ГОНТАРЬ Людмила Олеговна
Эксперт International Cyber-Terrorism Regulation Project (ICTRP), руководитель Цифрового образовательного проекта «knowledge+», член ТРГ «Сколково», советник государственной гражданской службы 3-го класса, (119991, г. Москва, ул. Ленинские горы, 1, стр. 13, тел.: +7 968–049–77–27, email: cambridge.gontar@gmail.com)

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ РАЗВИТИЯ ИНТЕРНЕТ-КОМПАНИЙ: МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ VS САМОРЕГУЛИРОВАНИЕ

Аннотация. *В статье анализируются вопросы международного правового регулирования защиты персональных данных в условиях развития интернет-компаний (цифровых платформ). Активно популяризируются следующие виды проблем, связанных с защитой персональных данных: проблема массовой утечки персональных данных, их последующее использование; использование пробелов в терминологическом толковании понятия «персональные данные» для последующего изъятия данных и использования в собственных целях и т.д. Цифровые платформы (интернет-компании) набирают широкую известность и имеют собственные документы в сфере регулирования.*

Кроме того, проблема заключается не только в обеспечении баланса между международно-правовым регулированием и саморегулированием международных организаций. Проблема в большей степени связана с новыми концепциями «обезличивания данных», в должной мере не доработанных, но используемых в законодательных инициативах большинства государств. Мы подробно рассмотрим некоторые правовые нормы регламента GDPR как мегарегулятора данных на уровне ЕС.

В статье внимание читателя будет обращено на множество международных документов, в которых затронуты не только базовые вопросы обработки и использования персональных данных, но и новые концепции в сфере данных, с точки зрения сформировавшейся дисциплины «науки о данных». Такими документами являются, например руководства ОЭСР, МСЭ. Это объясняется тем, что данные международные организации предпринимают попытки исследовать не только механизмы правового регулирования, но и сущность объекта правового регулирования (данные, персональные данные). Междисциплинарный подход в сфере защиты персональных данных является важным элементом, который необходим для формирования качественной международно-правовой базы.

Ключевые слова: *защита персональных данных, интернет-компании, цифровые платформы, обезличивание данных, трансформационные нормы без привязки; нормо-цифровые окна, регламент GDPR, проект ОЭСР «Going digital».*

> *Как же им видеть что-то иное, кроме теней, раз всю свою жизнь они вынуждены держать голову неподвижно?*
>
> *Платон*[161]

В условиях развития международных технологических процессов и появления новых концепций данных (в условиях Big data) следует особое внимание уделить защите персональных данных конкретных граждан. Трансформационные процессы на уровне международных организаций, использование той или иной технологии (в нашем случае цифровых платформ), порождают ряд вопросов, связанных с защитой персональных данных, процессом обезличивания данных и т.д. Напри-

[161] Jowett, Benjamin, trans., The Republic of Plato: An Ideal Commonwealth. New York: Colonial Press,1901.p.209.

мер, массовые утечки информации о пользователях, использование данных их аккаунтов злоумышленниками, незаконный перенос данных с одной цифровой платформы на другую и т.д.

Трансформационные процессы затрагивают и вопросы развития новых технологий, которые тесно связаны с защитой данных. Данными технологиями выступают: Iot (интернет вещей); Big Data (большие данные); AI (искусственный интеллект). Данное взаимодействие мы рассмотрим далее в статье.

В статье нами будут рассматриваться международно-правовые концепции защиты данных, которые нашли свое выражение в международных документах. Кроме того, в статье будет представлен краткий анализ кейс-практики саморегулирования конкретных интернет-компаний. В данной статье мы предложим свои соображения по поводу решений, которые можно было бы проработать на международном уровне.

Для глубокого анализа международно-правовой базы в сфере защиты данных мы позволим себе остановиться на следующих терминологических разъяснениях. Именно эти разъяснения будут применяться в данной статье. Мы выделяем следующие понятия исключительно в указанных значениях:

а) *цифровые платформы (интернет-компании)* — платформы (технические решения с отдельным интерфейсом и функциональностью), которые используются интернет-компаниями (Facebook, Google и т.д.), которые используют данные зарегистрированных пользователей в собственных интересах;

б) *защита персональных данных* — комплекс организационных, правовых действий на международном и национальном уровне с целью предотвращения возможных будущих нарушений, связанных со сбором и использованием персональных данных пользователей.

