identified or who may be identified independently or combined with other information, either directly or indirectly, through an electronic or non-electronic system. Data subjects have specific rights set out under Article 5-14 of the *PDP Law*, including the right to be informed about the purpose of data collection, how the data will be used, and the liability and obligations of the party requesting the personal data. Data subjects also have the right to withdraw their consent at any time.

As previously noted, prior to the *PDP Law*, consent was the primary basis for processing personal data. While the *PDP Law* maintains this requirement, it also recognises, under Article 20, other grounds for processing personal data, including fulfilling contractual obligations, meeting legal obligations of the controller, protecting the vital interests of the data subject, performing public duties for public interest or service, or exercising lawful authority of the controller, and the processing of personal data to fulfill other lawful interests. Article 65 and 66 of the *PDP Law* prohibits certain uses of personal data, such as illegally obtaining or collecting personal data, unlawfully disclosing personal data, using personal data of another in a manner that contravenes the law, and creating false or fake personal data that may cause harm to other persons. Infractions of the *PDP Law* carry varying sanctions, ranging from fines to imprisonment. The law has a transitional period of two years for compliance from the date of its enactment, and a data protection authority will be established pursuant to Article 58 through a presidential regulation, reporting directly to the president.

---

59 Law No. 27 of 2022 on Protection of Personal Data.

60 Iskandar, E., Lubis, D.B., & Hartanto, A.W. (2023, January 6). *The technology, media and telecommunications review: Indonesia.* The Law Reviews. https://thelawreviews.co.uk/title/the-technology-media-and-telecommunications-review/indonesia

61 Panggabean, K., Purba, J., & Karina, T. (2022, October). *Highlights of Indonesia's personal data protection law.* Norton Rose Fulbright. https://www.nortonrosefulbright.com/en/knowledge/publications/31bce8f0/highlights-of-indonesias-personal-data-protection-law

Liability for misuse of satellites

Liability and responsibility under international legal framework

As previously discussed, the main international frameworks regarding use of satellites for remote sensing and disaster management are not legally binding, and do not deal with data privacy concerns arising from misuse of satellites. Thus, liability for misuse of satellites which results in privacy breaches might be difficult to impose if reliance is placed solely on the *Remote Sensing Principles* and *Disaster Charter*. Also, it is debatable whether the *Liability Convention*,[62] which deals with liability arising from damages caused by space objects, would cover violations of individual privacy rights (Nafis et al., 2021). Based on Articles II and III of the Convention, it has been argued that the Convention was primarily designed to address physical damages[63] collisions between spacecrafts and component parts (Christol, 1980; Dodge, 2014).

Notwithstanding, liability can arise under general international law if a State can successfully argue that another State's activities, including those of its private actors or corporations, caused damage to it or its nationals (Schmalenbach, 2022).[64] For instance, State A could argue that State B's remote sensing activities violated the privacy of State A's nationals. In addition, most of the principles under the *Remote Sensing Principles* restate the rules under the *Outer Space Treaty* or allude to general principles of international law.[65]

Also, the Preamble of the *Disaster Charter* refer to the *Remote Sensing Principles* which implies that the Principles should be observed when carrying out remote sensing activities under the *Disaster Charter*. Article VI of the *Outer Space Treaty* provides that 'State Parties to the Treaty shall bear international responsibility for national activities in outer space... whether such activities are carried on by government agencies or by non-government entities...' This means that States are responsible for any wrongdoing caused in outer space either by the government, or by private entities. This would extend to commercial activities. Remote sensing is listed as a type of commercial activity which is increasingly being carried out by private entities (Gupta & Raju, 2019).

Resultantly, through a combined reading of the above international instruments, States can be held responsible for remote sensing activities carried out by them, and their private entities during natural disasters.[66] Since Australia and Indonesia are parties to the *Outer Space Treaty*, it would therefore be important to examine the liability provisions under their various national laws as they relate to satellites.

Liability and responsibility under national legal framework

Australia

The *Space Act* sets out legal liability for any damage caused in outer space by a space object launched by Australia. Section 8 of the Act defines 'damage' in the same way as the *Liability*

[62] Convention on International Liability for Damage Caused by Space Objects (UN GA Res 2777 (XXVI), annex)—adopted on 29 November 1971, opened for signature on 29 March 1972, entered into force on 1 September 1972.

[63] Article I define damage as 'loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations.

[64] A common example of this is environmental pollution. Here, States have claimed that transboundary pollution injures their rights to enjoy their territory or that the transboundary pollution is causing injury to their nationals.

[65] *See* Principle IV, *Remote Sensing Principles.*

[66] *See* Principle XIV of the *Remote Sensing Principles* which buttresses this point.

Convention. Therefore, the same argument made earlier applies here, which is that violation of privacy rights resulting from the misuse of satellites for remote sensing activities are not covered by this Act. Notwithstanding that the *Space Act* liability provisions might only apply to physical damage involving satellites during launch into outer space or re-entry into Earth, the *Privacy Act* will apply to privacy breaches relating to data collected through satellites or other means.

By virtue of Section 13(1)(a) of *Privacy Act,* an act or practice that breaches any of the APPs in relation to personal information about an individual is an interference with the privacy of such an individual. Where this act or practice is done repeatedly by the APP entity, such would be a serious and repeated interference with privacy and is classified as a civil liability under Section 13G. Under Section 13G (2) and (3), the maximum penalty that can be imposed on a body corporate for this contravention is $50,000,000, and $2,500,000 for a person other than a body corporate. It should be noted that by virtue of Section 80U, only the Information Commissioner is authorised to bring an application before the Federal Court or Federal Circuit Court and Family Court of Australia in respect of a civil liability action.[67] Thus, if a satellite is used by an APP entity for remote sensing activities that violate the provisions of any of the APPs under the *Privacy Act*, the following enforcement actions can be taken against that entity — civil liability actions, infringement notices, enforcement undertakings, and injunctions.

Indonesia

Pursuant to Article 41(1) of the *Space Law,* Indonesia is responsible for overseeing all of its national space activities and is accountable for any wrongful acts that result from the misuse of satellites. Like Australia, Indonesia has provisions in its *Space Law*[68] that deal with liability for damage caused in space, on Earth or to an aircraft in flight. However, damage in this context is limited to physical damage and does not cover liability for privacy breaches resulting from misuse of satellites.

Regarding the violation of personal data under the *PDP Law*, both administrative and criminal sanctions may be imposed. In the absence of a standalone regulatory framework specific to the misuse of satellites in the context of privacy breaches, the provisions of the *PDP Law* will be applicable. As provided under Article 67 and 68 of the *PDP Law*, criminal sanctions include a fine of up to IDR 6 billion and/or imprisonment of up to six (6) years. Administrative sanctions include written warning, temporary suspension of personal data processing activity, deletion of personal data, or imposition of administrative fines under Article 57. These penalties may be imposed on the management, controller, instructor, beneficial owner, or corporation.

Conclusion

In conclusion, it is apparent that international rules on the use of satellites for remote sensing activities generally lack binding force, and they do not effectively address the issue of privacy breaches that may result from satellite misuse. International human rights framework such as UDHR and ICCPR which provide for right to privacy are broad, and their provisions are not sufficiently robust to cover use of satellite data, especially for commercial or private use. In the context of natural disasters, it is even more important to ensure data privacy concerns are given due consideration

[67] *See also* Flannery, A., & Cass, S. (2020, May 21). Australia: Liability for breaches of Privacy Act to increase, but class actions unlikely to be supported. *Mondaq*. https://www.mondaq.com/australia/data-protection/938568/liability-for-breaches-of-privacy-act-to-increase-but-class-actions-unlikely-to-be-supported

[68] *See* Article 76(2).

while the satellites are being used for remote sensing during the disaster management process (Mosteshar, 2016).

As already stated, with advancements in technology, it becomes even more probable that data collected during natural disasters by the sophisticated sensors placed on LEO satellites would include those capable of identifying individuals. As a result, safeguards need to be in place to ensure that satellites continue to play the important role of aiding in rescue efforts during natural disasters without infringing on individuals' privacy rights in the process. As this article highlighted, it is a challenging feat to try to balance the public interest in disaster management with individual privacy rights, mainly because the expectation of privacy during natural disasters differs considerably from non-emergency situations (Sanfilippo et al., 2020). However, this should not be a basis for countries to take with levity the need to adequately consider and take steps to mitigate the materialisation of the risks of privacy breaches resulting from remote sensing activities during natural disasters.

In the absence of a uniform set of rules at the international level that adequately regulates data sharing or privacy issues, individual countries can address these issues through the instrumentality of their national laws.[69] In the case of Australia and Indonesia, both countries lack standalone legal frameworks that specifically address privacy breaches caused by misuse of satellites during natural disasters. However, a combination of space activity legislation and data protection laws in both countries can serve as a temporary measure to determine liability for privacy breaches resulting from satellite misuse during natural disasters.

Ultimately, it is recommended that both countries review their existing legal frameworks to address the potential unintended consequences of advancing remote sensing capabilities on data privacy. Since both countries have provisions in their space legislation[70] requiring adequate insurance in respect of liability for damage (Kerkonian, 2021), the scope of what constitutes liability for damage under both legal frameworks could be expanded to explicitly include provisions relating to privacy.

Another suggestion is for both countries to make remote sensing activities subject to licensing through their domestic laws. This is supported by the provision of Article VI of the *Outer Space Treaty* which imposes an obligation on countries to authorise and supervise space activities within their respective jurisdictions. This authorisation regime, which could be in form of compulsory licensing for entities engaged in remote sensing activities, provides an opportunity for both countries to impose restrictions or conditions on space activities, including provisions for respecting privacy. These restrictions could include satellite capacity limits, resolution limits for satellite images, exclusive acquisition of rights to relevant satellite images[71], requirements of blurring personal identifying information in satellite images, and more. National legislation should play a significant role in addressing privacy concerns arising from remote sensing activities conducted with LEO satellites (Linden, 2016), as not only States, but also private entities and individuals globally are increasingly involved in commercial remote sensing activities. Expressly including respect for privacy as a condition for engaging in space activities would be a pioneering move and set a precedent for other countries to follow.

---

69 Rotola, G., Farrar, L., Nasr, F., Wiser, L., Navalgund, R., Ciarravano, L., & Grattan, K. (2022, January). *Earth Observation Data, Climate Change, and Human Rights*. Jus Ad Astra. http://www.jusadastra.org/SGAC-Law-Climate-Change.html

70 Space (Launches and Returns) Act, 2018, Section 48; Law No 21 of 2013 Concerning Space Activities, Article 84(1).

71 Rotola, G., Farrar, L., Nasr, F., Wiser, L., Navalgund, R., Ciarravano, L., & Grattan, K. (2022, January). *Earth Observation Data, Climate Change, and Human Rights*. Jus Ad Astra. http://www.jusadastra.org/SGAC-Law-Climate-Change.html

References

1. Alazab, M., Hong, S.-H., & Ng, J. (2021). Louder bark with no bite: Privacy protection through the regulation of mandatory data breach notification in Australia. *Future Generation Computer Systems*, *116*, 22–29. https://doi.org/10.1016/j.future.2020.10.017
2. Boon, H. (2013). Preparedness and vulnerability: An issue of equity in Australian disaster situations. *Australian Journal of Emergency Management*, *28*(3), 12–16. https://search.informit.org/doi/10.3316/agispt.20132324
3. Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review*, *32*(1), 4–15. https://doi.org/10.1016/j.clsr.2015.12.001
4. Christol, C. Q. (1980). International liability for damage caused by space objects. *American Journal of International Law*, *74*(2), 346–371. https://doi.org/10.2307/2201505
5. Coffer, M. M. (2020). Balancing privacy rights and the production of high-quality satellite imagery. *Environment Science & Technology*, *54*(11), 6453. https://doi.org/10.1021/acs.est.0c02365
6. Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law & Security Review*, *34*(3), 477–495. https://doi.org/10.1016/j.clsr.2018.01.005
7. De Beer, A. (2020). The refusal of access to high-resolution remote sensing data for reasons of national security–a rule of customary international law? *Tydskrif Vir Die Suid-Afrikaanse Reg* [*Journal of South African Law*], *2020*(1), 74–87.
8. Dodge, M. (2014). Earth Observation and the Needs of the Many: The Future Structure of International Disaster Relief Law and Management. *Annals of Air and Space Law*, *39*, 355.
9. Sitanggang, D.F.D. (2018). International Law Analysis of the Restrictions Imposed on Remote Sensing Satellite Through Shutter Control. *Jurnal Mimbar Hukum*, *30*(2), 389–406. https://doi.org/10.22146/jmh.31151
10. Emery, W., & Camps, A. (2017). *Introduction to satellite remote sensing: Atmosphere, ocean, land and cryosphere applications*. Elsevier. https://doi.org/10.1016/C2015-0-04517-8
11. Freeland, S., & Ireland-Piper, D. (2022). Space law, human rights and corporate accountability. *UCLA Journal of International Law and Foreign Affairs, 26* (1), 1–34.
12. Freeland, S., & Pecujlic, A. N. (2018). How do you like your regulation: Hard or soft? : The Antarctic Treaty and the Outer Space Treaty compared. *National Law School of India Review, 30*(1), 11–36. https://repository.nls.ac.in/nlsir/vol30/iss1/2
13. Froehlich, A., & Seffinga, V. (2018). *National space legislation: A Comparative and Evaluative Analysis*. Springer. https://doi.org/10.1007/978-3-319-70431-9
14. Georgiades, E. (2020). A Right that should've been: Protection of personal images on the Internet. *IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property*, *61*(2), 275–327.
15. Gummadi, G., & Gupta, B. (2022). Remote sensing data and international IP laws. *Journal of Legal Subjects*, *20*(2), 13–28. https://doi.org/10.55529/jls22.13.28
16. Gupta, B., & Raju, K. (2019). Understanding international space law and the liability mechanism for commercial outer space activities—unravelling the sources. *India Quarterly*, *75*(4), 555–578. https://doi.org/10.1177/0974928419874553
17. Hakim, W. L., & Lee, C.-W. (2020). A review on remote sensing and GIS applications to monitor natural disasters in Indonesia. *Korean Journal of Remote Sensing*, *36*(6_1), 1303–1322. https://doi.org/10.7780/kjrs.2020.36.6.1.3
18. Housen-Couriel, D. (2016). Cybersecurity threats to satellite communications: Towards a typology of state actor responses. *Acta Astronautica*, *128*, 409–415. https://doi.org/10.1016/j.actaastro.2016.07.041

19. Kuner, C., & Marelli, M. (2020). *Handbook on data protection in humanitarian action*. The International Committee of the Red Cross. https://shop.icrc.org/download/ebook?sku=4305.01/002-ebook
20. Ito, A. (2011). *Legal aspects of satellite remote sensing*. Brill.
21. Mosteshar, S. (2016). Regulation of remote sensing by satellites. In R. Jakhu, & P.S. Dempsey (Eds.), *Routledge Handbook of Space Law* (pp. 144-159). Routledge. https://doi.org/10.4324/9781315750965
22. National Research Council. (1996). *Cryptography's role in securing the information society.* National Academy Press. https://doi.org/10.17226/5131
23. Nishara, N., & Pandey, R. (2015). Enhancing security in public clouds using data anonymization techniques. *International Journal of Computer Applications*, *128*(1), 33–36. https://doi.org/10.5120/ijca2015906428
24. Kaku, K. (2019). Satellite remote sensing for disaster management support: A holistic and staged approach based on case studies in Sentinel Asia. *International Journal of Disaster Risk Reduction*, *33*, 417–432. https://doi.org/10.1016/j.ijdrr.2018.09.015
25. Kemp, K. (2022). Strengthening enforcement and redress under the Australian Privacy Act. *Global Privacy Law Review*, *3*(3), 150–162. https://doi.org/10.54648/gplr2022016
26. Kerkonian, A. D. (2021). National regulation of space activities. In A.D. Kerkonian (Ed.), *Space Regulation in Canada: Past, Present and Potential* (pp. 235–319). Springer. https://doi.org/10.1007/978-3-030-68692-5
27. Linden, D. (2016). The impact of national space legislation on private space undertakings: Regulatory competition vs. harmonization. *Journal of Science Policy & Governance*, *8*(1), 1–17.
28. Maniadaki, M., Papathanasopoulos, A., Mitrou, L., & Maria, E.-A. (2021). Reconciling remote sensing technologies with personal data and privacy protection in the European Union: Recent developments in Greek legislation and application perspectives in environmental law. *Laws*, *10*(2), No. 33. https://doi.org/10.3390/laws10020033
29. Nafis, R. W., Supriyadhie, M. K., & Adya, P. (2021). The Utilization of GSO by Indonesia as a Subjacent State Based on Space Treaty 1967. *Proceedings of the 1st International Conference on Science and Technology in Administration and Management Information, ICSTIAMI 2019, 17-18 July 2019, Jakarta, Indonesia*. http://dx.doi.org/10.4108/eai.17-7-2019.2303333
30. Nugraha, T. R., Putro, Y. M., Aditya Nugraha, R., & Christiawan, R. (2022). Indonesian space activities: The long and winding road. *Astropolitics*, *20*(2–3), 238–250. https://doi.org/10.1080/14777622.2022.2141113
31. Page, J., & Besco, L. (2021). Dispossession through collision: Low-Earth orbit and planetary sustainability. *Territory, Politics, Governance*, 1–18. https://doi.org/10.1080/21622671.2021.1903543
32. Qu, Y., Nosouhi, M. R., Cui, L., & Yu, S. (2019). Privacy preservation in smart cities. In D. B. Rawat, & K. Z. Ghafoor. *Smart cities cybersecurity and privacy* (pp. 75–88). Elsevier. https://doi.org/10.1016/C2017-0-02545-4
33. National Research Council. (2001). Realizing the potential of remote sensing. In *Transforming remote sensing data into information and applications*. National Academies Press. https://doi.org/10.17226/10257
34. Sanfilippo, M. R., Shvartzshnaider, Y., Reyes, I., Nissenbaum, H., & Egelman, S. (2020). Disaster privacy/privacy disaster. *Journal of the Association for Information Science and Technology, 71*(9), 1002–1014. https://doi.org/10.1002/asi.24353
35. Santos, C., & Rapp, L. (2019). Satellite imagery, very high-resolution and processing-intensive image analysis: Potential risks under the GDPR. *Air and Space Law, 44*(3), 275–295. https://doi.org/10.54648/aila2019018
36. Sheinidashtegol, P., Musaev, A., & Atkison, T. (2019). Investigating personally identifiable information posted on Twitter before and after disasters. In Y. Xia, L.-J. Zhang. *Services — SERVICES 2019: 15th World Congress, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings* (pp. 31–45). Springer. https://doi.org/10.1007/978-3-030-23381-5_3

