Научная статья
УДК: 347
DOI: 10.17323/tis.2023.17800

Original article

# РЕСТРУКТУРИРОВАННАЯ ИНФОРМАЦИЯ И КОНТЕНТ В ГРАЖДАНСКОМ ОБОРОТЕ

# RESTRUCTURED INFORMATION AND CONTENT INVOLVEMENT INTO CIVIL TURNOVER

**Владимир Львович ЭНТИН**
МГИМО (У) МИД РФ, Центр правовой защиты интеллектуальной собственности, Москва, Российская Федерация,
entin@klishin.ru,
ORCID: 0009-0002-7331-9728

Информация об авторе
В.Л. Энтин — директор некоммерческого фонда «Центр правовой защиты интеллектуальной собственности», адвокат, доцент МГИМО (У) МИД РФ, кандидат юридических наук, член-корреспондент Международной академии сравнительного права (Франция), ассоциированный член Кафедры ЮНЕСКО НИУ ВШЭ

Аннотация. Авторское право и смежные права регулируют гражданский оборот информации, которая приобретает структурированный характер в результате интеллектуальной деятельности. Структурированная информация, которая обрабатывается в автоматическом режиме, если она не описана в терминах права интеллектуальной собственности, оказывается вне сферы его действия. Структурированная информация, в отношении которой могут быть предъявлены требования в связи с владением, пользованием или распоряжением ею, охраняется правом. Ее коммерческое использование получает моральную и юридическую оценку. Когда информация обезличена, моральная и юридическая оценки расходятся. Объекты авторских и смежных прав, независимо от того, охраняются имущественные права на них или нет, обезличиваются собирательным термином «контент». Размещение контента в интернете делает возможным его переработку без ведома правообладателя. Последствия такой переработки для создания результатов интеллектуальной деятельности естественным или искусственным интеллектом оцениваются правом. Примитивное присвоение осуждается правом и моралью. Присвоение через творческую переработку, агрегирование информации и майнинг — нет. Параллельно складываются универсальные тренды регулирования хранения и передачи личной информации, куда нередко попадают и «фейки».

Слабости технического контроля над интернет-пространством государства стремятся компенсировать юридическими средствами. Усиливается регуляторный надзор. Ужесточается ответственность за несоблюдение административных предписаний. Расширение зон регулирования информации сопровождается разработкой специализированного правового аппарата, позволяющего вовлекать в гражданский оборот различные элементы информационного пространства.

Ключевые слова: присвоение информации, информационные пузыри, конкуренция регуляторов, фрагментация информационного пространства

Для цитирования: *Энтин В.Л.* Реструктурированная информация и контент в гражданском обороте // Труды по интеллектуальной собственности (Works on Intellectual Property). 2023. Т. 46, № 3. С. 29–37;
DOI: 10.17323/tis.2023.17800

**Vladimir L. ENTIN**
MGIMO (U) of the Russian Federation Ministry of Foreign Affairs, Nonprofit Foundation "Centre for Intellectual Property Legal Protection", Moscow, Russian Federation,
entin@klishin.ru,
ORCID: 0009-0002-7331-9728

Information about the author
V.L. Entin — Associate Professor of MGIMO (U), director of the Foundation, Associate Member of the International Academy of Comparative Law (France), Associate Fellow of the UNESCO Chair at HSE University, Candidate of Legal Sciences

Abstract. Copyright and Related rights are designed to regulate civil turnover of the information that have been restructured by the intellectual activity. Structured information that is processed automatically and fails to be described in intellectual property terms find itself outside intellectual property law. Legal protection is extended to the information that can be submitted to the legal claims of ownership, use and disposal. Commercial use of that information receives legal and moral assessment. When the information is depersonalized, moral and legal judgments drift apart. The objects protected by copyright and by related rights are depersonalized when they are indiscriminately treated as content. Being displayed online they are vulnerable to processing without the knowledge of the right holders. The attitude towards such a processing committed by human or artificial intellect is legally the same. Primitive appropriation is legally and morally condemned. The attitude towards creative adaptation, appropriation of the aggregated information or of the results of mining is much more tolerant. We are witnessing universal trends of dealing with personal information that is far from fake proof. The flaws of technical control over Internet states try to compensate by legal remedies. Regulators' supervision is stepped up. The liability for administrative noncompliance becomes harsher. The scope of information regulation extension is accompanied by legal constructions development aimed at the involvement of different information elements into civil turn over.