Защита персональных данных в условиях развития цифровых платформ

Мы позволим себе обратиться к книге Т. Сибела «Цифровая трансформация»[162]. В данной книге автор представляет нашему вниманию три основных этапа цифровой революции:

1. Iot (интернет вещей);
2. Big data (большие данные);
3. AI (искусственный интеллект)[163].

Данные технологии неразрывно связаны друг с другом, хоть и имеют разные технические алгоритмы и функциональные особенности. Автор демонстрирует неразрывную связь данных элементов со всеми процессами, происходящими в условиях цифровой трансформации (не исключаются и организационно-правовые вопросы)[164]. Потому мы с полной уверенностью можем сказать, что данные процессы связаны между собой. Big data выступает совокупностью данных и процессов их обработки, структурирования, а защита персональных данных выступает своего рода перечнем (ограниченным предметно[165]) действий для реализации защиты определенных групп собранных и используемых данных.

Персональные данные выступают частью Big data и связаны со всеми вышеназванными процессами трансформации. Это обусловлено связью интернет-компаний с данными процессами и их интеграции. Именно интернет-компании выступают хранителем персональных данных и центром их обработки.

[162] Т. Сибел Цифровая трансформация. Как выжить и преуспеть в новую эпоху.— М.: Изд-во Манн, Иванов и Фербер. 2021. С. 5–15.

[163] Там же.

[164] Там же.

[165] Речь идет о различных отношениях в сфере Big data. Данные отношения могут касаться защиты данных, обмена данными, доступности данных и т.д.

Реализация защиты персональных данных на международном уровне

Реализацию защиты персональных данных на международном уровне мы будем рассматривать через призму следующих международных организаций:

1. Европейский союз (далее — ЕС);
2. Международный союз электросвязи (далее — МСЭ);
3. Организация экономического сотрудничества и развития (далее — ОЭСР).

Мы позволим себе отметить, что затрагиваем в нашей статье именно те организации, которые участвуют не только в формировании своей собственной информационной политики, но и участвует в гайдах, исследуют вопросы защиты персональных данных. Пояснить это можно с позиции вопросов, которые мы намерены раскрыть в данной статье.

В большей степени нас интересуют «внешние» документы (что мы получаем по итогу международного нормотворчества), а не внутренние. Например, документы политики конфиденциальности и документы по обращению с данными, созданные Управлением Верховного комиссара Организации Объединённых Наций по делам беженцев[166], безусловно важны для формирования общей политики защиты персональных данных. Однако в нашей статье мы затрагиваем проблему цифровых платформ интернет-компаний. Потому нам важно перечень субъектов сделать более узким и целевым.

GDPR на уровне Европейского союза: структура и основные понятия

На уровне ЕС 25 мая 2018 г. был принят регламент GDPR (Общий регламент по защите данных)[167]. Целью

[166] См. https://www.un.org/ru/sections/nobel-peace-prize/office-united-nations-high-commissioner-refugees-unhcr/index.html

[167] Regulation (EU) 2016/679 of the European Parliament and of the Council of

принятого регламента является укрепление прав субъектов персональных данных. GDPR подразумевает ответственность за несоблюдение правил хранения и обработки персональной информации. Данный регламент по определению является неким мегарегулятором защиты данных и регламентирует их трансграничную передачу.

В регламенте приводятся базовые термины. Условно выделим основные из них:

— *персональные данные*, т.е. любая информация, относящаяся к субъекту данных, а именно к идентифицированному и поддающемуся идентификации физическому лицу (т.е., лицу которое можно прямо или косвенно идентифицировать, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайновый идентификатор или один или несколько факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица);

— *обработка* — любое действие (операция) или совокупность тех или иных действий (операций), которые совершаются с персональными данными с использованием средств автоматизации или без использования таких средств, включая сбор, запись, организацию, структурирование, накопление, хранение, адаптацию или изменение, просмотр, использование, раскрытие посредством передачи или иной вид предоставления доступа, сопоставления или комбинирования, сокращения, удаления или уничтожения;

27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Электронный ресурс: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (дата обращения — 10.03.2021).

— *ограничение обработки* — это маркировка хранимых персональных данных с целью ограничения их возможной обработки в будущем;

— *контролер (контроллер)* — это любое физическое или юридическое лицо, государственный орган, учреждение или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных (контролер или критерии для его определения могут быть установлены законодательством Союза или государства-члена);

— *процессор* — это физическое или юридическое лицо, государственный орган, учреждение или другой орган, который обрабатывает персональные данные от имени и по поручению контролера;

— *получатель* — это физическое лицо, государственный орган, учреждение или иной орган, которому раскрываются персональные данные, независимо от того, является ли он третьим лицом или нет;

— *согласие субъекта* — это добровольное, конкретное, информированное и однозначное волеизъявление, в котором субъект данных с помощью заявления или четкого утвердительного действия дает согласие на обработку данных.