37. Sainty, K., & Rowe, B. (2020). OAIC v Facebook. *Communications Law Bulletin*, *39(2)*. http://www5.austlii.edu.au/au/journals/CommsLawB/2020/19.pdf
38. Sastrawidjaja, L., & Suryanegara, M. (2018). Regulation challenges of 5G spectrum deployment at 3.5 GHz: The framework for Indonesia. *Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)*, 213–217. http://dx.doi.org/10.1109/EECCIS.2018.8692880
39. Schmalenbach, K. (2022). Convention on International Liability for Damage Caused by Space Objects. In P. Gailhofer, D. Krebs, A. Proelss, K. Schmalenbach, R. Verheyen (Eds.), *Corporate liability for transboundary environmental harm: An international and transnational perspective* (pp. 523–536). Springer Cham. http://dx.doi.org/10.1007/978-3-031-13264-3_11
40. Singh, R., Kaul, S., & Deva Rao, S. (2012). *Current developments in air space law*. National Law University Press.
41. Supancana, I. B. R. (2006). *Space law development in retro and prospect*. Mitra Karya Publisher.
42. Supancana, I. B. R. (2015). How the progressive development of outer space law affects the formulation of national space legislation: The experience of Indonesia. *Air and Space Law*, *40*(1), 93–106. https://doi.org/10.54648/aila2015009
43. Svantesson, D. J. B. (2014). The extraterritoriality of EU data privacy law-its theoretical justification and its practical effect on US businesses. *Stanford Journal of International Law*, *50*(1), 53–102.
44. Svantesson, D. J. B. (2015). Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation. *International Data Privacy Law*, *5*(4), 226–234. http://dx.doi.org/10.1093/idpl/ipv024
45. Tatem, A. J., Goetz, S. J., & Hay, S. I. (2008). Fifty years of Earth-observation satellites: Views from space have led to countless advances on the ground in both scientific knowledge and daily life. *American Scientist*, *96*(5), 390–398.
46. Tronchetti, F. (2015). Legal aspects of satellite remote sensing. In F.G. von der Dunk, & F. Tronchetti (Eds.), *Handbook of Space Law* (pp. 501–553). Edward Elgar Publishing.
47. Verco, E. (2021). Satellites are cyber insecure: We need regulation to avoid a disaster. *Australian National University Journal of Law and Technology*, *2*(2), 57–94. https://anujolt.org/article/30203-satellites-are-cyber-insecure-we-need-regulation-to-avoid-a-disaster
48. von der Dunk, F. (2013). Outer space law principles and privacy. In R. Purdy, & D. Leung (Eds.), *Evidence from Earth observation satellites* (pp. 241–258). Brill Nijhoff. https://doi.org/10.1163/9789004234031
49. von der Dunk, F. (2002). United Nations principles on remote sensing and the user. In R. Harris (Ed.), *Earth observation data policy and Europe* (pp. 29–40). CRC Press.
50. von Dietze, A., & Allgrove, A.-M. (2014). Australian privacy reforms—An overhauled data protection regime for Australia. *International Data Privacy Law*, *4*(4), 326–341. http://dx.doi.org/10.1093/idpl/ipu016
51. Yu, M., Yang, C., & Li, Y. (2018). Big data in natural disaster management: A review. *Geosciences, 8*(5), No. 165. https://doi.org/10.3390/geosciences8050165
52. Zollner, K. (2018). United Nations platform for space-based information for disaster management and emergency response (UN-SPIDER). In C. Brünner, G. Königsberger, & A. Rinner (Eds.), *Satellite-based Earth observation.* Springer. 235–241. https://doi.org/10.1007/978-3-319-74805-4_24
53. Zunnuraeni, Z., Minollah, M., Ilwan, M., & Nurbani, E. S. (2020). Legal concept for remote sensing as the foundation of Indonesian space law. Proceedings of the 1st Annual Conference on Education and Social Sciences (ACCESS 2019). Atlantis Press. 83–85. https://doi.org/10.2991/assehr.k.200827.022

Information about the authors:

Temitope Lawal* — Ph.D. Candidate, Faculty of Law, Bond University, Robina, Queensland, Australia.
tlawal@bond.edu.au
ORCID: https://orcid.org/0000-0002-3844-3945

Melanie Jackson — Senior Teaching Fellow, Faculty of Law, Bond University, Robina, Queensland, Australia.
mjackson@bond.edu.au
ORCID: https://orcid.org/0000-0002-5386-4406

Eugenia Georgiades — Ph.D. in Law, Assistant Professor, Faculty of Law, Bond University, Robina, Queensland, Australia.
egeorgia@bond.edu.au
ORCID: https://orcid.org/0000-0002-4040-7652

Сведения об авторах:

Лаваль Т.* — аспирант, юридический факультет, Университет Бонд, Робина, Квинсленд, Австралия.
tlawal@bond.edu.au
ORCID: https://orcid.org/0000-0002-3844-3945

Джексон М. — старший преподаватель, юридический факультет, Университет Бонд, Робина, Квинсленд, Австралия.
mjackson@bond.edu.au
ORCID: https://orcid.org/0000-0002-5386-4406

Георгиадес Е. — Ph.D. in Law, доцент, юридический факультет, Университет Бонд, Робина, Квинсленд, Австралия.
egeorgia@bond.edu.au
ORCID: https://orcid.org/0000-0002-4040-7652

https://doi.org/10.38044/2686-9136-2023-4-2-40-63

СТАТЬИ

ЭЛЕКТРОННАЯ ФОРМА СДЕЛОК: ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Р.И. Шугаев

Фонд «Центр стратегических разработок»
125009, Россия, Москва, Газетный пер. 3–5/1

Аннотация

Данная статья посвящена анализу формы сделок, совершенных с использованием электронных и иных технических средств (электронной формы). Целью настоящего исследования является изучение сущностных особенностей и поиск оптимальной модели регулирования электронной формы сделок с учетом зарубежного опыта, теоретических наработок и судебной практики. Актуальность исследования объясняется увеличением количества сделок в электронной форме, которые требуют адекватного правового регулирования и правоприменительной практики. В статье последовательно разбираются международно признанные принципы правового регулирования электронной формы сделок (недискриминации, технологической нейтральности, функциональной эквивалентности) и их реализация в российском и зарубежном праве. Помимо этого, автор анализирует вопрос о соотношении письменной и электронной форм, разбирает и опровергает аргументы в пользу выделения электронных способов формирования воли в качестве самостоятельной (*sui generis*) разновидности формы сделок. С учетом текущей практики российских судов и иностранного опыта определяются критерии и способы достоверной идентификации лица, совершающего волеизъявление электронным способом. На основе догматических и политико-правовых аргументов отвергается излишне формальная идея о том, что единственным способом такой идентификации может быть использование квалифицированной электронной подписи. Автор также предлагает оптимальное толкование требования ГК РФ о воспроизводимости содержания электронной сделки на материальном носителе в неизменном виде. По результатам исследования предлагается ряд рекомендаций, носящих практический характер и позволяющих обеспечить принятие судьями справедливых и обоснованных решений в конкретных ситуациях при толковании положений ГК РФ об электронной форме сделок.

Ключевые слова

сделки в электронной форме, письменная форма сделок, электронный документ, электронная подпись, материальный носитель

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.
Благодарность	Автор выражает благодарность Зикуну И.И. за ценные комментарии и замечания. В то же время за любые ошибки и недочеты работы отвечает исключительно автор.

Для цитирования Шугаев, Р.И. (2023). Электронная форма сделок: вопросы правового регулирования. *Цифровое право,* 4(2), 40–63. https://doi.org/10.38044/2686-9136-2023-4-2-40-63

Поступила: 20.05.2023, принята в печать: 15.06.2023, опубликована: 31.07.2023

ARTICLES

ELECTRONIC FORM OF TRANSACTIONS: ISSUES OF LEGAL REGULATION

Roman I. Shugaev

Center for Strategic Research
3–5/1, Gazetny pereulok, Moscow, Russia, 125009

Abstract

This paper analyzes the form of transactions made with the use of electronic and other technical means (electronic form). The research aims to determine the essential features and develop an optimal model of regulation of electronic transactions form, considering foreign experience, theoretical advances, and judicial practice. The relevance of the study is explained by the increasing number of e-transactions which require adequate legal regulation and law enforcement practice. The author consecutively describes internationally recognized regulatory principles of electronic transactions form (non-discrimination, technological neutrality, functional equivalence) and their implementation in Russian and foreign law. In addition, the author analyzes the issue of the correlation between the written and electronic forms, considers and rejects arguments in favor of singling out electronic methods of will formation as an independent (sui generis) form of transactions. Considering the current Russian judicial practice and foreign experience, the study determines the criteria and methods of reliable determination of a person effecting an electronic transaction. On the grounds of dogmatic and political arguments, the overly formalistic idea that the use of a qualified electronic signature is the only way of such identification is rejected. The author also formulates an optimal interpretation of the Russian Civil Code requirement on the reproducibility of the electronic transaction content on a tangible medium unchanged. Based on the results of the study, practical recommendations are described to help judges make fair and reasoned decisions in specific situations interpreting the provisions of the Russian Civil Code on the electronic form of transactions.

Keywords

e-transactions, written form of transactions, electronic document, electronic signature, tangible medium

Conflict of interest The author declares no conflict of interest.

Financial disclosure The study has no sponsorship.

Acknowledgments The author is grateful to Zikun I.I. for his valuable comments and remarks. At the same time, the author is solely responsible for any errors and shortcomings of the paper.

For citation Shugaev, R.I. (2023). Electronic form of transactions: Issues of legal regulation. *Digital Law Journal, 4*(2), 40–63. https://doi.org/10.38044/2686-9136-2023-4-2-40-63

Submitted: 20 May 2023, accepted: 15 June 2023, published: 31 July 2023

Введение

Развитие информационных технологий, электронной коммерции и цифровой экономики в целом делает электронный документооборот основным способом взаимодействия между экономическими субъектами, который вытесняет иные формы коммуницирования. Огромное количество договоров ежедневно заключается посредством электронных средств. Речь идет не только о бытовых сделках с участием потребителей, но и о многомиллионных контрактах *B2B*. В связи с этим перед правом стоит задача по адекватному регулированию новых технологий и адаптации их к существующим правовым институтам.

Одной из важнейших, если не первостепенной, задачей становится регулирование формы сделок, совершенных с помощью электронных или иных технических средств[1]. Важность исследования данной темы в зарубежной доктрине объясняется тем, что в отступление от принципа консенсуализма, в соответствии с которым для заключения договора по общему правилу достаточно волеизъявления сторон (Jansen & Zimmermann, 2018, p. 264–265), цифровому сегменту имманентно присуща необходимость соблюдения определенной формы (Mangin, 2020, p. 135).

Наднациональное регулирование, отдельные акты международной частноправовой унификации, опыт зарубежных правопорядков дают богатую почву для исследования электронной формы сделок. Российское право также не остается в стороне, уделяя внимание такому способу формирования волеизъявления в абзаце втором п. 1 ст. 160 ГК РФ и п. 2 ст. 434 ГК РФ.

В настоящей статье предпринята попытка систематически проанализировать электронную форму сделок. Правильное понимание ее природы и существа регулирования позволит принимать справедливые и обоснованные решения в конкретных ситуациях. К сожалению, отечественная доктрина, за редкими исключениями, не уделяет должное внимание этой теме, что отражается на состоянии правоприменительной практики.

Для достижения поставленной цели, как представляется, необходимо решить ряд задач:

- сформулировать и проанализировать принципы регулирования электронной формы сделок;
- определить ее соотношение с письменной формой сделок;
- разобрать специфические для указанной формы черты, которые закреплены в законодательстве (требования к идентификации лица, изъявившего волю, и воспроизводимости на материальном носителе).

Следует сразу оговориться, что настоящая статья не затрагивает такого аспекта, как заключение электронного договора (электронная оферта и акцепт, определение момента и места заключения договора), а также не ставит перед собой в качестве основной задачи исследование конкретных процессуальных особенностей предоставления электронных документов.

[1] Далее в статье будет использоваться термин «электронная форма», который нами рассматривается как нормативно-нейтральный и ни в коем случае не свидетельствует об отличной от письменной формы природе обозначаемого им понятия.

Данная работа фокусируется преимущественно на тех вопросах, которые характеризуют такой институт гражданского права, как форма сделок (договоров).

1. Принципы регулирования электронной формы сделок

Одним из фундаментальных принципов в сфере регулирования цифровой экономики является принцип недискриминации (*principle of non-discrimination*) между документами, составленными в электронном виде и на традиционных материальных носителях. На международном уровне данный принцип, в соответствии с которым документам не может быть отказано в действительности или исковой защите единственно на том основании, что они составлены в электронной форме, провозглашен в ст. 5 Типового закона ЮНСТИРАЛ об электронной коммерции[2], а впоследствии закреплен в ст. 8 Конвенции ООН об использовании электронных сообщений в международных договорах (Нью-Йорк, 23 ноября 2005 г.).

На общеевропейском уровне указанная идея проведена в Директиве Европейского парламента и Совета Европейского союза 2000/31/ЕС от 8 июня 2000 г. о некоторых правовых аспектах информационных услуг на внутреннем рынке, в частности об электронной коммерции (Директива об электронной торговле). В соответствии с ней государства-члены в том числе должны обеспечить, чтобы правовые требования, применимые к договорному процессу, не создавали препятствий для использования электронных способов заключения договоров и не приводили к тому, чтобы такие договоры лишались юридической силы и действительности в связи с тем, что они были заключены с помощью электронных средств[3]. Важным дополнением к указанному акту является Директива Европейского парламента и Совета Европейского союза 1999/93/ЕС от 13 декабря 1999 г. «О правовых основах регулирования электронных подписей в Сообществе» (Директива об электронных подписях), которая устанавливает, что государства-члены должны обеспечить, чтобы электронной подписи не было отказано в юридической силе и допустимости в качестве доказательства в судебном разбирательстве только на том основании, что она составлена в электронной форме, не основана на квалифицированном сертификате, выданном удостоверяющим центром, или не создана с помощью защищенного устройства создания подписи[4].

Великобритания во исполнение европейских директив приняла Закон об электронных коммуникациях 2000 г. и Положение об электронных подписях 2002 г., которые были направлены не на трансформацию действующего регулирования, а, как отмечается, на закрепление уже существовавших в *common law* подходов, и то в довольно ограниченных аспектах, касающихся электронной подписи. Британский законодатель не стал закреплять принцип недискриминации в отношении электронных документов, за исключением сделок с недвижимостью, руководствуясь теми соображениями, что соответствующие положения европейской Директивы уже заложены в *common law* и необходимость в принятии каких-либо нормативных актов отсутствует (Beale, 2016).

---

[2] UNCITRAL. (1999). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998.* United Nations. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf

[3] Art. 9 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, 2000 O.J. (L 178) 1–16.

[4] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 2000 O.J. (L 13) 12–20.

Куда более интересным представляется опыт Франции. Во французском праве необходимость соблюдения письменной формы нормативно рассматривается в двух аспектах: для целей доказывания (*ad probationem*) и в качестве условия действительности сделки (договора) (*ad validatem*). Для обоих случаев законодатель закрепил во Французском гражданском кодексе (далее — ФГК) принцип недискриминации, правда, с небольшими отличиями. Рассмотрим их подробнее.

1. Требование к форме *ad probationem* заключается в следующем: если стоимость сделки равна или превышает установленную сумму, ст. 1359 ФГК признает в качестве допустимых доказательств письменные документы, подкрепленные простой (*privé*) или удостоверенной (*authentique*) подписью, исключая возможность ее доказывания свидетельскими показаниями. Цели, преследуемые ст. 1359 ФГК, с одной стороны, состоят в снижении рисков от необдуманных и мошеннических действий при совершении сделки, с другой — в предотвращении судебных разбирательств, а также снижении литигационных издержек за счет большей определенности сделок, совершенных в письменной форме (Malaurie, Aynès & Stoffel-Munck, 2020, p. 321). Важность обеспечения равнозначности документов на электронных и материальных носителях объясняется тем, что договор, существование которого невозможно доказать, может не повлечь за собой никаких реальных последствий, даже если он является действительным (*idem est non esse aut non probari*) (Terré et al., 2019).

Равнозначность *ad probationem* складывается из двух принципов: эквивалентности (*principe d'équivalence*) и равенства (*principe d'égalité*). Принцип эквивалентности (ст. 1366 ФГК) гласит, что электронный документ имеет такое же доказательственное значение, как и документ, составленный на бумаге. Принцип равенства (*principe d'égalité*) (ст. 1368 ФГК) исходит из того, что при наличии противоречий между разными документами, в том числе между документами на электронном и материальном носителе, суд не вправе отдавать приоритет документам в традиционной письменной форме, а должен устранять противоречия путем определения наиболее достоверного документа (Andreu & Thomassin, 2021, p. 672).

2. Требование к форме *ad validatem* предполагает, что равнозначность формы на бумажных и электронных носителях действует не только в отношении способов доказывания (ст. 1366 и 1367 ФГК), но и в отношении условий формальной действительности сделок (ст. 1174 ФГК). Если закон обусловливает действительность договора необходимостью соблюдения письменной формы, то заключение такой сделки посредством использования электронных и иных технических средств также будет означать соблюдение письменной формы (Bénabent, 2021, p. 42).

Впрочем, равнозначность *ad validatem* исключена для некоторых сделок (ст. 1175 ФГК) в семейном и наследственном праве (поэтому электронное завещание невозможно), а также при предоставлении обеспечения непрофессионалом (электронный залог или поручительство, выданные потребителем, невозможны). В подобных случаях совершение сделки в электронной форме будет означать ее недействительность (Bénabent, 2021, p. 116).

Нельзя не отметить, что французское право предъявляет два требования, которым должен удовлетворять электронный документ для того, чтобы он имел равное с традиционными письменными документами значение как для целей *ad probationem*, так и для целей *ad validatem*:

1) лицо, от которого он исходит, может быть должным образом идентифицировано;

2) письмо составлено и хранится в условиях, гарантирующих его целостность (Terré et al., 2019, p. 1910)[5].

[5] Требования к электронной форме подробнее рассматриваются далее в контексте функциональной эквивалентности и в последующих главах.