Keywords: appropriation of information; information bubbles; regulators rivalry; information space fragmentation

For citation: *Entin V.L.* Restructured Information and Content Involvement into Civil Turnover // Trudi po Intellectualnoy Sobstvennosti (Works on Intellectual Property). 2023. Vol. 46 (3) P. 29–37; DOI: 10.17323/tis.2023.17800

Информация сродни солнечному излучению. Она пронизывает все, создавая ноосферу, но лишь ее небольшую часть люди используют осознанно, как и в случае с солнечным излучением. Эксплуатация информации в значительной мере ограничивается относительно примитивными способами: ее добычей, накоплением, присвоением, ограничением доступа к ней и ее распространением или сокрытием.

## ПРОТИВОПРАВНЫЙ ПРИМИТИВИЗМ

Примитивным способом присвоения информации является плагиат. Рассмотрим это явление на конкретном примере. В конце 2022 г. организаторы Фестиваля короткометражных фильмов в городе Клермонт-Ферранд, Франция [1], получили для участия в Фестивале рисованный мультипликационный фильм «Away From Home» («Вдали от дома»). Этот фильм воспроизвел один к одному короткометражный фильм Натальи Чернышевой «Снежинка», произведенный ООО «СТУДИЯ ПЧЕЛА» в 2012 г. и уже получивший к тому моменту много наград.

Единственная разница между двумя фильмами состояла в том, что в титрах режиссером и продюсером была указана гражданка Италии Брунелла Де Кола (Brunella De Cola). Информационно фильмы совпадали, но юридически между ними была огромная разница.

Во-первых, было нарушено законодательство об авторском праве и осуществлен ввоз контрафактной продукции. Так как фильм был ввезен на территорию Франции, нарушения должны квалифицироваться в соответствии с Кодексом интеллектуальной собственности Франции.

Во-вторых, Брунелла Де Кола совершила акт плагиата оригинального фильма «Снежинка», то есть осуществила противозаконное воспроизведение фильма полностью без согласия автора и обладателя авторских прав, а также произвела трансформацию фильма, заменив титры, хотя такие действия запрещены Кодексом интеллектуальной собственности Французской республики [2].

В-третьих, в отношении анимационного фильма «Снежинка» Брунелла Де Кола выполнила следующие действия:

- заменила оригинальное название фильма, переименовав его на «Away From Home»;
- заменила титры оригинального фильма;
- поместила в титры себя в качестве режиссера фильма и продюсера;
- сняла указания на то, что авторские права на фильм принадлежат ООО «СТУДИЯ "ПЧЕЛА"», обнародовавшему фильм в 2012 г.

В-четвертых, все указанные действия были совершены без согласия авторов фильма и правообладателей с нарушением авторских прав Натальи Чернышевой как создателя фильма и исключительных прав правообладателя — ООО «СТУДИЯ "ПЧЕЛА"». Такие действия нарушают авторские права, принадлежащие режиссеру и студии [2]. Действия по использование произведения, полученного в результате нарушения прав авторов и правообладателей, квалифицируются французским правом как контрафакт. По законодательству Франции контрафактным считается «всякое воспроизведение, публичный показ или распространение любыми средствами произведения в нарушение прав автора, как они установлены законом» [3].

Направив фильм «Away From Home» различным дистрибьюторам, нанятым для продвижения фильма на фестивалях короткометражных и анимационных фильмов, Брунелла Де Кола совершила действия по изготовлению и организации распространения контрафактного продукта.

Данный пример показывает, как применение недозволенных способов присвоения информации ведет к основному юридически значимому делению участвующей в гражданском обороте информации на законную и противозаконную, исходя из юридической квалификации действий, приведших к ее появлению.

С необходимостью отсеивания способов превращения информации в интеллектуальную собственность сталкиваются все отрасли права. Тем не менее многие области использования информации оказываются в «ничейной» зоне.

## РАСШИРЕНИЕ ЗОН ПРАВОВОГО РЕГУЛИРОВАНИЯ

Долгое время агрегирование накопленной информации в целях ее последующего использования в агрегированном виде оставалось вне зоны правового регулирования. Легитимация правового регулирования накопленной информации обосновывалась необходимостью обеспечить сохранность чувствительной информации личного характера от ее несанкционированного использования и разглашения.

Персональная информация имеет своего рода антиматерию в виде фейков. Правовое регулирование сталкивается с необходимостью решения двуединой задачи — защиты персональной информации и противостояния ее антиподу. Защита публичного интереса обеспечивается главным образом с помощью многочисленных карательных санкций, а исправление дефектной информации, нарушающей права гражданина, зависит от него самого и эффективности специально созданных бюрократических структур. То есть на юридическом уровне, с позиций равенства возможностей, проблема не сбалансирована.

Стремительное распространение основанной на домыслах и предположениях информации, которую поисковики и социальные сети разносят по интернету, привело к разработке правового инструментария, позволяющего бороться с информационными подделками, которые называют фейками. Проблема состоит в том, что фейки изготавливаются в промышленных масштабах. Они нередко укореняются в публичных институтах, тогда как бремя борьбы с ними возлагается на индивида в личном качестве.