Особое внимание заслуживает статья 5 регламента GDPR, в которой упоминаются принципы, касающиеся обработки персональных данных. К принципам относятся: законность, справедливость и прозрачность обработки данных; сбор и обработка для конкретных, отчетливых и законных целей; персональные данные должны быть адекватны и релевантны тому, что необходимо касательно целей, для достижения которых

они обрабатываются, а также ограничены этим; персональные данные должны храниться в форме, которая позволяет идентифицировать субъектов данных не дольше, чем это необходимо для целей, для которых эти данные обрабатываются; обработка должна осуществляться безопасным способом, включая мероприятия по защите от несанкционированной или незаконной обработки.

Принципы отличаются своим не абстрактным, максимально приближенным к объективным процессам характером изложения. Это важно, потому как конкретизация тех или иных процессов и возможность применения принципов к ним обеспечивает действие каждого из положений GDPR.

Вышеназванные термины фигурируют практически во всех пользовательских соглашениях или политиках конфиденциальности, что говорит о высокой степени эффективности данных положений.

Следует отметить, что авторы Регламента уделили особое внимание процессу обработки данных. Процесс обработки данных должен быть прозрачным, т.е. весь процесс обработки данных и понимание процедуры работы с данными должны быть доступны субъектам персональных данных.

В соответствии с Регламентом вводятся два термина: контролер и организация-обработчик (процессор). Под контроллером понимается организация, которая сама инициирует процесс обработки персональных данных сотрудников или клиентов, а также отчитывается перед надзорным органом за процесс обработки той или иной информации. Организацией-обработчиком является организация, которая обрабатывает персональные данные от имени контролера.

В регламенте уточняется термин «право на забвение». Под данным правом понимается право субъекта на удаление его персональных данных из поисковой

выдачи. Это право конкретизируется в части оснований его возникновения:

- личные данные больше не нужны в соответствии с целями их сбора и обработки;
- отзыв согласия на обработку персональных данных;
- возражение субъекта против обработки его данных;
- персональные данные были обработаны незаконно;
- данные должны быть удалены в соответствии с юридическим обязательством, закрепленном в законодательстве Европейского союза или государства-члена, которому подчиняется контролер;
- личные данные собраны в соответствии с предложениями услуг информационного общества.

Также уточнено право на перенос данных, оно включает в себя следующие основания, при которых контролер вправе беспрепятственно переносить данные:

- обработка основана на согласии пользователя;
- обработка осуществляется автоматизированными средствами.

Мы позволим себе особенно отметить, что в регламенте различаются понятия «сбор» и «использование» информации (не только на теоретическом, но и на практическом уровне). В этом и есть основной дискурс работы с современными данными, так как зачастую невозможно понять в чем состоит нарушение и где начинаются цифровые права другого человека.

В этой части регламент действительно выступает мегарегулятором, с точки зрения затронутых процессов

обработки данных и содержания права на защиту персональных данных и сущности регулируемых отношений.

Дополнительно мы хотим отметить, что проблемой является то, что ограничение территориальности безусловно создает определенные сложности в реализации. Хотя многие крупные интернет-компании, такие как Facebook, заявили, что будут исполнять регламент и внесут соответствующие изменения в собственные локальные акты[168]. Однако, не все интернет-компании и операторы на цифровом рынке поддерживают подобный регламент, ссылаясь на территориальные границы действия Регламента и законодательство Европейского союза.

Также при внедрении тех или технический решений при обработке персональных данных так и остается проблема информационной безопасности. Обеспечение полной безопасности данных в условиях развивающейся концепции «обезличивания данных» под влиянием big data, остается актуальным на данный момент времени.

Так, Минцифры России был предложен законопроект, регламентирующий политику обработки обезличенных данных[169]. Например, оператор не сможет использовать какую-либо дополнительную информацию, которая помогает определить принадлежность персональных данных конкретному субъекту. Под запретом также окажется деобезличивание данных, за исключением случаев, когда есть необходимость защитить здоровье человека. Как утверждают авторы законопроекта деобезличивание является обратимым процессом.

Данная инициатива демонстрирует замкнутую цепочку действий по обработке персональных данных (именно о данных рисках предупреждает документ ОЭСР,

[168] См. https://marketinfo.pro/news/facebook-grozit-shtraf-do-163-mlrd-za-narushenie-po-zaschite-personalnyh-dannyh

[169] Законопроект «О внесении изменений в Федеральный закон «О персональных данных»». Электронный ресурс: https://sozd.duma.gov.ru/bill/992331–7 (дата обращения: 15.03.2021 г.).

о котором далее пойдет речь). Складывается следующий неопределенный процесс по работе с данными. При передаче обезличенного массива данных третьему лицу обработка этих данных в иных целях, кроме тех, для которых данные были собраны, невозможна. Этот процесс требует получения нового согласия физического лица, но обратиться за ним будет невозможно.