Российское регулирование формы сделок во многом напоминает французское. Требования к соблюдению письменной формы также можно рассматривать в двух аспектах: *ad validatem* (п. 2 ст. 162 ГК РФ) и *ad probationem* (п. 1 ст. 162 ГК РФ). В отечественном праве принцип недискриминации можно вывести из абзаца второго п. 1 ст. 160 ГК РФ, который приравнивает сделки, совершенные с помощью электронных или иных технических средств, к сделкам в письменной форме.

Принцип недискриминации должен распространяться как на случаи, когда несоблюдение формы сделки влечет ее недействительность, так и на ситуации, когда последствием такого несоблюдения является невозможность ссылаться на свидетельские показания.

Как и во французском праве, не каждая сделка может быть совершена в электронной форме с точки зрения *ad validatem*. ГК РФ приводит в качестве единственного такого примера недопустимость составления завещания с использованием электронных и иных технических средств под угрозой ничтожности (абзацы второй, четвертый п. 1 ст. 1124 ГК РФ)[6].

Поскольку ГК РФ не знает других подобных исключений, принятый им подход представляется довольно либеральным в отличие, например, от французского права, содержащего намного больше примеров недопустимости совершения сделок в электронной форме, о чем говорилось ранее. Статья 9 Директивы ЕС об электронной торговле позволяет национальным правопорядкам запрещать совершение в электронной форме куда большего количества сделок. Подобная «дискриминация» допустима в отношении:

- договоров, направленных на возникновение или передачу прав на недвижимость, за исключением права аренды;
- договоров, требующих при заключении привлечения суда, органов власти или иных лиц, осуществляющих публичные функции;
- обеспечительных сделок, по которым обязанным лицом является потребитель;
- договоров, определяемых семейным или наследственным правом.

Причины для введения соответствующей оговорки были различными. Если первые два случая объяснялись невозможностью в краткосрочной перспективе перевести все публичные органы на электронный документооборот, то последние две категории включены из-за невозможности предсказать, как электронная форма таких сделок отразится на внутреннем рынке (Lodder, 2017, p. 25).

Следует выразить надежду, что российский правопорядок не пойдет по пути расширения количества сделок, которые не могут быть совершены в электронной форме. Электронный документооборот при правильно настроенных параметрах способен гарантировать такую же степень защищенности и достоверности, что и письменная форма.

Другим важнейшим принципом регулирования электронной формы сделок является принцип технологической нейтральности (*principle of technological neutrality*)[7]. В соответствии с Типовым законом ЮНСИТРАЛ он предполагает, что внутреннее законодательство не может исходить из признания юридической силы исключительно тех документов, которые сформированы и направлены с использованием определенных способов, технологий и электронных носителей (Sorieul et al., 2001). В самом деле, с учетом динамики в развитии технологий представляется как минимум нецелесообразным нормативно определять в рамках регулирования *ex ante* конкретные виды технологий, с помощью которых может быть соблюдена электронная

[6] Подход ГК РФ в этом вопросе встречает критику в доктрине (Gorina & Gerasimova, 2021).

[7] UNCITRAL. (2018). *UNCITRAL Model Law on Electronic Transferable Records*. United Nations. P. 23. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf

форма. Таким образом, в силу принципа технологической нейтральности недопустим дифференцированный подход к регулированию в зависимости от того, была ли сделка совершена с помощью электронной почты, мессенджеров, на веб-сайте или иным способом в рамках цифровой среды. Законодатель и правоприменитель не должны отдавать предпочтения одним технологиям в ущерб другим.

ГК РФ также придерживается принципа технологической нейтральности, используя при описании сделок в электронной форме такой признак, как совершение их «с помощью электронных либо иных технических средств», не конкретизируя при этом в императивном порядке, каких именно. Вместе с тем в судебной практике встречаются случаи, когда суды нарушают данный принцип на основании характеристик используемого технического средства. Так, в одном из дел суд указал, что «переписка из мессенджера *Telegram* не является надлежащим доказательством оформления правоотношений между сторонами в отсутствие какой-либо первичной бухгалтерской документации (актов приема-сдачи оказанных услуг), факта заключения договора»[8], не придав значение тому, что такая переписка сама по себе может свидетельствовать о заключении договора в электронной форме.

Наконец, значимым является принцип функциональной эквивалентности (*principle of functional equivalence*), позволяющий адаптировать существующие материально-правовые нормы к электронному документообороту[9]. Метод функциональной эквивалентности (*équivalents fonctionnels, functional-equivalent approach*) позволяет не фокусироваться на формальных различиях между материальными и электронными способами фиксации волеизъявления, а определить «функциональные качества» традиционных материальных носителей, характеризующих письменную форму, а затем проверить, сохраняются ли эти качества при совершении сделки в электронной форме и при каких условиях это происходит (Demoulin & Montero , 2002, p. 21).

Впервые функциональная методика оценки равнозначности была предложена ЮНСИТРАЛ и реализована в Типовом законе об электронной коммерции. Унификация электронной и письменной форм на основе функциональной равнозначности предполагала анализ тех отличительных черт, которые характеризуют традиционную письменной форму, и того, каким образом в электронной форме эти особенности могут быть сохранены. Важной предпосылкой для подобного анализа, является исходное допущение о том, что традиционные материальные носители отличаются от электронных (Guomin & Shengmian, 2018, p. 1542–1543).

Данная методология помогает не только законодателю, но и судьям адаптировать существующие материально-правовые нормы к сделкам, совершенным в электронной форме. Не секрет, что правила, представленные в гражданском законодательстве (о форме сделок, заключении договоров и т.д.), в момент принятия зачастую не предполагали их применения к сделкам, совершенным на цифровых носителях, так как при создании соответствующих положений никакого электронного документооборота не было и в помине. А потому перед законодателем и правоприменителями стоит задача определить, могут ли, и если да, то при каких условиях традиционные нормы применяться к сделкам, заключенным в электронной форме.

Необходимо подчеркнуть, что для судей адаптация правил в силу функциональной равнозначности похожа, но отличается от аналогии закона. В отличие от последней она может предполагать не перенос существующей нормы, а создание нового правила, отличающегося гипотезой

[8] Решение АС г. Санкт-Петербурга и Ленинградской области от 17 февраля 2022 г. по делу № А56-5688/2021.

[9] Guo Yu (2022). Functional Equivalence to a Piece of Paper: A comment on the UNCITRAL Model Law on Electronic Transferable Records. [White Paper]. Hors Serie. Vol. XXVI. P. 2. https://www.wgtn.ac.nz/law/research/publications/about-nzacl/publications/special-issues/hors-serie-volume-xxvi-2021/01-guo-yu-pdf

или диспозицией от действующей нормы, если того требует соблюдение функциональной равнозначности (Veerpalu, 2019, pp. 141–142).

Отмечается, что использование метода функциональной равнозначности позволяет решить несколько проблем: соединить традиционное регулирование и электронную коммерцию; упростить законодательство в области электронной коммерции; сохранить гибкость и согласованность регулирования с развитием технологий (Guomin & Shengmian, 2018, p. 1544). Продемонстрировать то, каким образом метод функциональной равнозначности был реализован на практике применительно к форме электронных сделок, позволит несколько примеров.

Так, одной из отличительных особенностей письменной формы является то, что она в отличие от устной формы позволяет запечатлеть и сохранить на будущее отраженную на материальном носителе информацию. Электронная форма может достигнуть такого же эффекта при условии, если она позволяет обеспечить доступность изложенных в ней сведений для последующего использования. Документ в электронной форме, который не фиксирует заложенную в нем информацию и не предполагает возможность ее последующего использования (например, для предоставления его в судебном разбирательстве), не может быть функционально равнозначным письменной форме. В связи с этим для достижения эквивалентности между письменной и электронной формами правопорядок должен предъявлять требование о воспроизводимости к документам на цифровых носителях (Guomin & Shengmian, 2018, p. 1542)[10]. В российском праве оно выражено в ст. 160 ГК РФ, в соответствии с которой электронные либо иные технические средства должны позволять «воспроизвести на материальном носителе в неизменном виде содержание сделки».

Помимо этого, письменная форма предполагает идентификацию лица, от которого исходит волеизъявление (например, подпись). Для достижения функциональной эквивалентности электронной формы также требуется обеспечить возможность достоверного определения автора юридически значимого действия. Это можно сделать разными способами. Например, ст. 8 Типового закона ЮНСИТРАЛ об электронной коммерции исходит из того, что если закон сопровождается требованием к проставлению подписи, необходимо, чтобы при составлении и отправлении электронного документа использовался метод, (a) позволяющий идентифицировать лицо и указывающий на одобрение им содержащейся в электронном документе информации и б) надежный, а также — в свете всех сопутствующих обстоятельств — пригодный для создания и передачи сообщения. Ст. 160 ГК РФ и ст. 1366 ФГК используют более лаконичную формулировку, указывая на то, что для идентификации может использоваться любой способ, позволяющий должным образом определить лицо, от которого исходит волеизъявление.

Во французской доктрине введение соответствующих требований к электронной форме объясняется тем, что электронные документы в большей степени подвержены фальсификации, которая с трудом поддается распознаванию, по сравнению с традиционными бумажными носителями, а потому составление электронного документа без дополнительных технических способов удостоверения личности автора и обеспечения неизменности документа не может подтверждать согласие лица, изъявившего волю, и достоверность документа (Terré et al., 2019, p. 1910).

В качестве предварительного вывода следует отметить, что вышеизложенные принципы регулирования электронной формы сделок (недискриминации, технологической нейтральности,

[10] См., например, ст. 6 Типового закона ЮНСТИРАЛ об электронной торговле (UNCITRAL. (1999). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998*. United Nations. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf), ст. 1366 ФГК.

функциональной равнозначности) должны иметь не только теоретическое, но и практическое значение. Их основная ценность состоит не в том, чтобы с их помощью ученые могли описать форму сделок, совершенных с помощью электронных и иных технических средств, а в том, чтобы ими руководствовались законодатель и правоприменитель. Нормы закона и решения судов, принятые с грубым нарушением указанных принципов, не могут быть признаны справедливыми и отвечающими международным стандартам.

2. Соотношение электронной и письменной формы сделок

В отечественной доктрине в основу классификации форм сделок положено в том числе деление на словесные и несловесные способы волеизъявления. При словесном способе волеизъявления, предполагающем совершение сделки в устной, простой письменной и нотариальной формах, «субъект, воспринимающий волю, может непосредственно судить о ее содержании». Для несловесных форм изъявления воли характерно, что содержание волеизъявления определяется косвенно, исходя из поведения субъекта его совершающего, а не из доносимых до контрагента и распознаваемых последним слов, символов и иных знаков. То, что электронная форма признается словесным способом оформления волеизъявления, в российской доктрине не ставится под сомнение (Tatarkina, 2012, p. 25-27).

Куда более интересным представляется вопрос о соотношении электронной и письменной форм сделок. В силу абзаца второго п. 1 ст. 160 ГК РФ письменная форма сделки ***считается соблюденной*** также в случае совершения лицом сделки с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание сделки. Использование законодателем такого речевого оборота, как «считается соблюденной», может свидетельствовать в равной степени как о признании электронной формы разновидностью письменного способа заключения договоров, так и об использовании приема фикции (Grin, 2019), в силу которого электронная форма, как самостоятельное явление, отличается от письменной формы и приравнена к ней исключительно из практических соображений.

В российском правовом дискурсе встречаются как сторонники признания электронного способа оформления волеизъявления новой формой сделок (Idrisov, 2020), так противники такого подхода, считающие электронную форму разновидностью письменной (Belov, 2021).

По мнению Л.Г. Ефимовой, электронная форма представляет собой новую форму волеизъявления, которая отличается от письменного способа ввиду тех особенностей, которые присущи сделкам, заключенным с использованием электронных или иных технических средств (Efimova, 2019). Следует подробнее остановиться на высказываемых в пользу такой позиции аргументах и оценить их.

Аргумент 1. Внешний вид электронного документа отличается от документа на традиционных материальных носителях. В частности, сделка в электронной форме совершается «не на человеческом, а на “компьютерном” языке» в виде информации, представленной компьютерным кодом, которая не может непосредственно без технической обработки восприниматься человеком (Efimova, 2019).

В самом деле, для электронных сделок характерно, что волеизъявление изначально формируется в цифровом формате и доставляется адресату и воспринимается им в таком же виде (Karapetov, 2020). Однако свидетельствует ли это о том, что электронная форма не удовлетворяет признакам письменного способа волеизъявления?

В отдельных национальных правопорядках при квалификации того или иного документа в качестве письменного фундаментальным является понятие письма. Так, во Франции письмом (*l'écrit*) признается документ, состоящий из последовательности букв, знаков, цифр, а также любых иных обозначений или символов, имеющих понятное значение, вне зависимости от носителей, на которых они представлены (ст. 1365 ФГК). Французский законодатель не закрепляет привязку к конкретным носителям (материальным или электронным), на которых может быть составлено письмо, а также языку и символам, которые в нем используются (компьютерный код такое же письмо, как и иероглифы на папирусе). Таким образом, во французском праве закреплена идея о том, что электронный документ не представляет собой явление *sui generis*, а считается составленным в письменной форме (Andreu & Thomassin, 2021, p. 670). Главное — письменный документ, представленный как на электронных, так и на материальных носителях, должен быть предназначен для передачи информации и понятен, чтобы он имел юридическое значение (Malaurie, Aynès & Stoffel-Munck, 2020, p. 320–321).

Равным образом в Великобритании письмо (*writing*) включает в себя набор текста, печатание, литографию, фотографию и другие способы представления или воспроизведения слов в видимой форме (Приложение 1 к Закону о толковании 1978). На основании указанного положения в доктрине утверждается, что акты, составленные и направленные с помощью электронной почты или созданные в рамках веб-сайта, удовлетворяют признакам письменной формы[11], что дало законодателю основания не регламентировать электронную форму в законе (Beale, 2016).

В то же время акты международной частноправовой унификации не содержат в себе единой позиции по указанному вопросу. Так, Принципы международных коммерческих договоров (Принципы УНИДРУА) (1994 г.) и Принципы европейского договорного права (*Principles of European Contract Law (PECL)*) признают электронную форму в качестве разновидности письменной. Модельные правила европейского частного права (*Draft Common Frame of Reference (DCFR)*) (I.–1:106), напротив, исходят из того, что письменная форма (*in writing*) означает наличие текста на бумажном или ином материальном носителе. В качестве родового понятия, объединяющего документы на материальных и электронных носителях, *DCFR* используют термин «текстовая форма» (*textual form*). Вместе с тем именно текстовая форма является отражением письменной в национальных кодификациях, выполняя ее функции при заключении большинства договоров и совершении иных сделок (Bar & Clive, 2009, p. 151–153).

В российском праве вопрос о письменном характере электронной формы считается спорным из-за отсутствия внятной регламентации и должного понимания признаков письменной формы. Так, Х.В. Идрисов, опираясь на Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — ФЗ об информации), который последовательно разводит письменную и электронную формы (ч. 3 ст. 17.1 ФЗ об информации), делает вывод о том, что электронная форма является самостоятельным явлением и не сводится к письменной форме (Idrisov, 2020). Довольно сомнительной представляется идея опираться на нормы Закона, который не имеет к регулированию формы сделок никакого отношения, поскольку сфера его применения довольно ограничена. Указанный Закон регламентирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий,

[11] Вместе с тем электронный обмен данными (*electronic data interchange*) не будет соответствовать признакам письменной формы, поскольку не предполагает видимого текста, удовлетворяющего определению письма, что, как представляется, нарушает принцип технологической нейтральности.

обеспечении защиты информации (ст. 1 ФЗ об информации). Вместо этого следует обратиться к систематическому толкованию норм ГК РФ и посмотреть, каким образом Кодекс смотрит на электронную форму в других своих статьях. Ответ мы найдем в п. 2 ст. 434 ГК РФ, в соответствии с которым «договор в письменной форме может быть заключен путем составления одного документа (в том числе электронного), подписанного сторонами, или обмена письмами, телеграммами, электронными документами либо иными данными». Таким образом, ГК РФ не проводит различий между договорами, заключенными на материальных и электронных носителях, признавая, что все они составлены в письменной форме. Именно с таких позиций и следует подходить к электронной форме сделок в целом, рассматривая ее в качестве разновидности письменного способа заключения.

Аргумент 2. Электронная форма существует не только в качестве электронного статического документа (файла), но и в качестве электронного динамического гипертекстового документа (компьютерной программы), к которому в виде гипертекстовых ссылок прилагаются любые пояснения, спецификации и иные источники информации, не являющиеся частью договора как документа (Efimova, 2021).

Данный аргумент представляется сомнительным. Дело в том, что волеизъявление лица, зафиксированное на материальном носителе, может непосредственно не содержать всех условий, а отсылать к иным документам. Например, ГК РФ прямо говорит о том, что договор может отсылать к примерным условиям (ст. 427), которые, формально не будучи частью договора как документа, тем не менее будут определять программу договорных отношений сторон[12]. Кроме того, отмечается, что электронный динамический документ самостоятельно реагирует на новые события, фиксирует и инициирует исполнение обязательств, предоставляет сторонам дополнительную информацию и выполняет иные действия (Efimova, 2021). Вместе с тем неясно, по каким причинам договор, который самостоятельно выполняет определенные действия, не изменяя изначальные договоренности сторон помимо их воли, не будет удовлетворять признакам письменной формы.

Аргумент 3. В отличие от письменной формы закон не требует обязательного применения подписи для электронной формы, а позволяет считать форму соблюденной, если возможно достоверно определить лицо, от которого исходит волеизъявление (абзац второй п. 1 ст. 160 ГК РФ) (Efimova, 2019; Efimova, 2021).

Данный аргумент представляется нерелевантным в связи с неточностью исходной предпосылки о том, что письменная форма непременно сопровождается обязательным проставлением подписи. Как указывает А.Г. Карапетов, сопровождение волеизъявления в письменной форме на материальных носителях подписью или ее аналогом требуется далеко не во всех случаях. Например, иногда документ доводится до всеобщего сведения, в частности, если публичное обещание награды опубликовано в газете, условия приобретения товара размещены на соответствующей вендинговой машине, предложение по заключению договора по поводу парковки автомобиля указано на паркомате. В подобных случаях договор заключается

[12] ВАС РФ толкует данную норму следующим образом: «Для определения условий договоров стороны могут воспользоваться примерными условиями (стандартной документацией), разработанными в том числе саморегулируемыми и иными некоммерческими организациями участников рынка для договоров соответствующего вида и опубликованными в печати (статья 427 ГК РФ). При этом стороны могут своим соглашением предусмотреть применение таких примерных условий (стандартной документации) к их отношениям по договору как в полном объеме, так и частично, в том числе по своему усмотрению изменить положения стандартной документации или договориться о неприменении отдельных ее положений» (п. 7 Постановления Пленума ВАС РФ от 14 марта 2014 г. № 16 «О свободе договора и ее пределах»).