Человек, оказавшийся в ситуации, когда о нем распространяются фейки, становится жертвой бьющей по площадям техники массированного информационного воздействия в разных направлениях:

а) внутри «информационных пузырей», когда всем окружающим персонально скармливаются поступающие из одного и того же источника подборки событий, информации, вычленяемые алгоритмом на основе предпочтений получателя. Технология надувания «информационных пузырей» основывается на том, что люди склонны получать информацию из ограниченной группы источников, которые считают заслуживающими доверия, поэтому исходящая от них информация оценивается ими некритически как правдивая с высокой степенью вероятности. Например, в Европе представления о злокозненности всех, кто хоть как-то связан с Россией, получают статус факта, укореняясь в силу их многократного повторения в политическом дискурсе;

б) неумышленные фейки или так называемые личные мнения о человеке, без прямого умысла манипулировать общественным мнением;

в) целенаправленные фейки, или множители, делающие любую оценку, какой бы вздорной она ни была, известной огромному числу людей. Это техника создания так называемого информационного шума, который гасит здравый смысл. Информационный шум многократно усиливается, когда в качестве множителя используется отрицательная репутация страны происхождения;

г) направленная дезинформация, или операция влияния, — коммерчески или политически мотивированная стратегия управления информационным пространством.

Юридические средства ограждения граждан ЕС от поддельных новостей (fake news) являются одним из рекомендуемых направлений законодательной политики Комиссии ЕС [4].

## ВОЗВРАЩЕНИЕ СУВЕРЕНИТЕТА НАД ИНФОРМАЦИОННЫМ ПРОСТРАНСТВОМ

Для мобилизации общественного мнения против чрезмерного могущества GAFA (под этой аббревиатурой понимается олигополия Google, Amazon, Facebook, Apple — четырех американских онлайн-платформ, которые вместе с Microsoft заняли господствующие позиции в киберпространстве), а также для преодоления сопротивления тех, кто по различным идеологическим основаниям выступает против правового регулирования в интернете, было разработано и принято несколько нормативных актов Европейского союза, развернувших правовое регулирование и правоприменительную практику в отношении крупнейших и экономически успешных онлайн-платформ в сторону активного государственного вмешательства.

Говоря об инструментах возвращения суверенитета в киберпространстве, мы имеем в виду прежде всего следующие нормативные документы:

1) Регламент ЕС 2016/679 от 27 апреля 2016 г. «О защите физических лиц в отношении обработки персональных данных и свободы движения таких данных и отмене Директивы 95/46 ЕС» (Общий регламент защиты данных, англоязычная аббревиатура — GDPR) [5];

2) Регламент ЕС 2018/1725 от 23 октября 2018 г. «О защите физических лиц в отношении обработки их персональных данных ведомствами, агентствами, учреждениями и юридическими лицами и свободного движения таких данных, отмена Регламента № 45/2001» и Решение комиссии ЕС № 1247/2002 [6].

Регламенты действуют на территории ЕС и стран Европейской ассоциации свободной торговли (ЕАСТ). Они служат правовой основой для действий против злоупотребления поисковиками и социальными сетями своими возможностями по фильтрации информационных потоков в сети, а также регулированию доступа к информации безотносительно к ее ценности или полезности.

Избранная правовая форма «регламент» превращает эти документы в акты прямого действия. Это означает, что при обращении в суд за защитой нарушенного права можно ссылаться на закрепленные в регламентах принципы, правовые позиции и нормы, независимо от их имплементации в национальное законодательство государств-членов. Кроме того, эти регламенты подстегнули национальное нормотворчество в сторону усиления административного давления и увеличения штрафных санкций в случае несоблюдения положений регламентов.

Официально прокламируемой целью заявленных мер является повышение защищенности граждан ЕС от негативной информации, становящейся доступной благодаря размещению ее на общедоступных интернет-сайтах, с помощью законодательных мер, направленных на возвращение физическим лицам статуса субъекта информационного процесса.

В силу ст. 18 (бывшая ст. 12 Договора о Европейском сообществе) запрещается какая-либо дискриминация на основе гражданства [7], а ст. 19 (бывшая ст. 13 Договора о Европейском сообществе) особо запрещает какую-либо дискриминацию по причине расового или этнического происхождения [8]. Эти основополагающие положения могут быть использованы для оспаривания бездействия со стороны уполномоченных органов ЕС в случае игнорирования или неисполнения обязанностей, возложенных на них правом ЕС, если связать такое бездействие с тем обстоятельством, что гражданство является приобретенным, а не полученным в силу рождения.