Поэтому важно предвидеть определенные риск-факторы для обеспечения реального действия GDPR.

Правовая позиция МСЭ

МСЭ в отличие от Европейского союза посчитал верным держать позицию «комментатора» и по мере необходимости давать рекомендательные и разъяснительные положения (как собственные, так и по регламенту GDPR).

В отношении Регламента МСЭ высказался в статье «Влияние общей защиты данных (GDPR) на данные бизнес-моделей: портативность данных и Facebook»[170]. В данной статье анализируется свойство «портативности» (переносимости) данных. Подобное свойство оценивается как перспектива, которая может иметь положительный результат. Переносимость данных, легально закреплённый процесс, решающий проблему блокировки и последующих монополий, где давление конкуренции может повысить качество собираемых данных и предоставляемых услуг.

По мнению авторов статьи свойство портативности данных устраняет «эффект блокировки». Эффект блокировки пользователи цифровой платформы Facebook испытывали из-за затрат на переключение, связанных с сохранением своих данных на прежней платформе. Блокировки, по мнению авторов статьи, искажают конкуренцию, устанавливая рыночные барьеры. Следовательно, право на портативность данных (переносимость), закрепленное в GDPR, может стимулировать инновации, поскольку в данном праве частично отражаются стандарты совместимости нескольких платформ и возможность переноса данных на ту или иную платформу.

Авторы отмечали, что Facebook может расширить свою бизнес-модель с помощью вышеназванного свойства (портативность данных). Например, компания может предложить функцию импорта данных для передачи музыкальных данных Spotify.

Вышеописанный процесс обеспечивает доверие потребителя к цифровой платформе и стимулирует цифровые платформы на развитие добросовестной конкуренции на цифровом рынке.

Также МСЭ выпустил рекомендацию от 2017 г. «Информационные технологии. Методы безопасности. Свод правил защиты информации, позволяющей установить личность»[171]. Данная рекомендация носит диспозитивный характер. Рекомендация содержит кодифицированный свод правил, в котором особое внимание уделено защите персональных данных в технических устройствах и на организационном уровне (организации и т.д.).

Особое внимание заслуживает раздел о криптографии, где упоминается контролирование криптографических процессов при обработке данных. Далее, авторами рекомендации подробно рассматривается операционная безопасность. Именно раздел об операционной безопасности включает в себя пункты о процессе вхождения в систему и ее мониторинг, контроль операционного компьютерного обеспечения, аудит информационных систем.

[170] Article 2 — The General Data Protection's (GDPR) impact on data-driven business models: the case of the right to data portability and facebook. Электронный ресурс: https://www.itu.int/pub/S-JOURNAL–ICTS.V1I2–2018–2 (дата обращения: 12.03.2021).

[171] Information technology — Security techniques — Code of practice for personally identifiable information protection. Электронный ресурс: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13182 (дата обращения: 12.03.2021).

Данную рекомендацию МСЭ нельзя рассматривать как аналог GDPR, так как направление стандарта достаточно узкое и сосредоточено исключительно на аспектах обеспечения безопасности, а не на сбалансированном регулировании комплекса прав на персональные данные. Но, мы заметим, что раздел о криптографии и операционной безопасности следовало бы в дальнейшем учитывать в решении многих вопросов, связанных с правовым регулированием защиты персональных данных. Подобные технические аспекты могли бы стать основой для технических стандартов.

ОЭСР и проект «Going digital»

Проект «Going digital» находится на третьей фазе своего развития, которая называется «Управление данными»[172]. В ходе проекта данные пользователей стали основой цифровых технологий, таких как искусственный интеллект и направления по повышению производительности и инноваций, а также совершенствования процесса принятия автономных решений. Изменение ценности данных, понимание их влияния на социальную систему и разработка более эффективных механизмов управления данными имеют решающее значение для получения максимальной отдачи от цифровой трансформации при одновременном решении таких вопросов, как конфиденциальность данных, конкуренция и защита прав интеллектуальной собственности.

Третий этап проекта рассчитан на открытие новых горизонтов трансформации и ее постепенного воздействия на общество с помощью четырех групп в сфере данных:

- управление данными, доступ, совместное использование и контроль;

[172] Подробнее см. http://www.oecd.org/going-digital/

- трансграничные потоки данных;
- использование данных фирмами и рынками;
- измерение данных.