в отсутствие какой-либо подписи, но письменная форма все равно будет считаться соблюденной, если возможно определить авторство лица, совершившего волеизъявление (Karapetov, 2020, p. 852)[13]. Исходя из этого, можно сделать вывод, что наличие подписи не является необходимым атрибутом письменной формы и не свидетельствует о ее отличии от электронной формы.

Таким образом, высказываемые в литературе аргументы в пользу признания электронной формы самостоятельной разновидностью формы сделок являются неубедительными. Практическая ценность такого подхода также довольно сомнительна. Следует признать, что электронная форма сделок является разновидностью письменного способа заключения договоров.

3. Способы определения лица, совершившего волеизъявление

Основной вопрос, который возникает в связи с идентификацией автора сделанного в электронной форме волеизъявления, заключается в том, при каких способах подтверждения личности правопорядок признает соблюдение требования к форме. В российском праве данный вопрос в первую очередь сводится к тому, будет ли документ в электронной форме равнозначен документу на материальных носителях, если он не сопровождается квалифицированной электронной подписью (далее — ЭЦП).

Как известно, российское законодательство признает три вида ЭЦП:

1) простая ЭЦП — электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом (ч. 2 ст. 5 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее — ФЗ об ЭЦП)). Примером простой ЭЦП может быть совершение действий из личного кабинета пользователя веб-сайта, доступ к которому обеспечивается полученными при регистрации логином и паролем, или *SMS*-код, подтверждающий совершение юридически значимого действия (Karapetov, 2018, p. 242);

2) неквалифицированная ЭЦП — электронная подпись, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяет определить лицо, подписавшее электронный документ, позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания и создается с использованием средств электронной подписи (ч. 3 ст. 5 ФЗ об ЭЦП);

3) квалифицированная ЭЦП — электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам: ключ проверки электронной подписи указан в квалифицированном сертификате; для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в ФЗ об ЭЦП (ч. 4 ст. 5 ФЗ об ЭЦП).

При этом в соответствии с ФЗ об ЭЦП электронные документы будут иметь различное материально-правовое и процессуальное значение в зависимости от вида ЭЦП, которым они подписаны. Так, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, будет только электронный документ, подписанный квалифицированной ЭЦП

[13] ВС РФ в п. 9 Постановления Пленума ВС РФ от 25 декабря 2018 г. № 49 указал, что «при заключении договора путем обмена документами для целей признания предложения офертой не требуется наличия подписи оферента, если обстоятельства, в которых сделана оферта, позволяют достоверно установить направившее ее лицо (пункт 2 статьи 434 ГК РФ)».

(ч. 1 ст. 7 ФЗ об ЭЦП). В то же время электронный документ, подписанный простой и неквалифицированной ЭЦП, будет признаваться равнозначным бумажному документу, подписанному собственноручной подписью, ***только в случаях***, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами (далее — НПА), нормативными актами ЦБ РФ или соглашением между участниками электронного взаимодействия (ч. 2 ст. 6 ФЗ об ЭЦП).

Абзац второй п. 1 ст. 160 ГК РФ, напротив, не предусматривает требования к квалифицированной ЭЦП, а исходит из того, что письменная форма сделки считается соблюденной в случае ее совершения лицом с помощью электронных либо иных технических средств, если использован ***любой способ, позволяющий достоверно определить лицо, выразившее волю***. В доктрине встречается мнение, что решение, изложенное в абзаце втором п. 1 ст. 160 ГК РФ, свидетельствует о намерении законодателя либерализовать требования к совершению электронных сделок (Avtonova et al., 2019).

Таким образом, в то время как ГК РФ исходит из признания эквивалентности сделкам на материальных носителях сделок, заключенных в электронной форме, при условии что возможно достоверно установить лицо, изъявившее волю, ФЗ об ЭЦП для подавляющего большинства случаев признает такую равнозначность, только если электронный документ подписан квалифицированной ЭЦП.

Нельзя не отметить, что масло в огонь подливает и сам ГК РФ в последнем предложении абзаца второго п. 1 ст. 160, в соответствии с которым законом, иными правовыми актами и соглашением сторон может быть предусмотрен специальный способ достоверного определения лица, выразившего волю. Если толковать указанное положение буквально, то получается, что ФЗ об ЭЦП как раз и является таким законом, который устанавливает специальный способ достоверного определения лица путем использования квалифицированной ЭЦП для всех гражданско-правовых сделок. Однако подобное толкование явно ошибочно и требует телеологической редукции. Действительно, закон и иные НПА могут устанавливать специальные способы достоверного определения лица, совершающего сделку, но в строго ограниченных случаях, а не посредством генеральной оговорки о применении к любым сделкам[14]. Никакого унифицированного требования и единого решения в этом вопросе быть не может, о чем будет сказано далее.

Обратимся к судебной практике. В системе арбитражных судов еще не сформирована однозначная позиция по указанному вопросу. В соответствии с наиболее консервативной позицией равнозначным документу на бумажном носителе будет только электронный документ, подписанный квалифицированной ЭЦП[15].

Встречается и довольно демократичный подход к идентификации личности лица, изъявившего волю. В силу п. 3 постановления Пленума ВАС РФ от 23 марта 2012 г. № 14 «Об отдельных вопросах практики разрешения споров, связанных с оспариванием банковских гарантий» требования ст. 368 ГК РФ о письменной форме банковской гарантии считаются соблюденными,

[14] Такое толкование встречает поддержку в судебной практике: «Электронный документ должен быть подписан электронной цифровой подписью **только в прямо** предусмотренных законом или соглашением сторон случаях» (постановление АСМО от 23 мая 2022 г. № Ф05-8352/2022 по делу № А40-159015/2021).

[15] «При этом в силу ч. 1 ст. 6 Закона об ЭП независимо от дополнительных указаний законов и соглашения сторон такая равнозначность установлена только для электронных документов, подписанных квалифицированной электронной подписью» (постановление 9 ААС от 16 ноября 2020 г. № 09АП-53492/2020 по делу № А40-118166/2019).

к примеру, когда гарантия выдана в форме электронного сообщения с использованием телекоммуникационной системы *SWIFT* (СВИФТ), т.е. без использования квалифицированной ЭЦП (Avtonova et al., 2019).

Решения нижестоящих судов также подкидывают несколько любопытных правовых позиций, демонстрирующих приверженность некоторых судов либеральному подходу к идентификации личности. Так, в ряде дел предметом рассмотрения выступало требование по уплате денежных средств по банковской гарантии, которое было направлено по электронной почте, но не было подписано электронной подписью. Суды квалифицировали такое требование в качестве односторонней сделки, указав, что ФЗ об электронной подписи не предусматривает подписание ЭЦП в качестве обязательного условия признания документа электронным. Только в прямо предусмотренных законом или соглашением сторон случаях электронный документ должен быть подписан ЭЦП. В случае, если законом или соглашением сторон для конкретного случая не предусмотрено необходимости подписания электронного документа ЭЦП, он считается надлежащим и в случае отсутствия такой подписи[16].

В практике арбитражных судов можно встретить и компромиссный вариант решения указанной проблемы. Так, некоторые суды признают, что «по общему правилу документы между коммерческими организациями должны быть подписаны с двух сторон квалифицированными электронными подписями и иметь ключи проверки к ним»[17]. Использование фразы «по общему правилу» свидетельствует о том, что идентификация личности лица, изъявившего волю, может осуществляться и иным образом. Так, например, в одном из дел суд указал, что «неквалифицированная электронная подпись позволяет достоверно определить лицо, подписавшее электронный документ»[18], признав требование к форме соблюденным даже в отсутствие договоренности сторон или указания закона на допустимость использования данного способа согласия с содержанием сделки.

В то же время в судах общей юрисдикции практически повсеместно доминирует архаичный подход, признающий юридическую силу исключительно за электронными документами, подписанными усиленной квалифицированной подписью (если иное не предусмотрено НПА или соглашением сторон), который сводится к следующему:

а) отсутствие НПА, из которых следует признание равной юридической силы электронных документов, подписанных простой или неквалифицированной электронной подписью, и документов на бумажных носителях, подписанных собственноручной подписью, предполагает, что равная юридическая сила договоров в электронной форме и договоров, составленных на материальных носителях, может быть основана исключительно на ранее заключенных между сторонами рамочных договорах, которые допускают подобный порядок заключения последующих договоров с применением простой или неквалифицированной электронной подписи;

---

[16] Постановления 9 ААС от 13 января 2022 г. № 09АП-82222/2021-ГК, 09АП-85536/2021-ГК по делу № А40-159015/2021; АСМО от 23 мая 2022 г. № Ф05-8352/2022 по делу № А40-159015/2021; 13 ААС от 21 ноября 2022 г. № 13АП-30729/2022 по делу № А56-57238/2022.

[17] См., например, постановления 9 ААС от 14 августа 2023 г. № 09АП-34471/2023-ГК по делу № А40-26669/2023; 15 ААС от 9 марта 2023 г. № 15АП-165/2023 по делу № А53-22292/2022; решения АСГМ от 15 августа 2023 г. по делу № А40-29353/23–65–338; АС Забайкальского края от 24 марта 2023 г. по делу № А78-15637/2022.

[18] Постановления 8 ААС от 4 августа 2022 г. № 08АП-7315/2022 по делу № А70-80/2022; 9 ААС от 22 апреля 2022 г. № 09АП-20340/2022 по делу № А40-190043/2021; 11 ААС от 24 августа 2022 г. № 11АП-11254/2022 по делу № А55-83/2022.

б) такие рамочные договоры должны быть составлены на бумажном носителе и собственноручно подписаны сторонами[19].

Противоречивость судебной практики ставит задачу по поиску оптимального решения названной проблемы. Обратимся к зарубежному опыту. А.И. Савельев указывает на то, что современные акты европейского законодательства, например *DCFR* (Bar & Clive, 2009, p. 151), дифференцированно подходят к вопросам регламентации формы и подписи (Savel'ev, 2013). Равным образом в Типовом законе ЮНСИТРАЛ об электронной коммерции не содержится никаких указаний относительно того, каким образом может быть создана электронная подпись, чтобы идентифицировать лицо, изъявившее волю (Ilobinso, 2016, p. 67). Отмечается, что функция собственноручной подписи будет выполняться с помощью любых способов, позволяющих идентифицировать автора документа и подтвердить, что он одобрил его содержание[20].

Во Франции подпись рассматривается не как формальность, а как функция, позволяющая идентифицировать автора юридически значимого действия. В этой связи суды признавали подписью различные средства, позволяющие с достоверностью определить личность автора и подтверждающие его согласие с содержанием документа. ЭЦП, предусматривающая наличие сертификата, не является обязательной при совершении сделок, ее использование лишь создает презумпцию достоверности совершенного волеизъявления и личности лица, изъявившего волю. Идентификация может осуществляться и иными способами (Andreu & Thomassin, 2021, p. 671).

В Великобритании согласие лица, выразившего волю в электронной форме, определяется на основании того, можно ли с точки зрения разумного субъекта утверждать, что его поведение свидетельствует о намерении совершить сделку. Отмечается, что идентификация лица может быть осуществлена с помощью: электронной подписи с системой шифрования с двойным ключом; рукописной подписи, отсканированной на компьютере и включенной в электронное письмо или другой документ; проставления ФИО (инициалов)[21]; установки программы, посредством которой идентификация производится автоматически; согласия, выраженного нажатием кнопки на веб-сайте о принятии условий сделки; подтверждения оплаты или предоставления личных данных (Beale, 2016, § 5-028).

Представляется, что российское право должно придерживаться аналогичного подхода, в соответствии с которым требование к форме сделки может быть соблюдено при отсутствии квалифицированной ЭЦП лица, изъявившего волю. Функцию идентификации, помимо ЭЦП, могут выполнять любые иные способы, позволяющие достоверно определить лицо, выразившее волю (абзац второй ч. 1 ст. 160 ГК РФ) (Kozlovskaya, 2018). Квалифицированная ЭЦП должна

---

[19] Подобная практика широко представлена практически во всех кассационных судах общей юрисдикции (см.: определения Первого кассационного суда общей юрисдикции от 12 декабря 2022 г. № 88-34059/2022; Второго кассационного суда общей юрисдикции от 12 июля 2021 г. № 88-14927/2021, от 22 ноября 2022 г. № 88-24148/2022; Третьего кассационного суда общей юрисдикции от 17 марта 2020 г. № 88-4104/2020; Четвертого кассационного суда общей юрисдикции от 30 ноября 2022 г. по делу № 88-36535/2022; Шестого кассационного суда общей юрисдикции от 30 марта 2022 г. № 88-7175/2022; Седьмого кассационного суда общей юрисдикции от 24 декабря 2020 г. № 88-18972/2020; Восьмого кассационного суда общей юрисдикции от 30 июня 2023 г. № 88-13339/2023 по делу № 2-1-214/2023, № 88-13338/2023 по делу № 2-1-212/2023).

[20] UNCITRAL. (1999). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998*. United Nations. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf

[21] В США также указание в электронном письме имени отправителя будет выполнять функцию его идентификации (подписи) и согласия с условиями сделки (Wang, 2014, p. 135–136).

признаваться одним из возможных, но не единственным способом определения автора юридически значимого действия.

В обоснование указанной позиции можно привести как политико-правовые, так и догматические аргументы. Безусловно, квалифицированная ЭЦП позволяет наиболее достоверно определить лицо, совершившее волеизъявление, минимизировать риск заключения договора неуполномоченным лицом от чужого имени. Это обстоятельство имеет значение на этапе судебного разбирательства: подобный способ идентификации позволяет сократить литигационные издержки. Для формирования суждения о личности совершившего волеизъявление лица суду достаточно удостоверится в наличии квалифицированной ЭЦП и не исследовать иные обстоятельства, если на то нет особых причин (например, заявления о фальсификации или о получении третьим лицом несанкционированного доступа к ЭЦП). Однако далеко не каждая сделка в электронной форме сопровождается судебным спором, и даже если такой спор возникает, то вопрос об определении личности лица, совершившего сделку, ставится не всегда. Подавляющее большинство сделок заключаются и исполняются, не приводя к возникновению судебных разбирательств (Karapetov & Savel'ev, 2012, p. 447). В этой связи аргумент о минимизации судебных издержек не может быть основным. Более оправданно обратиться к тому, как квалифицированная ЭЦП влияет на обычный хозяйственный оборот. Ведь ее получение связано с материальными и временны́ми затратами и представляется нерациональным как минимум при оформлении сделок на незначительную сумму или сделок, совершенных потребителями. Так, во Франции на практике электронные сделки, сопровождающиеся квалифицированной ЭЦП, практически не встречается (Andreu & Thomassin, 2021, p. 673).

Помимо этого, нельзя не отметить, что возможности использования квалифицированной ЭЦП довольно ограничены. Например, при совершении сделок путем переписки в мессенджерах или посредством направления *SMS* сложно представить, каким образом может быть применена квалифицированная ЭЦП. С политико-правовой точки зрения возможность идентификации лица иным образом способствует снижению трансакционных издержек и временных затрат на оформление и заключение договоров, что в итоге отражается на увеличении количества сделок в цифровой среде и росте общественного благосостояния.

Догматическим аргументом в защиту изложенной позиции может служить обоснование приоритета действия абзаца второго п. 1 ст. 160 ГК РФ через принципы *lex specialis derogat generali* и *lex posterior derogat priori*. В силу ст. 1 ФЗ об ЭЦП указанный Федеральный закон регулирует отношения в области использования электронных подписей «при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий». Таким образом, сфера регулирования ФЗ об ЭЦП не ограничивается гражданско-правовым сделками, а распространяется и на иные области права, в то время как абзац второй п. 1 ст. 160 ГК РФ посвящен исключительно форме гражданско-правовой сделки и потому носит специальный по отношению к ФЗ об ЭЦП характер. Помимо этого, правило, изложенное в абз. 2 п. 1 ст. 160 ГК РФ, было введено в 2019 г.[22], в то время как нормы ФЗ об ЭЦП о соотношении документов в письменной форме на бумажных и электронных носителях — в 2011 г. Правила, установленные в ГК РФ, имеют приоритет перед ст. 6 ФЗ об ЭЦП.

Таким образом, если электронный документ позволяет достоверно определить лицо, от которого исходит волеизъявление, несмотря на отсутствие квалифицированной ЭЦП, требование

[22] Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // СЗ РФ. 2019. № 12. Ст. 1224.

к форме должно считаться выполненным[23]. Безусловно, в отношении отдельных сделок закон может вводить повышенные требования для идентификации автора волеизъявления (абзацы второй, четвертый п. 1 ст. 160 ГК РФ) в том числе посредством необходимости использования квалифицированной ЭЦП[24].

Следует сразу оговориться, что единого способа достоверного определения лица, совершившего сделку, не существует. Это зависит от множества различных факторов, в первую очередь от способа совершения сделки.

Основной массив сделок в электронной форме совершается путем переписки и обмена документами с помощью электронной почты[25], *SMS*, мессенджеров[26], веб-сайтов и мобильных приложений[27]. Это предопределяет необходимость более детально рассмотреть подходы, выработанные судебной практикой, к идентификации лица, совершающего сделку.

1. Суды требуют, чтобы при заключении договора посредством электронной почты имелась возможность достоверно определить стороны, а также их адреса электронной почты[28]. В судебной практике принадлежность электронной почты лицу, совершившему волеизъявление, констатируется, если:

- ранее заключенный договор (например, рамочный) содержит электронный адрес лица, совершившего волеизъявление[29];
- осуществлен обмен отсканированными документами, на которых проставлена собственноручная подпись и печать[30];
- ранее сторона, отрицающая факт совершения сделки, в отношениях с другими субъектами указывала аналогичные идентифицирующие ее сведения[31];

---

23 Указанная позиция встречает поддержку в отечественной доктрине (см.: Karapetov, 2020, p. 857; Kozlovskaya, 2018).

24 См., например, ч. 3–5 ст. 51 Федерального закона от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // СЗ РФ. 2013. № 14. Ст. 1652.