В рамках вышеназванного третьего этапа было издано «Руководство по защите неприкосновенности частной жизни и трансграничных потоков персональных данных»[173] В редакции документа освещены принципы обеспечение неприкосновенности частной жизни, такие как:

- справедливый, законный и ограниченный сбор персональных данных, получаемых с ведома и согласия физического лица;
- данные собираются в соответствии с целями обработки, обеспечивается их полнота и актуальность;
- использование данных для новых целей должно быть либо совместимо с первоначальной целью обработки, либо требуется согласие субъекта персональных данных на новые виды использования или раскрытия информации;
- используются разумные меры безопасности для защиты данных и обеспечивается подотчетность всех операторов данных.

Также в Руководстве отмечается, что у субъекта персональных данных есть право на доступ к хранящейся информации о нем (данным о пользователе), а также право на ее уничтожение или исправление. Кроме того, усилены требования к подотчетности оператора данных независимо от местонахождения данных, а также к обработке данных самим оператором, его представителями и при передаче другому оператору. Важным является, как упоминается в руководстве, сконцентрировать вни-

[173] The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Электронный ресурс: http://www.oecd.org/sti/ieconomy/privacy.htm (дата обращения: 11.03.2021).

мание государств на трансграничном сотрудничестве между уполномоченными органами по защите данных.

В ОЭСР решили продолжить данную работу по развитию концепции защиты персональных данных в рамках проекта «Цифровой трансформации» («Going digital»)[174]. Однако вектор развития сменился, на наш взгляд, на более радикальный. ОЭСР выпустила отчет, в котором исследуются возможности расширения доступа к данным и обмена ими (EASD)[175] в контексте растущего значения искусственного интеллекта и интернета вещей.

В отчете подчеркивается польза «открытости данных» и отмечается закономерность повышения социальной значимости и повышения роли таких данных. Вместе с тем, подчеркивается риск-фактор утечки данных и необходимость его учета. В отчете приводится несколько проблем, которые можно решить при использовании концепции «открытости данных»:

1. Контрактные соглашения, которые подразумевают рыночный подход к расширению доступа к данным и обмену ими в контексте B2B, в частности, использование через цифровые рынки данных;
2. Открытость данных часто трактуется правительствами как экстремальный подход, что выражается в оправдании более ограничительных подходов к доступу к данным и их совместному использованию;
3. Переносимость данных пользователей может предоставлять пользователю как защиту, так и условия для развития риск-факторов ее взлома;
4. Ограничение оборота данных чаще подменяется понятиями «конфиденциальной информации». Однако в научных исследованиях и в сфере уже развиваются инициативы типа «данные для общественного блага».

[174] Enhancing Access to and Sharing of Data Reconciling Risks and Benefits for Data Re-use across Societies. Электронный ресурс: http://www.oecd.org/going-digital/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm (дата обращения: 11.03.2021).

[175] См. там же.

Авторы отчета в заключении отмечают потребность в структурах управления данными, которые включают общегосударственные подходы и их согласованность во всех секторах — социальных и экономических.

ОЭСР с помощью подобных проектов предпринимает важные концептуальные и аналитические попытки изучения новых аспектов развития Big data. Мы полагаем, что влияние данных концепций на международное правовое регулирование защиты персональных данных может привести к переосмыслению объекта правового регулирования (данных) и его роли в международных отношениях.

Цифровые платформы и защита данных в условиях новых концепций Big data. Ответственность интернет-компаний.

В условиях цифровой трансформации всю большую актуальность начинают приобретать цифровые платформы, которые, как известно, обладают самым большим объемом персональных данных. Цифровые платформы принадлежат крупным интернет-компаниям, представительства которых размещены по всему миру. Они находятся в социальной, игровой, экономических, цифровых сферах.

Цифровые платформы создают свои стандарты регулирования, которые прослеживаются через следующие виды документов:

- пользовательские соглашения;
- политики конфиденциальности;
- дополнительные соглашения (например, по борьбе с мошенничеством и т.д.).

Саморегулирование в сфере защиты данных — это внутрикорпоративное решение, оформленное вышеназванными документами, каждой из интернет-компаний,

принятое их внутренними органами. Данные виды документов не обсуждаются с пользователями (второй стороной), к ним возможно лишь присоединение и последующее согласие с установленными правилами.

Данные документы обладают следующими общими характерными признаками:

— *гибкость*. Нормы соглашений близки к нормам soft law, но не указывают на конкретные составы норм;

— *предоставление данных — главное условие.* Нормы соглашений содержат условия о предоставлении персональных данных пользователя взамен на конкретные услуги либо возможность их оказания;

— *трансформационные нормы без привязки*. Данные виды норм напоминают коллизионные нормы, но таковыми не являются. Они содержат отсылку к законодательству, но вместе с тем и отсылку к собственным правилам, которые также носят широкий характер;

— *учтены минимальные международные требования*. Такие компании как Facebook следуют регламенту GDPR и проводят аудит на соответствие внутренних норм данному регламенту.