25 Постановления АС Московского округа от 29 марта 2022 г. № Ф05-3486/2022 по делу № А40-110161/2021; АС Северо-Западного округа от 6 декабря 2022 г. № Ф07-19231/2022 по делу № А13-17046/2021; АС Центрального округа от 15 декабря 2021 г. № Ф10-6102/2021 по делу № А14-15192/2019. Довольно знаковым для формирования судебной практики стало Постановление Президиума ВАС РФ от 12 ноября 2013 г. № 18002/12 по делу № А47-7950/2011, в котором сформирована следующая позиция: «...получение или отправка сообщения с использованием адреса электронной почты, известного как почта самого лица или служебная почта его компетентного сотрудника, свидетельствует о совершении этих действий самим лицом, пока им не доказано обратное».

26 Постановления АС Центрального округа от 20 июля 2020 г. № Ф10-1241/2020 по делу № А68-4/2019; 4 ААС от 10 апреля 2023 г. № 04АП-650/2023 по делу № А58-5856/2022.

27 Определения Первого кассационного суда общей юрисдикции от 17 мая 2023 г. № 88-12753/2023; Второго кассационного суда общей юрисдикции от 4 июля 2023 г. по делу № 88-16733/2023.

28 Постановления ФАС Северо-Кавказского округа от 31 августа 2011 г. по делу № А53-20977/2010; АС Западно-Сибирского округа от 22 июня 2022 г. № Ф04-3110/2022 по делу № А67-9105/2020; 7 ААС от 2 декабря 2021 г. № 07АП-9447/2021 по делу № А45-774/2021.

29 Постановление АС Восточно-Сибирского округа от 21 января 2022 г. № Ф02-6854/2021 по делу № А19-19914/2020.

30 Определение Судебной коллегии по гражданским делам ВС РФ от 19 сентября 2017 г. № 78-КГ17-56; постановления АС Дальневосточного округа от 4 июня 2020 г. № Ф03-2030/2020 по делу № А24-5005/2019; АС Центрального округа от 6 марта 2023 г. № Ф10-31/2023 по делу № А14-19747/2019.

31 Согласно фабуле одного из дел, ответчик направил на электронный адрес истца гарантийное письмо с заверением о намерении произвести расчет за полученный товар не позднее определенного срока. Суд принял во внимание, что ответчик участвовал в электронных торгах на различных торговых площадках с иными субъектами и указывал все реквизиты, полностью совпадающие с теми, что были высланы в адрес истца, вплоть до номера телефона и адреса электронной почты (см. постановление АС Московского округа от 3 июня 2022 г. № Ф05-11153/2022 по делу № А40-213916/2021).

- электронный адрес содержит в себе официальный домен лица, совершившего волеизъявление[32];
- на официальном веб-сайте лица размещен адрес электронной почты[33];
- адрес электронной почты указан в Едином государственном реестре юридических лиц[34].

2. Необходимость достоверного определения личности существует и при совершении сделок посредством мессенджеров и *SMS*[35]. Основным способом является установление принадлежности лицу номера телефона, к которому привязан мессенджер[36] или с которого было отправлено *SMS* (например, на основании запросов у сотовых операторов[37] или предоставления доказательств размещения номера телефона на официальном веб-сайте[38]).

3. Наконец, требуемая идентификация личности при совершении сделок на веб-сайтах или в мобильных приложениях достигается за счет: дополнительной проверки путем отправки сообщения по принадлежащему лицу номеру телефона[39]; использования личного кабинета, доступ к которому осуществляется посредством авторизованных данных (логина и пароля)[40]; указания персональных данных (ФИО, даты рождения, места работы и должности, номера телефона и адреса электронной почты) и регистрации на веб-сайте[41]; *IP*-адреса, который ранее использовался лицом[42].

Помимо указанных способов, требование о надлежащей идентификации лица будет выполнено, если им совершены конклюдентные действия по исполнению условий оферты (например, произведена оплата, выставлены счета, начата отгрузка товара или выполнение работ и т.д.)[43]. В этих случаях суды руководствуются п. 3 ст. 434 ГК РФ, в соответствии с которым письменная форма считается соблюденной, если совершен акцепт конклюдентными

---

32 Постановления АС Московского округа от 17 февраля 2021 г. № Ф05-20389/2020 по делу № А40-121264/2019; АС Уральского округа от 9 июня 2023 г. № Ф09-3363/23 по делу № А76-38949/2021.

33 Постановление АС Московского округа от 15 июля 2021 г. № Ф05-15967/2021 по делу № А40-112851/2020.

34 Постановление АС Московского округа от 18 июня 2020 г. № Ф05-8086/2020 по делу № А40-87487/2018.

35 «Направление письма с электронной почты не позволяет достоверно установить отправителя и получателя писем, наличие и объем их полномочий на совершение юридически значимых действий. Аналогичная позиция применяется и при переписке по телефону. Принадлежность телефонных номеров конкретным лицам, их отношения к ответчику, объем полномочий истцом не доказаны. Переписка в специальных телефонных программах, равно как и по электронной почте[,] не позволяет достоверно установить ни отправителя, ни получателя сообщения» (постановления 9 ААС от 22 мая 2023 г. № 09АП-21979/2023 по делу № А40-168452/2022, от 16 января 2023 г. № 09АП-86800/2022 по делу № А40-156167/2022).

36 Постановление АС Московского округа от 18 июня 2020 г. № Ф05-8086/2020 по делу № А40-87487/2018.

37 Постановления 9 ААС от 21 июня 2022 г. № 09АП-36975/2022 по делу № А40-103116/2021; 16 ААС от 28 апреля 2022 г. № 16АП-248/2022 по делу № А63-6538/2021; 19 ААС от 21 марта 2022 г. № 19АП-643/2022 по делу № А14-20655/2019.

38 Постановление АС Поволжского округа от 27 октября 2021 г. № Ф06-8969/2021 по делу № А65-21924/2020.

39 Постановление АС Центрального округа от 6 марта 2023 г. № Ф10-31/2023 по делу № А14-19747/2019; определение Шестого кассационного суда общей юрисдикции от 22 июня 2022 г. № 88–12587/2022.

40 Постановление 13 ААС от 2 июня 2023 г. № 13АП-10631/2023 по делу № А56-90353/2022.

41 «Заключение пользовательского соглашения и дача согласия на обработку персональных данных названным путем посредством регистрации на сайте пользователя, которого можно однозначно идентифицировать ввиду указания определенных персональных данных и который должен и имеет реальную возможность ознакомиться с текстом пользовательского соглашения, не противоречит [ст. 438 ГК РФ]» (постановление АС Волго-Вятского округа от 18 ноября 2020 г. № Ф01-13471/2020 по делу № А43-3858/2020).

42 Постановление АСМО от 1 марта 2023 г. № Ф05-46/2023 по делу № А40-31607/2022.

43 Подробнее об акцепте действием см.: Savkunova, 2016.

действиями[44]. В практике можно встретить довольно много примеров, когда суды констатируют заключенность договора и соблюдение требования к электронной форме, если совершаются действия по исполнению[45]. Однако важно помнить, что совершение действий по исполнению не всегда означает его заключение. Возможна и иная ситуация — когда договор в электронной форме заключен иным образом (например, посредством обмена электронными документами) и во исполнение уже заключенного договора производятся определенные действия. Необходимо отметить существующую разницу, которая имеет критическое значение, когда речь идет, например, об ограничении договора определенным сроком, который привязан к моменту заключения договора, или об изменении законодательства, устанавливающего для сторон иные правила (п. 2 ст. 422 ГК РФ).

Безусловно, упомянутые способы определения автора волеизъявления не являются исчерпывающими. Открытый характер абзаца второго п. 1 ст. 160 ГК РФ создает возможность для использования иных методов. Более продуктивной представляется выработка критериев, на основании которых можно было бы судить об их достаточности или, напротив, недостаточности.

Прекрасный пример таких критериев, которые могут быть взяты на вооружение российскими судами, представлен в комментарии к Типовому закону ЮНСИТРАЛ об электронной коммерции. Так, оценка достоверности методов идентификации лица, изъявившего волю, должна предполагать анализ различных юридических, технических и коммерческих факторов, среди которых выделяются, в частности, оценка характера деятельности участников сделки, интенсивность коммерческой деятельности между сторонами, вид и размер сделки, существование определенных обычаев делового оборота или практики в соответствующей области, которая предполагает использование определенных способов идентификации, наличие альтернативных способов идентификации и затраты на их использование и т.д.[46]

Подобный перечень факторов не может быть исчерпывающим. Во внимание должны приниматься любые обстоятельства, продиктованные необходимостью защиты определенных политико-правовых ценностей (например, справедливости, экономической эффективности) и обеспечивающие необходимый баланс интересов участников оборота.

4. Требование воспроизводимости содержания электронной сделки на материальном носителе

Одним из условий, при которых электронная форма приравнивается к письменной, является возможность воспроизведения на материальном носителе в неизменном виде содержания сделки (абзац второй п. 1 ст. 160 ГК РФ).

[44] «Таким образом, закон предусматривает три способа соблюдения письменной формы договора (как в документарном, ***так и бездокументарном, то есть электронном виде***): составление одного подписанного сторонами документа, обмен письменными волеизъявлениями и акцепт оферты на заключение договора путем совершения акцептантом конклюдентных действиями» (постановления АС Западно-Сибирского округа от 29 июня 2023 г. № Ф04-2552/2023 по делу № А70-18141/2022; АС Западно-Сибирского округа от 15 августа 2023 г. № Ф04-3439/2023 по делу № А70-12294/2022).

[45] См., например: постановления АС Северо-Западного округа от 31 мая 2023 г. № Ф07-2435/2023 по делу № А05-3443/2022; АС Волго-Вятского округа от 26 октября 2021 г. № Ф01-5690/2021 по делу № А43-12627/2020.

[46] UNCITRAL. (1999). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998*. United Nations. P. 39. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf

В судебной практике встречаются дела, в которых в качестве аргумента о несоблюдении требования к форме выдвигается невозможность воспроизведения содержания электронной сделки на материальном носителе. Так, в одном из споров истец договорился в мессенджерах «ДомКлик» и *Viber* с ответчиками о продаже квартиры. Суд, отказывая в удовлетворении исковых требований, указал, что представленные доказательства не позволяют воспроизвести на материальном носителе содержание договора в неизменном виде (в частности, при распечатывании)[47]. В другом деле, где суд также указал на такую невозможность, речь шла о внесении изменений в договор потребительского кредита с использованием системы «Сбербанк Онлайн»[48]. Аналогичный подход можно встретить в деле, в котором стороны заключили договор займа в мессенджере *WhatsApp*[49].

Следует отметить, что в судебной практике аргумент о невоспроизводимости содержания сделки на материальном носителе на сегодняшний день носит единичный характер, составляя, скорее, статистическую погрешность. Однако это никоим образом не отменяет значимости этого признака электронной формы.

А.И. Савельев выделяет два возможных подхода к пониманию критерия воспроизводимости сделки на материальном носителе. Первый вариант, вдохновленный *DCFR* и некоторыми директивами ЕС, состоит в «сохранении информации таким образом, чтобы она была доступна для ознакомления в будущем в течение достаточного времени при обеспечении возможности ее воспроизведения в неизменном виде» (Savel'ev, 2020, p. 272–273). Второй вариант сводится к тому, что воспроизводимость сделки на материальном носителе будет обеспечена только за счет применения средств криптографии путем использования квалифицированной ЭЦП (Savel'ev, 2020, p. 273). О недостатках возведения квалифицированной ЭЦП в ранг единственно возможного способа, обеспечивающего соблюдение требований к форме, уже сказано, а потому, соглашаясь с А.И. Савельевым в том, что подобный подход существенно сужает возможности совершения электронных сделок (Savel'ev, 2020, p. 273), следует отвергнуть такой вариант толкования.

Остановимся на первом варианте, который, как уже было сказано, опирается на текст *DCFR* и отдельные директивы ЕС. Так, ст. I.–1:106 *DCFR* использует термин «надежный носитель» (*durable medium*), который базируется на двух элементах: надежности и неизменяемости отправителем содержащейся на нем информации. К таким носителям относятся дискеты, *CD*, *DVD*, жесткие диски персональных компьютеров[50] или серверы, на которых размещается электронная почта. В то же время веб-сайт по общему правилу не признается надежным носителем, за исключением случаев, когда он позволяет хранить на нем в течение достаточно длительного времени информацию, которая не может быть изменена лицом, разместившим ее (Poyton, 2004, p. 153). Необходимым условием также является обеспечение постоянного доступа адресата информации на надежном носителе. Например, речь может идти об отправке адресату документа на *DVD* или на электронную почту, к которой он имеет доступ (Bar & Clive, 2009, p. 153).

[47] Апелляционное определение Нижегородского областного суда от 30 ноября 2021 г. № 33-13813/2021, 2-4428/2021.

[48] Решение Верхнесалдинского районного суда Свердловской области от 25 июня 2021 г. № 2-241/2021~М-37/2021.

[49] Решение Облученского районного суда Еврейской автономной области от 30 марта 2021 г. по делу № 2-126/2021.

[50] Любопытная позиция встречается в практике английский судов, в соответствии с которой при рассмотрении некоторых дел жесткий диск или компьютер в целом были приравнены к документу (*Kent Pharmaceuticals Limited v. Director of Serious Fraud Offences and Others*, (2002) EWHC 3023; *R v. Misic*, (2001) 3 NZLR 1; *R(H) v. Commissioners of Inland Revenue*, (2002) EWHC 2164). Безусловно, такой подход ошибочен. Сам по себе жесткий диск или компьютер не являются документами, а служат источниками накопления и хранения информации. Документами могут быть лишь сохраненные на них файлы, в которых отражена соответствующая информация.

Абзац второй п. 1 ст. 160 ГК РФ явно нацелен на такое понимание требования о воспроизводимости «на материальном носителе в неизменном виде содержания сделки». Тем не менее представляется, что принципы, сформулированные в *DCFR* в части определения надежного носителя, не могут быть безоговорочно применены к толкованию соответствующего правила ГК РФ. Дело в том, что требование к соблюдению электронной формы с возможностью воспроизведения на надежном носителе не является общим правилом *DCFR* и предусмотрено для довольно ограниченного числа случаев (например, при информировании потребителей (II.–3:106), доведении информации о праве на отказ от договора (II.–5:104), составлении гарантийного документа (IV.A.–6:103), оформлении договора дарения (IV.H.–2:101)) (Bar & Clive, 2009, p. 153). Общим же правилом достаточным для заключения договора посредством информационных технологий является составление документов в текстовом виде, позволяющем «прочитать, записать и воспроизвести на материальном носителе содержащуюся в тексте информацию» (I.-1:106 §2). В отличие от требований к воспроизводимости документов на надежном носителе, несмотря на всю с ним схожесть, текстовая форма не требует, чтобы информация была постоянно доступна. Вместо этого достаточно, чтобы информация (например, в виде текста на веб-сайте) была представлена таким образом, чтобы ее можно было скачать и записать (Bar & Clive, 2009, p. 152-153). Подобный подход позволит переложить на адресата информации неблагоприятные последствия в связи с его неосмотрительностью и расторопностью, если он не сохранил соответствующую информацию, а контрагент предоставил свой экземпляр договора. Лицу, изъявившему волю, достаточно будет доказать, что он принял все необходимые действия для того, чтобы его визави мог сохранить условия сделки в момент ее совершения.

Представляется, что такой подход более чем оправдан в качестве общего правила, которое, возможно, потребует некоторой телеологической редукции соответствующей нормы абзаца второго п. 1 ст. 160 ГК РФ. В условиях отсутствия неравенства переговорных возможностей его применение не вызывает серьезных опасений. Толкование, принятое в *DCFR* при определении надежного носителя, справедливо в отношениях с участием слабой стороны для ее защиты (например, в потребительских договорах) или при совершении сделок, в которых подлинность и содержание волеизъявления лица должны подвергаться более пристальному анализу (в сделках, носящих безвозмездный характер).

Заключение

В завершение хотелось бы изложить ряд основных выводов, сделанных в рамках данной статьи.

Во-первых, регулирование электронной формы сделок строится на принципах недискриминации, технологической нейтральности и функциональной эквивалентности. Указанные императивы должны иметь не только теоретическое, но и практическое значение. Их основная ценность состоит не в том, чтобы с их помощью ученые могли описать форму сделок, совершенных с помощью электронных и иных технических средств, а в том, чтобы ими руководствовались законодатель и правоприменитель. Нормы закона и решения судов, принятые с грубым нарушением указанных принципов, не могут быть признаны справедливыми и отвечающими международным стандартам.

Во-вторых, электронная форма сделок по своей природе является письменной. Подход, в соответствии с которым форма сделок, совершенных с помощью электронных средств, признается

самостоятельным способом их заключения, представляется несостоятельным и имеет довольно сомнительную практическую ценность.

В-третьих, при совершении сделок в электронной форме квалифицированная электронная цифровая подпись по общему правилу не является обязательной. Требование к форме считается соблюденным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю. При решении вопроса о том, позволяет ли в каждом конкретном случае используемый способ идентифицировать автора волеизъявления, должны приниматься во внимание разные юридические, технические и коммерческие факторы, например оценка характера деятельности участников сделки, интенсивность коммерческой деятельности между сторонами, вид и размер сделки, существование определенных обычаев делового оборота или практики в соответствующей области, которая предполагает использование определенных способов идентификации, наличие альтернативных способов идентификации и затраты на их использование и т.д.

Наконец, сделки в электронной форме по общему правилу должны совершаться таким образом, чтобы можно было прочитать, записать и воспроизвести на материальном носителе содержащуюся в них информацию. Повышенные требования к материальному носителю, который бы обеспечивал доступность информации в течение достаточно длительного времени и возможность ее воспроизведения в неизменном виде, могут предъявляться в отношениях с участием слабой стороны с целью ее защиты (например, в потребительских договорах) или при совершении сделок, в которых подлинность и содержание волеизъявления лица должны подвергаться более пристальному анализу (в сделках, носящих безвозмездный характер).

Данная статья не претендует на исчерпывающее изложение всех проблем, связанных с регулированием сделок, совершенных с использованием электронных или иных технических средств. Самостоятельного и более пристального анализа заслуживают такие аспекты, как использование ЭЦП, процессуальные вопросы доказывания соблюдения электронной формы и представления электронных документов в суде (Karapetov, 2020), вопросы фальсификации и вмешательства третьих лиц, приводящих к искажению электронных документов, а также заключение электронных договоров[51].