Рассмотрим проблему защиты персональных данных на примере кейс-практики пользовательских соглашений интернет-компаний. Так, пользовательское соглашение с *Facebook* более точечно прописывает предмет пользовательского соглашения: персонализация работы с платформой; связь с людьми и организациями; тематические направления; поиск контента, товаров и услуг, которые могут заинтересовать; борьба с вредным поведением, защита и поддержка сообщества; использование и разработка передовых технологий для предоставления

всем людям безопасных и функциональных сервисов; исследование способов повышения качества сервисов, обеспечение единообразия и удобства различных продуктов компании Facebook.

Facebook имплементировал в свои внутренние документы такие положения GDPR, как:

1) согласие субъекта:

1.1.) пользователь должен добровольно предоставить явное, осведомленное согласие и недвусмысленно выразить его посредством четкого утвердительного действия;

1.2) человек имеет право отозвать свое согласие (пользователь должен быть явно осведомлен об этом);

1.3) согласие должно быть предоставлено лицом, достигшим возраста дееспособности, установленного в соответствующей стране-участнице, либо родителем или опекуном;

2) законные интересы:

2.1) компания или третья сторона должна иметь законные интересы при обработке персональных данных;

2.2) в случае возражения со стороны пользователя обработка данных должна быть приостановлена;

3) договорная необходимость (обрабатываемые данные должны быть необходимы для предоставления услуг и определены в договоре с субъектом).

Дополнительно следует отметить, что в документах Facebook также указано, что компания использует CRM-системы компаний, чтобы сопоставлять их с людьми в базе данных Facebook. Вышеназванный процесс используется и для создания на основе этой информации пользовательских аудиторий для рекламных кампаний.

В ходе анализа документов Facebook мы обратили внимание на условие о трансграничной передаче данных. В обязательстве по исполнению регламента GDPR Facebook указывает на отказ от применения Рамочной программы по передаче между ЕС и США. В сертификате уточняется, что при передаче данных за пределы Евро-

пейской экономической зоны Facebook придерживается правил, установленных разделом 5 GDRP.

Также при обработке данных пользователей Facebook ссылается на дополнительный документ — Политику использования данных. В вышеупомянутом документе компания указывает на типы информации, которые подлежат сбору и последующей обработке (например, контент пользователя, сообщества и связи, информация о транзакциях, информация с устройств и т.д.). В Политике также указывается на условия использования информации. Информация используется компанией для предоставления и поддержки продуктов компании и связанных сервисов.

Следует особенно выделить условие, в котором указывается на цели исследований и инноваций для общественного блага. Речь идет об использовании информации для проведения и поддержки исследований и внедрения инноваций во всех сферах общего социального обеспечения, технического прогресса, общественных интересов, здравоохранения и благополучия.

В документах цифровой платформы *LinkedIn* также содержится указание на регулирование сбора, использования и передачи персональных данных отдельной Политикой конфиденциальности[176]. В соглашении также указывается согласие пользователя с обработкой LinkedIn пользовательской информации и персональных данных. В целом обязательства в сфере защиты данных отличаются только тем, что обозначены менее точечно в отличие от сети Facebook.

Заметим, что данная сеть заблокирована по решению Роскомнадзора в России ввиду нарушения законодательства о защите персональных данных (в частности, требования об их локализации на территории РФ)[177]. Мы не будем комментировать это решение, но отметим, что

[176] https://www.linkedin.com/legal/privacy-policy

[177] См. https://rkn.gov.ru/news/rsoc/news41615.htm

данная цифровая платформа не запрашивала паспортных данных граждан либо иную информацию для функционирования аккаунта на базовых настройках. В этой связи пользовательское соглашение данной платформы не содержит каких-либо норм, закрепляющих или скрывающих информацию о реальных запросах компанией.

Аналогичные условия закреплены в политиках конфиденциальности Google и Youtube.

Исходя из вышеизложенного, можно заключить, что нормы саморегулирования содержат прямое упоминание норм GDPR, а могут не содержать таковых и регулируют обработку, сбор и использование данных с учетом собственных норм. Однако, схожесть этих норм с регламентом GDPR высокая, что позволяет сделать вывод, что интернет-компании постепенно адаптируются под международные нормы и в целом одобряют их воздействие на собственные правила и нормы в интернет-компании.

Ответственность интернет-компаний (цифровых платформ)

В науке международного права принято выделять ответственность государств, международных организаций. По нашему мнению, утверждать об ответственности государств и международных организаций в информационной сфере преждевременно, по крайней мере с практической точки зрения. А об ответственности интернет-компаний вполне возможно утверждать как в теоретическом, так и в практическом смыслах.