Список литературы / References

1. Andreu, L., & Thomassin, N. (2021). *Cours de droit des obligations* (19e éd.) [Law of obligations course (19th ed.)]. Gualino.
2. Avtonova, E.D., Astapenko, P.A., Borejsho, D.V., Do M. Yu., Mal'shakov, A.A., Mymrin, V.A., Nikulushkina, A.S., Papilin, I.I., Romanova, O.I., & Khodasevich, L.S. (2019). Kommentarij k Postanovleniyu Plenuma VS RF ot 25.12.2018 No. 49 "O nekotoryh voprosakh primeneniya obshchikh polozhenij Grazhdanskogo kodeksa Rossijskoj Federacii o zaklyuchenii i tolkovanii dogovora" [Comment on Resolution of the Plenum of the Supreme Court of the Russian Federation No. 49 Dated December 25, 2018 "On Some Issues of the Application of the General Provisions of the Civil Code of the Russian Federation on Contract Execution and Interpretation"]. *Vestnik ekonomicheskogo pravosudiya Rossijskoj Federacii [Herald of Economic Justice]*, *9*, 68–118.
3. Bar, C., & Clive, E.M. (Eds.). (2009). *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR)*. Sellier European Law Publishers.

[51] Отмечается, что заключение электронных договоров отличается рядом особенностей и вносит существенные коррективы в традиционный способ заключения договора посредством акцепта оферты (Malaurie, Aynès & Stoffel-Munck, 2020, p. 103).

4. Beale, H. (Ed.) (2016). *Chitty on Contracts. Vol. 1 (General principles)* (32nd ed.). Sweet & Maxwell.
5. Belov, V.A. (2021). Elektronnaya torgovlya: Ponyatie, pravovoe regulirovanie i sudebnaya praktika [E-commerce: Concept, Legal Regulation, and Judicial Practice]. *Vestnik arbitrazhnoj praktiki [Herald of Arbitrazh Practice]*, *4*, 11–20.
6. Bénabent, A. (2021). Droit des obligations (6e éd.) [Law of Obligations]. LGDJ.
7. Demoulin, M. & Montero, É. (Eds.). (2002). Le formalisme contractuel à l'heure du commerce électronique [Contractual Formalism in the Age of E-commerce]. In *La théorie générale des obligations, suite [The General Theory of Obligations, Continued]* (p. 99–181). Formation Permanente CUP.
8. Efimova, L.G. (2019). Eshche raz o ponyatii i pravovoj prirode elektronnoj formy sdelki [One More Time on the Concept and Legal Nature of the Electronic Form of the Transaction]. *Lex russica*, *8*, 129–137.
9. Efimova, L.G. (2021). Al'ternativnyj vzglyad na pravovoe regulirovanie grazhdansko-pravovyh otnoshenij v usloviyah cifrovoj ekonomiki [An alternative View of the Legal Regulation of Civil Law Relations in the Digital Economy]. *Aktual'nye problemy rossijskogo prava [Actual Problems of Russian Law]*, *8*, 52–62.
10. Grin', O.S. (2019). Transformacii trebovanij k forme dogovorov s uchetom razvitiya cifrovyh tekhnologij [Transformation of Contract Form Requirements Based on the Development of Digital Technologies]. *Aktual'nye problemy rossijskogo prava [Actual Problems of Russian Law]*, *6*, 49–57.
11. Gorina, N.V., & Gerasimova, N.N. (2021). *Elektronnoye zaveshchaniye — mif ili real'nost' [Electronic Will — Myth or Reality]. Notarius, 1*, 28–32.
12. Guomin, L. & Shengmian, Z. (2018). Functional-Equivalent Approach in UNCITRAL Electronic Commerce Legislation. In X. Xiao, H. Xue. (Eds.) *Proceedings of the 2018 2nd International Conference on Management, Education and Social Science (ICMESS 2018)* (p. 1542–1545). Atlantis Press. https://doi.org/10.2991/icmess-18.2018.338
13. Idrisov, H.V. (2020). Elektronnaya forma dogovora: Doktrina i pravovoe regulirovanie [Electronic Form of a Contract: The Doctrine and Legal Regulation]. *Rossijskij yuridicheskij zhurnal [Russian Law Journal]*, *3*, 107–113.
14. Ilobinso, I. (2016). Formation of Electronic Contracts: Melding the Traditional Contract Law with Contemporary Electronic Commerce. *Commercial and Industrial Law Review, 2*, 50–63.
15. Jansen, N. & Zimmermann, R. (2018). Commentaries on European Contract Laws. Oxford University Press.
16. Karapetov, A.G. (Ed.). (2018). *Sdelki, predstavitel'stvo, iskovaya davnost': postatejnyj kommentarij k stat'yam 153–208 Grazhdanskogo kodeksa Rossijskoj Federacii [Transactions, Agency, Limitation of Actions: Article-by-article Commentary to Articles 153–208 of the Civil Code of the Russian Federation].* M-Logos.
17. Karapetov, A.G. (Ed.). (2020). *Dogovornoe pravo (obshchaya chast'): Postatejnyj kommentarij k stat'yam 420–453 Grazhdanskogo kodeksa Rossijskoj Federacii [Contract law (General Part): Article-by-article Commentary to Articles 420-453 of the Civil Code of the Russian Federation].* M-Logos.
18. Karapetov, A.G., & Savel'ev, A.I. (2012). *Svoboda dogovora i yeye predely. T. 1: Teoreticheskiye, istoricheskiye i politiko-pravovyye osnovaniya printsipa svobody dogovora i yego ogranicheniy [Freedom of Contract and its Limits. Vol. 1: Theoretical, Historical and Political and Legal Foundations of the Principle of Freedom of Contract and its Limitations].* Statut.
19. Kozlovskaya, S.V. (2018). Problemy grazhdansko-pravovogo regulirovaniya sdelok, zaklyuchaemyh v ramkah elektronnogo vzaimodejstviya [The Problems of Civil-Law Regulation of Transactions Concluded in the Framework of Electronic Interaction]. In A.M. Shirvindt, N.B. Shcherbakov. (Eds.) *Opyty civilisticheskogo issledovaniya: sbornik statej (vypusk 2) [The Experiments of Civil Law Research: Digest of Articles. Vol. 2]* (p. 195–231). Statut.

20. Lodder, A. (2017). Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market. In Lodder, A. & A. Murray. (Eds.). *EU regulation of E-commerce* (pp. 15-58). Edward Elgar.
21. Malaurie, P., Aynès, L., & Stoffel-Munck, P. (2020). *Droit des obligations* (11e éd) [*Law of Obligations* (11th ed.)]. LGDJ.
22. Mangin, C. (2020). *L'expression numérique du consentement contractuel [The Digital Expression of Contractual Consent]* [Doctoral dissertation; Toulouse Capitole University]. Toulouse Capitole Publications. https://publications.ut-capitole.fr/id/eprint/42089/1/ManginCeline2020.pdf
23. Peel, E. (Ed.) (2015). *Treitel on the Law of Contract* (14th ed). Sweet & Maxwell.
24. Poyton, D.A. (2004). *Electronic Contracts: An Analysis of the Law Applicable to Electronic Contracts in England and Wales and its Role in Faciliating the Growth of Electronics.* [Doctoral Dissertation, Aberystwyth University]. Pure. https://pure.aber.ac.uk/ws/portalfiles/portal/9889033/Poyton_phd.pdf
25. Savel'ev, A.I. (2013). Elektronnaya kommerciya v Rossii bez ECP: Illyuziya ili real'nost'? [E-commerce in Russia without Electronic Signature: Illusion or Reality?]. *Vestnik grazhdanskogo prava [Civil Law Review]*, *3*, 43–88.
26. Savel'ev, A.I. (2020). *Elektronnaya kommerciya v Rossii i za rubezhom: pravovoe regulirovanie (3-e izd.) [E-commerce in Russia and Foreign Countries: Legal Regulation (3rd ed.)]*. Statut.
27. Savkunova, A.E. (2016). Akcept kak stadiya zaklyucheniya dogovora [Acceptance as a Stage of Contract Formation]. In A.M. Shirvindt, N.B. Shcherbakov. (Eds.) *Opyty civilisticheskogo issledovaniya: sbornik statej. [The Experiments of Civil Law Research: Digest of Articles]*, 310–336. Statut.
28. Sorieul, R., Clift, J.R., & Estrella-Faria, J.A. (2001). Establishing a Legal Framework for Electronic Commerce: The Work of the United Nations Commission on International Trade Law (UNCITRAL). *The International Lawyer, 35*(1), 107–122.
29. Tatarkina, K.P. (2012). *Forma sdelok v grazhdanskom prave Rossii [Form of Transactions in Russian Civil Law].* Izdatel'stvo TUSURa.
30. Terré, F., Simler, P., Lequette, Y., & Chénedé F. (2019). *Droit civil. Les obligations* (12e éd.) [Civil law. Obligations (12th ed.)]. Dalloz.
31. Veerpalu, A. (2019). Functional Equivalence: An Exploration through Shortcomings to Solutions. *Baltic Journal of Law & Politics, 12*(2), 134–162. https://doi.org/10.2478/bjlp-2019-0015
32. Wang, F.F. (2014). *Law of Electronic Commercial Transactions: Contemporary Issues in the EU, US and China* (2nd ed.). Routledge.

Сведения об авторе:

Шугаев Р.И. — магистр частного права (ВШЭ), фонд «Центр стратегических разработок», Москва, Россия
r.shugaev@csr.ru

Information about the author:

Roman I. Shugaev — LL.M. (HSE), Center for Strategic Research, Moscow, Russia.
r.shugaev@csr.ru

https://doi.org/10.38044/2686-9136-2023-4-2-64-72

СТАТЬИ

БИОТЕХНОЛОГИИ И ПАТЕНТНОЕ ПРАВО: ОПЫТ ЕВРОПЕЙСКОГО СОЮЗА

А.И. Щербакова

АО «Московское протезно-ортопедическое предприятие»
125412, Россия, Москва, Коровинское шоссе, 17а

Аннотация

Стремительное развитие биотехнологий требует повсеместной актуализации и консолидации действий. Для наиболее оперативного и надлежащего ввода новых технологий в жизнь необходимо создание механизмов и инструментов, отвечающих современным вызовам. В настоящей статье представлен обзор институциональных нововведений Европейского союза, которые создают благоприятные условия в том числе и для защиты результатов научных исследований в области биотехнологий. Одновременно с этим обозначены новые риски, обусловленные «охотой» на информацию, негласно объявленной в сфере биотехнологий. Особое внимание уделено взаимодействию и согласованию подходов к защите интеллектуальных прав в свете биотехнологий со стороны Европейского союза и Европейской патентной организации. В рамках данной статьи одним из ключевых факторов рассмотрения новой Системы европейского патента унитарного действия через призму биотехнологий выступает то, что акты, регулирующие деятельность, содержат в себе особые положения, обусловленные именно биотехнологиями. Последнее проявляется как в актах, вводящих Систему, так и в текущих форматах функционирования Единого патентного суда. В статье отмечается стремление ЕС сопроводить деятельность нового института цифровым возможностями. Такие инструменты предоставляются как на стадии ознакомления с правилами и процедурами функционирования Единого патентного суда, так и для совершения ключевых действий при непосредственной работе с европейским патентом унитарного действия. Вместе с тем перенос ряда процедур в цифровую плоскость сопряжен с возникновением некоторых рисков, связанных в первую очередь с безопасностью данных (например, в общем доступе могут оказаться закрытые сведения о разработке, либо персональные данные людей, участвующих в биотехнологических разработках). Утеря таких данных влечет за собой серьезные последствия как финансового, так и научного характера. В этой связи в статье указывается на предлагаемые в настоящий момент форматы защиты и потребность развития обозначенного направления.

Ключевые слова

биотехнологии, Система Европейского патента унитарного действия, Европейский патент унитарного действия, Единый патентный суд, цифровизация, киберпреступность

Конфликт интересов	Автор сообщает об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.

Для цитирования Щербакова, А.И. (2023). Биотехнологии и патентное право: опыт Европейского союза. *Цифровое право, 4*(2), 64–72. https://doi.org/10.38044/2686-9136-2023-4-2-64-72

Поступила: 13.05.2023, принята в печать: 27.06.2023, опубликована: 31.07.2023

ARTICLES

BIOTECHNOLOGIES AND PATENT LAW: THE CASE OF EUROPEAN UNION

Alena I. Shcherbakova

JSC "Moscow Prosthetic and Orthopedic Enterprise"
17A, Korovinskoe highway, Moscow, Russia, 125412

Abstract

The rapid development of biotechnologies requires taking comprehensive steps to actualise and consolidate actions. In order to introduce new technologies into life in the most rapid and appropriate way, it is imperative to establish mechanisms and instruments that meet contemporary challenges. This article presents an overview of institutional innovations of the European Union, which create favourable conditions, including for the protection of research results in the field of biotechnology. At the same time, this paper highlights new risks arising from the "information hunt" implicitly announced in the field of biotechnology. Particular attention is paid to the efforts to cooperate and harmonise approaches to the protection of intellectual rights in the biotechnology realm by the European Union and the European Patent Organisation. For the purposes of this article, one of the key factors in considering the new European Unitary Patent System through a biotechnologies perspective is the fact that the acts governing the activity contain distinctive provisions that are specific to biotechnologies. The latter manifests both in the acts introducing the System and in the current format of the Unitary Patent Court.
The article states that the EU is endeavouring to provide the new institution with digital tools. Such tools are provided both at the stage of familiarising oneself with the rules and procedures of the Unified Patent Court and for performing key actions when dealing directly with a European unitary patent.
However, the digitalisation of some procedures entails certain risks, primarily related to data security (e.g., sensitive development data or personal data of people involved in biotechnological developments may be made public). Once biotechnology development data are lost, there are serious consequences, both financial and scientific. In this regard, the article points out what protection formats are currently proposed and indicates that there is a need to further develop this field.

Keywords

biotechnology, Unitary Patent system, European Unitary Patent, Unified Patent Court, digitalization, cybercrime

Conflict of interest The author declares no conflict of interest.

Financial disclosure The study has no sponsorship.

For citation Shcherbakova, A.I. (2023). Biotechnologies and patent law: The case of European Union. *Digital Law Journal*, *4*(2), 64–72. https://doi.org/10.38044/2686-9136-2023-4-2-64-72

Submitted: 15 May 2023, accepted: 27 June 2023, published: 31 July 2023

Введение

Наравне с цифровыми технологиями в нашу повседневную жизнь активно входят биотехнологии. Биотехнология является одним из самых инновационных и влиятельных секторов в мире, ведь разрабатываемые и внедряемые в этой области инновации позволяют разрешать глобальные и всеобщие вопросы практически во всех сферах (от здравоохранения до сельского хозяйства, проблем мирового голода и изменений климата).

Термин «биотехнология» происходит от трех греческих слов: «биос» (*βίος*) — «жизнь», «технос» (*τεχνηος*) — «мастерство», «техника», «искусство» и «логос» (*λόγος*) — «слово», «разум», «наука», «учение» (Ereky, 1919). Считается, что одним из первых определение биотехнологии дал венгерский инженер Карл Эреки: «Биотехнология — это все виды работ, при которых из сырьевых материалов с помощью живых организмов производятся те или иные продукты».

Для многих развивающихся стран биотехнологии становятся точкой инновационного развития и способствуют построению биоэкономики. Кроме того, уровень развития биотехнологий все чаще выступает своеобразным показателем конкурентоспособности государства в высокотехнологичной сфере.

В соответствии с Конвенцией ООН о биологическом разнообразии (Рио-де-Жанейро, 5 июня 1992 г.) «биотехнология» определяется как «любой вид технологии, связанный с использованием биологических систем, живых организмов или их производных для изготовления или изменения продуктов или процессов с целью их конкретного использования» (ст. 2)[1].

На сегодня общепринятая классификация биотехнологий отсутствует. Вместе с тем многогранность данного вида технологий диктует необходимость в выработке системного подхода к этому вопросу. Достаточно интересной и наглядной представляется классификация биотехнологий, впервые предложенная доктором Ритой Р. Колвелл (Dr. Rita R. Colwell) в 2003 г. (Steiner, 2020):

- «красные», применяющиеся в области медицины и охраны здоровья;
- «зеленые», используемые в сельском хозяйстве;
- «белые», решающие вопросы промышленности, в частности в сфере энергетики[2].

Со временем доктрина дополнила указанную цветовую палитру, и в настоящий момент также выделяют следующие биотехнологии:

- «синие», чье действие связано с морскими генетическими ресурсами;
- «желтые» (в соответствии с некоторыми классификациями — «серые»), направленные на устранение последствий загрязнения окружающей среды;

[1] United Nations. (1993). *Конвенция ООН о биологическом разнообразии.*

[2] European patent office. (2022, November 14). *Red, white or green.* https://www.epo.org/news-events/in-focus/biotechnology-patents/red-white-green.html

- «коричневые», применяемые в пустынях и засушливых зонах;
- «золотые», используемые в сфере биоинформатики, информатики и чиповых технологий;
- «темные», связанные с биотерроризмом и биологическим оружием (Kafarski, 2012).

Биотехнологии — это новые возможности, новые права и свободы, новые этические подходы и т.д., однако биотехнологии — это и огромный сектор экономики.

В 2014 г. объем мирового рынка биотехнологий оценивался в 270 млрд долл. США[3]; в 2020 г. он увеличился более чем в полтора раза, и эта тенденция сохраняется. Ожидается, что к 2027 г. мировой рынок биотехнологий составит около 952 млрд долл. США[4].

Патент как основной механизм защиты прав интеллектуальной собственности

В 2016 г. журнал «Scientific American» опубликовал список ведущих биотехнологических стран мира, где одним из основополагающих показателей выступала защита интеллектуальной собственности (Abbate, 2016). Широко используемым механизмом правового регулирования защиты результатов научных исследований в области биотехнологий выступает патент.

Возможность получения патента на биотехнологию — это гарантия привлечения финансирования для разработчиков и возможность инвестировать в действительно перспективную сферу для инвесторов.

Роль патента для биотехнологий усматривается по трем направлениям:

1) нарастающий и перспективный сектор экономики;

2) двигатель прогресса в соответствующей области (транслятор тенденций), в том числе за счет увеличения межотраслевых технологических соглашений;

3) своеобразный индикатор морально-этического отношения к разработкам.

Стоит отметить, что системе патентования присуща транспарентность, так как публикация заявки влечет за собой распространение детализированной информации относительно последних технических достижений. Данные обычно размещаются на сайтах соответствующих ведомств. Например, Европейское патентное ведомство (далее — ЕПВ) публикует на своем сайте европейские патентные бюллетени[5], которые содержат библиографические и процессуальные данные (правовой статус европейских патентных заявок). Такие бюллетени находятся в свободном доступе и могут быть скачаны на электронные носители.

Текущая ситуация с патентованием биотехнологий в Европе

В Европейском патентном ведомстве биотехнология составляет около 4% всех патентных заявок: в 2021 г. из 188 600 полученных европейских патентных заявок 7 611 касались биотехнологий. Патенты в области биотехнологий в основном относятся к фармацевтическим продуктам (70%), за ними следуют промышленные процессы (26%) и сельское хозяйство (всего 4%)[6]. Необходимо отметить, что в 2015 г. заявки на изобретения в сфере биотехнологий также

[3] Frost & Sullivan. (2014). *Обзор рынка биотехнологий в России и оценка перспектив его развития*. https://media.rbcdn.ru/media/reports/биотехнологии_20141020_Russia_Biotechnology_Market_fin.pdf

[4] Ugalmugle, S., & Swain, R. (2021, May). *Biotechnology Market Size, Industry Analysis Report, Regional Outlook, Application Potential, Competitive Market Sahare and Forecast, 2019–2025*. Global Market Insights. https://www.gminsights.com/industry-analysis/biotechnology-market

[5] European Patent Office. (n.d.). *European Patent Bulletin*. https://www.epo.org/searching-for-patents/legal/bulletin.html

[6] European Patent Office. (n.d.). *The role of EPO*. https://www.epo.org/news-events/in-focus/biotechnology-patents/the-role-of-the-epo.html

составляли 4% от всей совокупности поданных в ЕПВ заявок: общее количество выданных патентов — 160 022, из них 6 048 в сфере биотехнологий[7].

ЕПВ даже выпущено специальное руководство, в котором особое внимание уделено проведению экспертизы изобретений в области биотехнологий[8] (оно регулярно обновляется, чтобы отвечать актуальным вызовам в сфере патентования биотехнологий)[9]. ЕПВ старается досконально проверить, является изобретение действительно новым или нет. В ход пускаются разные методы, в том числе изучаются и так называемые традиционные ноу-хау, т.е. те технологии, которые представляют собой определенные традиции для тех или иных народов. В связи с этим, в частности, ЕПВ получило доступ к индийской электронной библиотеке, посвященной традиционным ноу-хау Индии (*Indian Traditional Knowledge Digital Library*). Особое внимание привлекает база, содержащая информацию о традиционной индийской медицине. В 2009 г. ЕПВ подписало соглашение с правительством Индии, которое позволяет получать электронный доступ к этой базе служащим ЕПВ (Dattatraya & Suradkar, 2021). Аналогично с помощью специальных баз ЕПВ исследует существующие технологии Китая и Кореи[10].

Конвенция о выдаче европейских патентов (Европейская патентная конвенция) (Мюнхен, 5 октября 1973 г.)[11] (далее — ЕПК) считается первым основополагающим шагом на пути к учреждению Европейской патентной системы. При этом ЕПК представляет собой международно-правовой документ, не являющийся исключительно продуктом ЕС. ЕПК носит открытый характер и по состоянию на июль 2023 г. действует в отношении 39 государств, включая все государства — члены ЕС[12]. Однако обозначенный документ имеет большое значение как для формирования Единой европейской патентной системы в целом, так и для защиты прав интеллектуальной собственности в области биотехнологий в частности.

Примечательно, что в Европе действительно осуществляется выработка общих подходов к вопросам, связанным с патентованием биотехнологий. Так, Директива № 98/44/ЕС Европейского парламента и Совета Европейского союза от 6 июля 1998 г. о правовой охране биотехнологических изобретений[13] инкорпорирована в ЕПК в 1999 г., а ЕПВ следует толкованию названной Директивы, данному Судом ЕС, и интегрирует такое толкование в свою практику в сфере биотехнологий.

Амбициозным и внушающим надежду шагом является запуск функционирования Системы Европейского патента унитарного действия, состоявшийся 1 июня 2023 г.

Указанная Система базируется на совокупности трех нормативных правовых актов:

---

7 European Patent Office. (2022, November 2). *L'OEB et les brevets dans le domaine des biotechnologies*. https://www.epo.org/news-events/in-focus/biotechnology-patents_fr.html

8 European Patent Office. (n.d.). *Guidelines for Examination. Exclusions and exceptions for biotechnological inventions*. https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_5.htm

9 European Patent Office. (n.d.). *Guidelines for Examination in the European Patent Office*. https://www.epo.org/law-practice/legal-texts/guidelines.html

10 European Patent Office. (2022, November 2). *What is patentable?* https://new.epo.org/en/news-events/in-focus/biotechnology-patents/what-is-patentable

11 European Patent Office. (n.d.). *European Patent Convention*. https://new.epo.org/en/legal/epc

12 European Patent Office. (n.d.). *Member states of the European Patent Organisation*. https://www.epo.org/about-us/foundation/member-states.html

13 Official Journal of the European Communities. (1998). *Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the legal protection of biotechnological inventions*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.1998.213.01.0013.01.ENG

1) Регламент № 1257/2012 Европейского парламента и Совета Европейского союза от 17 декабря 2012 г., обеспечивающий осуществление расширенного сотрудничества в области создания единой патентной защиты;

2) Регламент № 1260/2012 Европейского парламента и Совета Европейского союза от 17 декабря 2012 г., обеспечивающий осуществление расширенного сотрудничества в области создания единой патентной защиты, в том числе в части правил осуществления переводов;

3) Соглашение об учреждении Единого патентного суда[14].

Единый патентный суд (*Unified Patent Court* (*UPC*)) создан для того, чтобы принимать решения, в частности, о нарушении и действительности как унитарных патентов, так и классических европейских патентов (выдаваемых ЕПВ). Он является общим судом для 17 государств — членов ЕС, для которых Соглашение об учреждении Единого патентного суда вступило в силу 1 июня 2023 г. Такими государствами являются Австрия, Бельгия, Болгария, Германия, Дания, Италия, Латвия, Литва, Люксембург, Мальта, Нидерланды, Португалия, Словения, Финляндия, Франция, Швеция, Эстония[15]. На долю обозначенных участников приходится около 80% ВВП Европейского союза. Вместе с тем участие открыто и для других государств — членов ЕС.

К числу самых заметных преимуществ Системы Европейского патента унитарного действия относятся:

- **получение одного унитарного патента**, действующего во всех государствах-участниках;
- **единое окно для регистрации и защиты патентов в Европе**. Следовательно, ожидается снижение затрат и сокращение бумажных документов. Унитарный патент будет стоить почти в три раза меньше по сравнению с нынешним порядком цен (5 тыс. евро против нынешних 29 тыс. евро);
- **Единый патентный суд**, обладающий юрисдикцией в отношении унитарных патентов и существующих европейских патентов, который позволит компаниям **более эффективно защищать свои патентные права**. Ожидается обеспечение более последовательной правовой основы для патентных споров и снижение риска противоречивых решений. Кроме того, один иск в Единый патентный суд заменит несколько параллельных разбирательств в национальных судах.

Необходимо отметить, что в рамках построения Единой патентной системы Европейский союз продолжает уделять особое внимание биотехнологиям. Так, среди назначенных судей есть отдельная отраслевая группа по биотехнологиям, в которую вошли лица с соответствующей технической квалификацией (восемь судей)[16].

Этапы получения унитарного патента:

1) подача заявки на европейский патент в ЕПВ;

2) проведение экспертизы ЕПВ, которая в случае положительного результата приводит к выдаче европейского патента;

3) принципиально новые возможности: в течение одного месяца с момента выдачи патента его владелец может запросить ЕПВ предоставить единое действие для государств — участников

[14] EUR-Lex. (n.d.). *Agreement on a Unified Patent Court.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A42013A0620%2801%29

[15] Official website of the Unified Patent Court. (n.d.). *A single patent court for Member States of the European Union.* https://www.unified-patent-court.org/en/organisation/upc-member-states

[16] Official website of the Unified Patent Court. (n.d.). *Unified Patent Court judicial appointments and Presidium elections.* https://www.unified-patent-court.org/en/news/unified-patent-court-judicial-appointments-and-presidium-elections

Соглашения. В то же время по давно сложившейся практике владелец европейского патента может также подтвердить его юридическую силу в других странах, не охваченных Системой Европейского патента унитарного действия, в соответствии с национальными процедурами.

Для всестороннего и полноценного развития и становления Единой патентной системы 7 марта 2023 г. председатель ЕПВ Антониу Кампинос и комиссар ЕС по внутреннему рынку Тьерри Бретон подписали рабочее соглашение о европейских унитарных патентах. Такое соглашение предусматривается ст. 14 Регламента № 1257/2012 и выступает основой для сотрудничества и обмена мнениями между двумя учреждениями с целью максимизации преимуществ Системы Европейского патента унитарного действия и содействия ее широкому использованию, особенно среди малых и средних предприятий. Кроме того, в нем содержится положение о том, что ЕПВ и Европейская комиссия должны обмениваться соответствующими данными и информацией, в том числе выводами из обзоров и тематических исследований, касающихся продвижения и использования унитарных патентов, а также проводить регулярные встречи для облегчения и поддержки их деятельности по сотрудничеству.

Вообще формированию Единой европейской патентной системы и функционированию Единого патентного суда во многом способствуют цифровые возможности. Примечательно, что председатель Апелляционного суда Единого патентного суда в день старта работы данного института отметил, что с этого момента указанный институт открывает свои цифровые двери[17]. Такая характеристика подтверждается и на деле, ведь, например, администрирование деятельности Суда осуществляется благодаря специальной *IT*-системе — *Case Management System of the Unified Patent Court*. Именно через нее осуществляется подача заявок, исков и любых иных представлений в Единый патентный суд, а также регистрация представителей / уполномоченных лиц (европейских патентных поверенных). Для доступа к названной системе необходимо получить сертификат аутентификации клиента (который должен находиться на физическом устройстве, таком как смарт-карта или *USB*-накопитель) и сертификат электронной подписи. На сайте данной системы размещен список провайдеров, заявивших, что они соответствуют необходимым техническим стандартам для сертификации.

Также ст. 44 Соглашения об учреждении Единого патентного суда накладывает на него своеобразное обязательство по должному использованию электронных процедур, что, в частности, может реализовываться посредством подачи представлений сторон и изложения доказательств в электронной форме, а также организации видео-конференц-связи.

Кроме того, серьезная цифровая поддержка выражается в многочисленных цифровых инструментах адаптации к новому Суду — брошюрах, курсах на онлайн-платформах, вебинарах и т.д. Уже сейчас заслуживает особого внимания широкий выбор онлайн-механизмов, опубликованных на сайте ЕПВ и направленных на быстрый и легкий переход заинтересованных лиц в плоскость Единого патентного суда[18].

Что касается информационных цифровых изданий, раскрывающих основные сведения о Единой патентной системе и соответственно унитарном патенте, то на данный момент опубликованы две брошюры (на английском, немецком, французском и испанском языках): «Делаем Европу более привлекательной для инноваций и инвесторов» и «Упрощенная и более широкая патентная защита при меньших затратах». На текущий момент доступны декабрьские редакции

[17] Official website of the Unified Patent Court. (2023, June 1). *The Unified Patent Court opens its doors!* https://www.unified-patent-court.org/en/news/unified-patent-court-opens-its-doors

[18] Official website of the Unified Patent Court. (n.d.). *The Unitary Patent.* https://e-courses.epo.org/course/view.php?id=296&lang=en%20%20https://www.transcriptionwing.com/biotechnology-security-why-biotech-companies-cant-ignore-it/

данных брошюр, однако инициаторы указывают, что их актуализация будет происходить на регулярной основе. Процедура выдачи унитарного патента также нашла свое отражение в электронном формате в «Едином патентном руководстве»[19].

Представляется, что обозначенные нововведения обогатят и упростят патентное сопровождение биотехнологий в Европейском союзе, а также более наглядно продемонстрируют большую роль ЕПК и ЕПВ для государств — членов Европейского союза.

Предоставляя изобретателям и предприятиям более простой и экономичный способ защиты своей интеллектуальной собственности в ЕС, новая Единая патентная система будет стимулировать инновации. Это также будет способствовать развитию и коммерциализации новых технологий и продуктов, повышению конкурентоспособности и экономическому росту, а также поможет привлечь иностранные инвестиции в ЕС.

Новые риски

Раскрытие данных о разработках в сфере биотехнологий в нужный момент и в конкретном объеме всегда выступало особым шагом для авторов соответствующей технологии. Конкурентная среда диктует условия, при которых излишние сведения о разработке могут привести к серьезным финансовым потерям, а иногда и к утрате возможности стать бенефициаром конечного продукта. В этой связи особое значение сегодня приобретают меры, направленные на предотвращение утечки данных. Вместе с тем необходимо отметить, что конечной целью злоумышленников может выступать как сама разработка (сведения о ней), так и персональные данные лиц, затронутых процессами становления биотехнологий.

Поэтому сегодня на рынке биотехнологий организации, чья деятельность направлена на обеспечение цифровой безопасности биотехнологических компаний, встречаются все чаще, а спектр предоставляемых ими услуг постоянно увеличивается и совершенствуется. На текущий момент основными инструментами для защиты данных выступают: шифрование, брандмауэры и регулярные аудиты безопасности.

При этом, даже если кибератака все-таки имела место, «выгоднее» действовать в рамках комплексного плана аварийного восстановления, поскольку за счет него удается свести к минимуму время простоя и гарантировать продолжение особо важных и неотложных манипуляций. К тому же такая предусмотрительность биотехнологических компаний предоставляет всем участникам соответствующей разработки дополнительные гарантии относительно безопасности и сохранности своих персональных данных. В этом контексте видится целесообразным указать на специфику персональных данных, оборот которых происходит в сфере биотехнологий: эти данные преимущественно неизменны (например, генетические данные). Соответственно биотехнологические компании должны уделять первоочередное внимание безопасности таких данных, чтобы завоевать и поддержать доверие клиентов.

Приверженность конфиденциальности не только защищает биотехнологические компании от финансовых потерь, но и помогает сохранить доверие пациентов, инвесторов и других заинтересованных сторон. Одновременно с этим компании показывают свое стремление следовать этическим и ответственным методам ведения бизнеса.

---

[19] Official website of the Unified Patent Court. (n.d.). *Unitary Patent Guide.* https://new.epo.org/en/legal/guide-up/2022/index.html

Заключение

Автор полагает, что к настоящему моменту патент утвердился в качестве главного механизма защиты прав интеллектуальной собственности в контексте биотехнологий, однако реальная перспективность разработок в этом направлении порождает ситуации, когда конкуренты изыскивают различные способы получения информации, необходимой им для выведения себя на лидирующие позиции. Во многих юрисдикциях нет полного осознания данной угрозы; инициативы по выработке превентивных механизмов исходят от частных компаний, которые предоставляют разработчикам биотехнологий дополнительные защитные инструменты. Вместе с тем нельзя исключать ситуации, когда лица, производящие кибератаки, и лица, предлагающие услуги по защите от них, могут работать в интересах друг друга. Таким образом, представляется целесообразным разрабатывать соответствующие защитные механизмы на уровне государств или интеграционного объединения — Европейского союза.

В этой связи особую роль приобретает Единый патентный суд. Принимая во внимание все цифровые намерения данного института, а также стремление к единому формату защиты прав интеллектуальной собственности в ЕС, можно прийти к выводу о том, что существующие угрозы в отношении биотехнологических компаний могут быть сняты именно за счет работы названного Суда и соответственно Единой патентной системы.

Обеспечение безопасности в части защиты прав интеллектуальной собственности в области биотехнологий будет способствовать развитию указанного направления, в том числе за счет создания благоприятного фона для инвесторов. Кроме того, защищенные должным образом базы персональных данных повысят лояльность и тех, кто обращается к достижениям биотехнологий.

Так, безопасность необходима для защиты значимых активов, соблюдения институциональных требований и предотвращения потенциального неправомерного использования данных.

Список литературы / References

1. Abbate, J., May, M., & Friedman, Y. (2016). Biotechnology on zero dollars a day. *Scientific American Worldview*, 5.
2. Ereky, K. (1919). Biotechnologie der Fleisch-, Fett-, und Milcherzeugung im landwirtschaftlichen Grossbetriebe: Für naturwissenschaftlich gebildete Landwirte verfasst [Biotechnology of meat, fat and milk production in large farms: Written for scientifically educated farmers]. P. Parey.
2. Dattatraya, T. K., & Suradkar, P. (2021). Traditional knowledge digital library: A Magic bullet in the war against biopiracy. *Library Philosophy and Practice (e-journal)*, 6108. https://digitalcommons.unl.edu/libphilprac/6108
3. Kafarski, P. (2012). Rainbow code of biotechnology. *CHEMIK*, *66*(8), 811–816.
4. Steiner, U. (2020). *Fachenglisch für BioTAs und BTAs*. Springer Spektrum. https://doi.org/10.1007/978-3-662-60666-7_1

Сведения об авторе:

Щербакова А.И. — кандидат юридических наук, методист Научно-образовательного центра АО «Московское протезно-ортопедическое предприятие», Москва, Россия.
sherbakovaalena1563@gmail.com
ORCID: https://orcid.org/0000-0003-0125-9340

Information about the author:

Alena I. Shcherbakova — Ph.D. in Law, Methodist, Scientific and Educational Center of JSC "Moscow Prosthetic and Orthopedic Enterprise", Moscow, Russia.
sherbakovaalena1563@gmail.com
ORCID: https://orcid.org/0000-0003-0125-9340

https://doi.org/10.38044/2686-9136-2023-4-2-73-79

BOOK REVIEW

PHENOMENON OF DIGITAL PLATFORMS AND LEGAL REGULATION

Max Gutbrod

University of Potsdam
Am Neuen Palais 10, House 9, Potsdam, Germany, 14469

Review of a book Inozemtsev, M.I., Sidorenko, E.L., & Khisamova, Z.I. (2022). *The Platform Economy. Designing a Supranational Legal Framework.* Palgrave Macmillan. https://doi.org/10.1007/978-981-19-3242-7

Keywords digital platforms, digital service, data use, data protection, digital law

For citation Gutbrod, M. (2023). Phenomenon of digital platforms and legal regulation. *Digital Law Journal, 4*(2), 73–79. https://doi.org/10.38044/2686-9136-2023-4-2-73-79

РЕЦЕНЗИЯ НА КНИГУ

ФЕНОМЕН ЦИФРОВЫХ ПЛАТФОРМ И ПРАВОВОЕ РЕГУЛИРОВАНИЕ

М. Гутброд

Потсдамский университет
14469, Ам Ноен Пали 10, д. 9, Потсдам, Германия

Рецензия на книгу Inozemtsev, M.I., Sidorenko, E.L., & Khisamova, Z.I. (2022). *The Platform Economy. Designing a Supranational Legal Framework.* Palgrave Macmillan. https://doi.org/10.1007/978-981-19-3242-7

Ключевые слова цифровые платформы, цифровые услуги, использование данных, защита данных, цифровое право

Для цитирования Гутброд, М. (2023). Феномен цифровых платформ и правовое регулирование. *Цифровое право, 4*(2), 73–79. https://doi.org/10.38044/2686-9136-2023-4-2-73-79

Introduction

This book presents us with an enormous, admirable wealth of ideas and thought processes about platforms, their development, legal regulation, and possibilities for legal science and practice, but also the difficulties of understanding new technology-related phenomena and regulation in their context. It assembles chapters by an impressive number of authors from different countries, in excellent English, and has been published by a renowned publisher. A general review of the literature suggests to me that there is currently no book on offer with similar breath. The number of times the book has been downloaded, namely more than 15,000 at the time of this writing, is a tribute to the importance of the topic and the content of this book.