Вопрос ответственности интернет-компаний (цифровых платформ) за нарушение законодательства защиты персональных данных получил широкую известность с 2020 г.

В США, в Комитете по торговле Сената США обсуждались непреднамеренные последствия раздела 230, так называемого «щита ответственности», и то, как лучше всего сохранить сеть интернет в качестве «форума» для

открытого обсуждения[178]. Диалог велся между сенаторами и руководителями Facebook, Twitter, Google.

Во вводной части слушаний указывалось, что технологические платформы стали мощными арбитрами. Американская общественность получает мало информации о процессе принятия решений, когда контент модерируется, и пользователи имеют мало возможностей для обращения, когда они подвергаются цензуре или ограничениями.

Компания Twitter в ходе слушаний более подробно указала на проблему защиты данных. В частности, при модерировании контента, чтобы лучше обслуживать потребителей, важно сохранить режим конфиденциальности пользователей, которые используют онлайн-сервисы. Twitter считает, что конфиденциальность — это фундаментальное право человека, а не его привилегия. Компания предлагает множество способов, с помощью которых люди могут управлять режимом конфиденциальности на цифровой платформе. Twitter утверждает что всегда работает над повышением прозрачности, в т.ч. по вопросу о том, какие данные собираются и каким образом используется. Компания считает, что физические лица должны контролировать личные данные, которые передаются компании, и предоставляет им инструменты, которые помогут обеспечивать процесс контроля. Через аккаунт-настройки в Twitter компания дает людям возможность выбирать свои данные, которые могут иметь режим конфиденциальности.

Компания Facebook указала на то, что в рамках предоставления пользовательской информации существует и режим ответственности за распространение ложной информации. Так, в компании есть ответственность за

[178] Committee to Hold Hearing with Big Tech CEOs on Section 230. Электронный ресурс: https:// www.com merce.senate.go v/2020/10 /committee-to-hold-hearing-with-big-tech-ceos-on-section-230 (дата обращения: 11.03.2021 г.). См. там же.

распространение информации, подрывающей выборы, информации о насилии, а также за взломы аккаунтов и использование персональной информации. Эти механизмы позволяют устранить угрозы постоянных судебных разбирательств, с которыми можно столкнуться.

Вышеназванные сетевые слушания являются первыми в истории, когда интернет-компании и государство (США) смогли обсудить вопросы ответственности за защиту персональных данных.

Подобная активность в отношении привлечения интернет-компаний к ответственности в части исполнения законодательства о защите персональных данных не является уникальной. В Австралии, России и странах Европейского союза активно практикуются способы применения национального законодательства и привлечения к ответственности в сфере защиты персональных данных[179].

Ответственность интернет-компаний на международном уровне как перспективное направление в сфере обеспечениязащиты персональных данных

На международном уровне можно наблюдать активность Еврокомиссии, которая активно выпускает документы о нарушении антимонопольного законодательства интернет-компаниями. Подобные нарушения тесно связаны и с защитой персональных данных, так как доминирующее положение той или иной компании на рынке тесным образом связано с персональными данными пользователей и их распределением между рекламными и иными сервисами. Это позволяет крупным интернет-компаниям разнообразить предоставляемые услуги пользователям и расширить свою аудиторию (таргетинг).

[179] Кейс Австралии см. https://www.accc.gov.au/media-release/accc-alleges-facebook-misled-consumers-when-promoting-app-to-protect-users-data; кейс России см. https://rkn.gov.ru/news/rsoc/news71720.htm.

Приведем в качестве примера штраф, наложенный на компанию Google Еврокомиссией за нарушение антимонопольного законодательства ЕС и злоупотребление доминирующим положением на рынке интернет-рекламы[180]. При помощи посреднической деятельности в поисковой рекламе компания фактически считывала всю пользовательскую информацию о поисковых запросах, о конкретном пользователе, который вводил запрос. Это позволяло компании предоставлять рекламу по конкретному запросу.

Вопросы защиты персональных данных чаще связывают именно с антимонопольным законодательством на международном уровне. Это можно объяснить следующими причинами:

а) для инициирования того или иного обвинения требуется отразить больший «эффект ущерба» для социальной и экономической сферы и подчеркнуть глобальный характер;

б) защита персональных данных может рассматриваться в пределах антимонопольного законодательства, так как вопрос передачи данных может содержать экономический эффект. Экономический эффект может выражаться в усилении доминирующего положения на цифровом рынке.