The following summary of its content with some further ideas by no means intends to be comprehensive, but rather focuses on some general and methodological considerations.

The numbers in the parentheses below refer to pages, and the mention of page numbers rather than authors is by no means meant to be complete or to the detriment of the authors.

Approach to Regulation of Platforms

The chapters of the book confirm how difficult it is to even be clear about what the current scholarly discussion is, or should be about, and for obvious reasons, related clarity would be a precondition for getting an understanding of what regulation would be appropriate and whether phenomena are covered that are not yet clear but likely to emerge given what is to be expected, taking likely technical and economic developments into account. Accordingly, the actual approach to regulation, the issues to be regulated, the most suitable approach to regulation, as well as the likely consequences of the regulations that have been or are likely to be introduced, are not overly clear. This is in spite of the chapters referring to many interesting, related approaches and remarks, and, again, I am not aware of any more comprehensive approach to the topic. To go into more detail, the book does contain references to timid (page 68) and inadequate (page 86) government responses, which it links to developments generally not allowing for (page 89) or being too quick to allow for the implementation of regulation (page 149), as well as the development of platforms posing intricate issues (see page 4). The book also alludes to the possibility of deriving criteria from Russian or Eurasian law (page 204), the very definition of platforms potentially leading to conclusions (pages 70, 250), variations in regulation (page 82), the many relevant criteria (page 84), and how potential regulations must deal with new demands, such as sustainability (page 5), so it would appear that scientific studies are required to adequately understand the issues (page 181). In addition, the number of existing laws and legal mechanisms that must be taken into consideration is said to be substantial (page 9). Law is frequently referred to as coming into existence based on custom: starting out as soft law, then turning into semi-hard law, and finally becoming standard law (pages 15 and 54), which begs the question: to what extent are successful systems able to influence law in a manner to support their business?

A more general approach to definitions, presumably with a view to establishing common terms for the phenomena being addressed, simply stresses the importance of having a definition of platforms and relevant ecosystems (pages 80 and 82). The likelihood of controversies concerning the topics (page 85) is also noted.

Given the systems of the platforms being referred to (pages 3 and 9), as well as the number of forms of access to those platforms that exist, the scope of interaction they allow is referred to as global (page 21), and it is natural to believe that national law is to be replaced or complimented

by international law (see pages 59, 64 and 9), while it is unclear how the appropriate level of decision making (by international institutions, countries working together, big countries taking the lead) would be determined, particularly taking into account the different relation platforms have to various countries (see page 50).

Market capitalization (noted in page 51) and the number of platforms (page 80) are mentioned as being an indication of arising issues, and it appears natural for antimonopoly bodies to take charge of regulation in general (page 69) or to believe that dominance in a market requires a reaction (page 69). At the same time, there does not seem to be much clarity about the delineation of the markets reviewed by authorities or the markets to be reviewed. Also while, in many contexts, it is stressed that the platforms have changed our lives, it does seem very likely that it would be possible to return to how life worked before these platforms existed. The question also arises as to whether those old markets, for instance, for advertisements that are predominantly distributed by newspapers, are still relevant. More narrowly, there is little to be found on the influence platforms have on supply chains, or even on complaint mechanisms and the rules governing disputes, which would presumably be frequently influenced by legal service platforms nowadays. Also, there seems to be surprisingly little evidence that anti-monopoly regulation or actions have met with any success or even demonstrated any effect on the markets they were intended to influence.

The above discussion on regulation seems to confirm the perception that can also, *mutatis mutandis*, be applied to a number of further topics, which will be discussed in more detail below: namely that the very emergence of platforms leads to the structure of the discussion changing, or at least leads to issues being presented in a different manner. However, if addressed in a more conventional manner, these issues and topics could be put into context more easily: namely the context known from previous discussions, and, in this context, the novelty of new phenomena, particularly platforms, could become evident more easily. To be more specific, a social network with a substantial market position may trigger reactions that are typical for dominant players, and while the use of this social platform will by no means be as important as, for instance, the supply of water, some of the rules for natural monopolies may be deemed useful in regulating this social network. From a more general perspective, it may well be that the acceleration of technological progress also requires us to revisit a notion that has may not have been discussed in as comprehensive a manner as it should have been: namely that science should not assume that it has comprehensive command of its own methodology, and should rather be open to revising this methodology on an ongoing basis.[1]

Employment or Contracting?

Given how many people have contact with platforms in some manner and are at least partially making use of a platform in one way or another, it is natural to discuss the rules on social protection that are already in place, which may or may not lead to satisfactory results for the people involved and the general population, and expand this discussion to what is to be expected in the foreseeable future. For instance, it could well be that unemployment will increase due to progress

[1] For obvious reasons, a full discussion of this topic is not possible here. I only note that I have been impressed by one of the masterminds of economic research and economic policy in postwar Germany, Eucken, in the review of his theory by Petersen (2019), pages 48ff using as a description of his method the term "morphology", which in itself is not further defined. Taking the example of the work of the eminent and, to my mind, insufficiently recognized German scholar Joachim Gernhuber as reference, I believe to soon be able to demonstrate another approach to legal science having to, on an ongoing basis, satisfy itself that it comprehensively covers the legal phenomena at hand.

in digitalization, leading to the likelihood that people will require various state sponsored subsidies or protection. Of course, it would be useful to expand this angle of examination to cover the current and potential role of trade unions in protecting employees and self-employed workers,[2] and to examine whether related regulation requires amendment if it is to accommodate the specifics of platforms. In contrast, of course, regulation can try to apply limits, for example, by creating rules limiting the permissible size of commissions to specific types of parties involved with platforms,[3] and the overall effect of such limited limitation would be of interest for other types of regulations.

Tellingly, the importance of related issues seems to be confirmed by the specifics, sheer number, and intricacy of criteria to be reviewed in different jurisdictions when making a decision on whether an employment relationship is in place,[4] as opposed to an independent contractor relationship. Accordingly, it is not surprising to read about the specific features with respect to various platforms which are relevant (page 90), as well as differences among countries (page 99), developments over time (pages 93*ff*), and the importance of direction rights of the platform (page 35).

Regulation and Characterization of Service

Interestingly, it does not seem to be immediately apparent what the services provided through platforms are or how they are to be defined. However, the differences from the traditional way of working together, referred to as collaborative economy (page 14), sales taking place (page 78), responsibility for products (pages 65*ff* and 70) or services sold (page 72) are noted. There is also reference to regulation that could lead to services collapsing (87), licensing requirements for providing services (page 86), in particular, drivers found through a platform (page 88), and the specifics of marketing (page 153). Cross-border payments (page 132) and related issues (page 131), the importance of platforms in daily life (page 142), and qualitative changes by platforms (page 17) are also discussed.

Of course, when comparing, in a very general matter, the above to what one remembers from when more traditional areas of the law are applied — for example, what is discussed under the title of law of obligations (Schuldrecht, *obyazatelstvennoe pravo*) in civil law countries — one does not find much about rules or discussions about implementing the very functions of the platforms, for example: on how law helps the granting of the ability to read, post, and access posts or personal profiles at a given moment or over time, the transport of messages, their interruption, be it because of malfunction, a change in user policy, the transparency of the placement, or the effect of placing marketing material, as well as on the openness of platforms to political or other various types of business influence,[5] such as the infringement of the secrecy of communications for political or security reasons.

[2] I have partially explained their role in Gutbrod, M. (n.d.). *About Managing Legal Reform (German).* Academia. Retrieved July 4, 2023, from https://www.academia.edu/18503022/About_Managing_Legal_Reform_German_

[3] Like the ones referred in Stogova E. (2023, April 24). *Vlasti ogranichat komissii agregatorov ot prodazhi biletov v teatry [The authorities will limit the fees of aggregators from the sale of tickets to theaters in Moscow].* RBK. https://www.rbc.ru/technology_and_media/24/04/2023/64466c879a7947eef66dc9a7?from=from_main_2

[4] The novel presentation used in Waas and Heerma von Voss (2017) for, inter alia, the difference between the contract for works and the employment contract. This study highlights the intricacy of the problem, in my dissertation (Gutbrod, 1993), pages *26ff*, it took me almost 10 pages and the collection of hitherto unassembled Brazilian material to provide for a similar summary which was clearly influenced by there being a compensation for the termination of trade and franchising agreements in Germany.

[5] See discussion of a recent example being Users being held hostage to business and political views of platforms. Lauer C. (2022, November 11). *Elon Musk fährt Twitter gerade voll gegen die Wand — will er die Plattform mit Absicht zugrunde*

In addition to what traditionally would be referred to as contractual obligations, procedural practice may also deserve attention. The ability to identify counterparties, for instance, for disputes involving libel or platforms purposefully offering goods from sellers in other jurisdictions in order to avoid consumer claims, could serve as examples.

Not least, whether or not compensation is adequate for the service provided may be an issue to be reviewed.[6] For instance, the timing of the service may be more important in the platform economy than it was at the time the Civil Codes were drafted.

Linking this civil law discussion to the market structure considerations discussed earlier, one could imagine that some of the approaches taken for the quality of services — for instance for it to be free of so-called 'hate speech' — would also have to deal with the benefit of leaving quality standards to the discretion of the platforms in order to increase the chance of further development and encourage new players, as well as, for example, whether demanding the implementation of systems, for instance systems that block hate speech or pornography, provide for barriers to market entry, and whether it is reasonable to believe that related procedures (self-enforcement or enforcement through state courts) demonstrate effectiveness over time.

When, more broadly comparing the current debate to earlier ones, it is striking how many issues are no longer considered to belong to the spere of civil law, with 'the right to be forgotten' on the internet being just one small example. Before the emergence of platforms, a comparable right and the relevant demands would have been a natural part of the life of the contract. Now, it is naturally seen as being part of data protection law. Trying to compare today's perspectives to history, the following general assessment comes to mind: "Legal regulations for contracts are not drafted on the basis of theories. As a rule, they are developed with a constant eye on the reality of the practice they are tasked to regulate."[7] While in the reality before platforms, or at least before mass contracts emerged, this "eye on reality" would most likely be the one of those who had to deal with such contracts. In the case of platforms, it appears that these types of practitioners are more difficult to find, and, in particular, taking the considerations above into account, the practical views alluded to would no longer be sufficient. It is striking how much Gernhuber's further assessment of the benefit of regulation applies to what platforms would benefit from: "In theory, in a legal system that provides for freedom of contract, regulating contracts through statutory regulation is superfluous; the *lex contractus* is sufficient to settle all relevant questions. In practice, both the development of a general law of obligations and the regulation of individual types of contractual obligation in a special law of obligations have proven to be necessary in view of a contractual practice in which the parties hardly ever take up questions of the general law of obligations and in the area of the special law of obligations draft extensive regulations only in the form of the contract of adhesion and in highly specialized individual contracts (for instance relating to equipment purchase agreements, but even then are not overly concerned about

richten? [Elon Musk is driving Twitter straight into the wall — does he want to ruin the platform on purpose?]. Business Insider. https://www.businessinsider.de/politik/elon-musk-faehrt-twitter-gerade-voll-gegen-die-wand-will-er-die-plattform-mit-absicht-zugrunde-richten-a/

6 See discussion of the related regulatory options in Lange (1990).

7 I am citing Gernhuber (1994), § 7 IV 3, S. 153 here in my free translation, not only to make his views better available, but also because I believe that few similar assessments exist. The German equivalent of the English is: „Vertragsordnungen werden nicht theoretisierend entworfen. Im Regelfall werden sie entfaltet mit stetem Blick auf die Lebenswirklichkeit, deren Regelung ihre Aufgabe ist."

completeness."[8] Indeed, and further to what has been set out above, it does very much seem that attention to contracting, where platforms are concerned, is one sided with respect to the operator of the platform, and the operator of the platform will initially be very interested in attracting as many users as possible by using amenable contractual provisions, with the likelihood being that this approach will be reversed during the life of the contract. Even more thinking about how to better position the parties for a meaningful determination of contractual obligations seems to be warranted. Possible modern examples of drafting contracts with the stated aim of protecting consumers, but with a possible view to establishing a level playing field,[9] can be found in § 305 BGB (contract of adhesion), § 651a BGB (travel agreement)[10] and § 491 BGB (consumer credit agreement).

Data Use and Protection

Interestingly, digital data is identified as the key factor for the operation of platforms (page 20). The importance of the related data value chain is also proposed as a metric (page 78), the turnover related to that data is noted (page 4), and examples are given (page 204). Not much can be found about, what would appear to me, to be the core of the business of platforms: namely the algorithms they use, specifics about the consequences the use of AI, and what the much talked about cookies really are. In a sense, while, as mentioned, the book presents us with a great multitude of facts, this multitude does not immediately make it possible to confirm or disprove the notion that the discussed platforms have largely transformed data into the oil of the future and monetized them, as predicted.

In contrast, when discussing data protection, one seems to return to a known normal, with quite some detail being cited (page 152) and GDPR emerging as a key regulation (pages 152*ff*) that might be an obstacle to newcomers from having success (page 153). Among specific issues requiring regulation, requirements for using an image (page 190), ownership issues (page 81), and the effect of platforms on media (page 206) are discussed, although protection of reputation is not discussed in much detail. Other new dangers, including scammers (page 188), and new emerging terms, such as IP addresses or bloggers (page 189), appear to require a special assessment.

Government Support for Platforms

Incentives in Russia (pages 160*ff*), as well as Glonass and Gosuslugi, are mentioned as examples (23), and the interest by Central Banks (page 131) is noted. Furthermore, how governments are using platforms to improve their educational systems is described in a very general manner (page 176), while more detail is given to various different countries (page 178), particularly the US (page 179) and Estonia (page 179), from which one can conclude that governments are primarily focusing

[8] Gernhuber (1994), § 7 IV 4, S. 154: The German original which I freely tranlated into is: „Theoretisch bedarf vertragliches Schuldrecht in einer Rechtsordnung, die Schuldvertragsfreiheit gewährt, keiner gesetzlichen Regelung; die lex contractus hat ggf. allein alle Fragen zu regeln. Praktisch ist sowohl die Ausbildung eines Allgemeinen Schuldrechts als auch die Regelung einzelner Schuldvertragstypen in einem besonderen Schuldrecht notwendig angesichts einer Vertragspraxis, in welcher die Parteien Fragen des Allgemeinen Schuldrechts kaum je aufgreifen und sich im Bereich des Besonderen Schuldrechts zu umfangreicheren Regelwerken nur im Formularvertrag und im hochspezialisierten Einzelvertrag (etwa: im Industrieanlagengeschäft) bereitfinden, aber auch dann um Vollständigkeit nicht besorgt zu sein pflegen."

[9] Gernhuber (1983) § 3 I 1 2, S. 17.

[10] A long time ago, I planned to compare the German Civil Law based system with the Russian licensing system, but never got beyond a draft.

on education and other already existing processes. At the same time, it would be interesting to understand whether the technical abilities that are emerging are also being used for innovation in education, for instance, for an enhanced use of grading systems so as to have a basis from which to target specific weaknesses.

Conclusion

When generally reflecting on what one can read in this book, one is reminded of a sort of contemporaneous history, of a display of details that are necessary but not sufficient for the many developments we have witnessed and are still likely to witness.

References

1. Gernhuber, J. (1983). Bürgerliches Recht (2. Auflage) [Civil law (2nd ed.)]. C. H. Beck.
2. Gernhuber, J. (1994). Das Schuldverhältnis (2. Auflage) [The law of obligations (2nd ed.)]. C. B. Mohr (Paul Siebeck).
3. Gutbrod, M. Handelsvertreter und Vertragshändler nach brasilianischem und deutschem Recht [Commercial agents and authorized dealers under Brazilian and German law]. [Doctoral dissertation, München Universität]. Peter Lang.
4. Lange, H. (1990). Schadensersatz-Richterrecht oder Gesetzesreform? [Compensation for damage — judicial law or legal reform?] In K.W. Nörr (Ed.), 40 Jahre Bundesrepublik Deutschland — 40 Jahre Rechtsentwicklung: Ringvorlesung der Juristischen Fakultät der Universität Tübingen 1989 [40 years of the Federal Republic of Germany — 40 years of legal development: Lecture series of the law faculty of the University of Tübingen 1989] (pp. 143-158). J. C. B. Mohr (Paul Siebeck).
5. Petersen, J. (2019). Rechtsordnung und Wirtschaftsordnung nach Eucken [Legal system and economic system according to Eucken]. De Gruyter. https://doi.org/10.1515/9783110666229
6. Waas, B, & Heerma von Voss, G. (Eds.). (2017). Restatement of Labour Law in Europe: Vol I: The Concept of Employee. Hart Publishing.

Information about the author:

Max Gutbrod — Dr. jur., Lecturer at the University of Potsdam, Former Partner and Managing Partner of Baker McKenzie, Potsdam, Germany.
gutbrod.max@gmail.com
ORCID: https://orcid.org/0000-0003-1970-8896

Сведения об авторе:

Гутброд М. — Dr. jur., лектор Потсдамского университета, бывший управляющий партнер международной юридической фирмы Baker McKenzie, Потсдам, Германия.
gutbrod.max@gmail.com
ORCID: https://orcid.org/0000-0003-1970-8896