Выводы

Исходя из анализа изложенных выше изменений, мы предлагаем следующие тезисы:

1. Саморегулирование интернет-компаний (цифровых платформ) и международные стандарты должны иметь больше точек соприкосновения в правовом регулировании защиты персональных данных. Это позволит

[180] Antitrust: Commission sends Statement of Objections to Google on comparison shopping service; opens separate formal investigation on Android Brussels, 15 April 2015. Электронный ресурс: https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4780 (дата обращения: 11.03.2021).

сформировать более эффективную систему защиты персональных данных. Можно использовать опыт применения и имплементации регламента GDPR.

2. Необходимо научно-аналитическое сопровождение концепции «общедоступных данных» с привлечением интернет-компаний к обсуждению и участию. Опыт интернет-компаний в регулировании персональных данных может быть полезен для проработки международно-правовых универсальных механизмов защиты персональных данных.

3. На организационно-административном уровне важно обеспечить международно-правовой универсальный диалог между цифровыми платформами и международными организациями для реализации концепций защиты и использования персональных данных. Это возможно реализовать на уровне международной конференции либо иной международной площадки.

4. Модель международных сетевых слушаний может стать удобным инструментом для рассмотрения дел, связанных с защитой персональных данных. Безусловно, при постановке такого тезиса возникнет вопрос о классической теории субъектов международного права. При ответе на данное замечание мы напомним о роли интернет-компаний и их внутренней саморегулируемой основе защиты персональных данных. В этой связи, полагаем, что первостепенным является практическая польза международного права и использование его возможностей для урегулирования споров, связанных с защитой персональных данных интернет-компаниями и государствами.

Вместе с вышеназванными практическими и административными рекомендациями следует особое внимание обратить на научные подходы к вопросу защиты персональных данных. Дело в том, что в теории международного права необходимо усилить внимание к междисциплинарным подходам, особенно, в сфере

информационной и кибербезопасности. Например, существует наука о данных[181], которая отдельно рассматривает методы обработки данных, исследует процесс обработки и использования данных.

Основы данной науки могут помочь сформировать прикладной инструментарий для собственно международно-правовых подходов к проблемам, одновременно создавая эмпирический материал для правового регулирования. Наука о данных включает в себя следующие направления: машинное обучение, коммуникации, экспертный опыт в предметной сфере, этику и регулирование использования данных, очистку данных, базы данных, компьютерные науки и высокопроизводительные вычисления, визуализация данных, статистика и оценка вероятности. Эмпирический материал необходим для более тонкого понимания процесса работы с данными, их передачи и алгоритмов действий с ними.

В этой связи важно получить новый материал как с позиции практической, так и с позиции теоретической для исследования перспектив защиты данных на цифровых платформах. На наш взгляд, исключительно в подобных условиях может формироваться грамотная практическая и теоретическая позиция в сфере защиты персональных данных на международном уровне в условиях новых вызовов Big data.

Библиографический список

1. *Сибел Т.* Цифровая трансформация. Как выжить и преуспеть в новую эпоху — М.: Изд-во Манн, Иванов и Фербер.2021 г.
2. *Келлехер Джон, Тирни Брендан* Наука о данных.— М.: Альпина паблишер. 2020.
3. *Jowett, Benjamin*, trans., The Republic of Plato: An Ideal Commonwealth. New York: Colonial Press,1901.

[181] Келлехер Джон, Тирни Брендан Наука о данных.— М.: Альпина паблишер. 2020 г. С. 13–22.

ПРАВО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

GNERRE Orazio Maria
PhD Student, University of Perugia, Piazza Università, 1, 06123, Perugia, Italy, oraziomaria.gnerre@studenti.unipg.it

NEUTRALIZATION, TECHNOLOGY, ALGORITHM: REFLECTING ON ARTIFICIAL INTELLIGENCE STARTING FROM CARL SCHMITT

Abstract: *Carl Schmitt's contribution to the study of law is of great proportions, especially since his approach to the subject has always been hybridized with the great themes of politics and technical development. This is why his work is still relevant today, and can be applied, as this essay does, to the question of the development of artificial intelligence and its practical applications. The essay therefore proposes to trace, through an immersion in Schmitt's thought, an examination of the problem of artificial intelligence in the face of matters of law.*

Keywords: *Carl Schmitt; Artificial intelligence; Philosophy of Technology; Philosophy of Law; Neutralizations.*

Introduction

Carl Schmitt is an author who was rightly considered an anticipator. Anticipator, because he was able to see within the historical period in which he lived — undoubtedly a crucial period — all those trends that then developed, and are still developing. Carl Schmitt also had a taste for great forecasts himself, which he emphasized in personalities that he explored in depth such as Donoso Cortés and Alexis de Tocqueville. If in Donoso Cortés he traced the awareness of the political potential of Russia, which he foresaw would first