В Регламенте ЕС 2016/679 [5] подчеркивается, что защита физических лиц в отношении обработки персональных данных является фундаментальным правом. Статья 8(1) Хартии Европейского союза об основных правах [9] и статья 16(1) Договора о функционировании Европейского союза (ДФЕС) [10] предусматривают, что каждый имеет право на защиту своих персональных данных. К основополагающим принципам относится положение, согласно которому *«принципы и правила защиты физических лиц в отношении обработки их персональных данных должны, независимо от гражданства или места жительства лиц, уважать их фундаментальные права и свободы, в частности их право на защиту персональных данных. Настоящий Регламент призван содействовать формированию свободного, безопасного, справедливого пространства, а также общего экономического пространства; содействовать созданию единого экономического пространства, а также экономическому и социальному развитию, укреплению и сближению экономик на внутреннем рынке, содействовать благосостоянию физических лиц»*.

В соответствии с приведенными выше регламентами специальные информационные права и средства их защиты действуют только применительно к обработке и распространению информации о персональных данных физических лиц — граждан ЕС. В результате происходит дробление всей персональной информации, аккумулированной на территории ЕС и стран Европейского экономического пространства, на три категории:

1) охраняемую правом ЕС;

2) охраняемую в силу соглашения между ЕС и третьими странами;

3) охраняемую в силу договора (согласия) на использование информации.

Положения о защите данных применяются к лицам, чьи персональные данные обрабатываются в любом контексте. Они неприменимы к умершим. Они не распространяются на юридических лиц.

Защита персональных данных распространяется на обработку личных данных полностью или частично в автоматическом режиме путем заполнения формуляров. Она распространяется на отдельные файлы или подборки файлов и их титульные страницы, структурированные по конкретным критериям.

Бремя доказывания существования превалирующего публичного интереса, деактивирующего охрану интересов, конституционных прав и свобод субъекта персональных данных, возложено на лицо, действующее в общественных интересах и осуществляющее свои официальные полномочия.

Каждый, чьи личные данные обрабатываются, должен иметь право подать жалобу Европейскому инспектору по защите данных (European Data Protection Supervisor) и пользоваться правом на эффективную судебную защиту в Суде справедливости ЕС, если субъект таких данных полагает, что: а) принадлежащие ему/ей права в соответствии с регламентом нарушены; б) Европейский инспектор по защите данных не отреагировал на жалобу, частично или полностью отклонил ее либо не действовал в том случае, когда действия были необходимы для защиты прав подателя жалобы. Обращение с жалобой требует проведения расследования в той мере, в какой это необходимо в конкретных обстоятельствах, а его результаты могут быть пересмотрены в судебном порядке.

Для упрощения подачи жалобы Европейский инспектор по защите данных должен предоставить формуляр подачи жалобы, который может быть заполнен в электронном виде, что не исключает использования других средств коммуникации.

На Европейского инспектора по защите данных возлагается обязанность осуществлять мониторинг применения положений Регламента ко всем процедурам обработки информации, выполняемым ведомствами и учреждениями ЕС.

В ст. 3 Регламента 2018/1725 [11] даны определения, которые стали общими для права ЕС и права государств-членов.

В п. 1 персональные данные определяются как *«любая информация, относящаяся к названному или идентифицируемому физическому лицу (субъекту данных). Идентифицируемым физическим лицом считается тот, кто может быть идентифицирован прямо или косвенно благодаря наличию идентификаторов. Ими служат: фамилия, идентификационный номер, местонахождение, онлайн-идентификатор, а также информация об особенностях физического, физиологического, генетического, ментального, экономического, культурного или социального характера, которые позволяют идентифицировать физическое лицо»*.

На управленческие структуры, получившие личные данные, возлагаются полномочия, обременения и ответственность, предусмотренные Регламентом. К ним применяется правовой режим «контроллера» (Controller) персональных данных. В силу подп. 8 ст. 3 Регламента [11] контроллером выступает любое ведомство, учреждение или организационная единица ЕС, которая самостоятельно или в сотрудничестве с другими определяет цели и способы обработки персональных данных; когда такие цели и способы определены в конкретном акте Союза, контроллер или критерии для его назначения определяются правом ЕС.

«Обработчик» в рамках контракта с контроллером решает, какие компьютерные программы будут использованы для обработки и хранения персональных данных, предоставленных контроллером.

Пункт 16 (ст. 12 GDPR) определяет, что «нарушение в отношении персональных данных» (personal data breach) означает нарушение, которое привело к случайному или незаконному уничтожению, потере, изменению, несанкционированному разглашению, доступу к персональным данным, переданным, хранящимся или иным образом обрабатываемым.

В ст. 4 Регламента 2018/1725 [11] перечислены принципы, которые должны быть положены в основу обработки персональных данных. Они должны обрабатываться на законных основаниях, справедливо и прозрачно для субъекта данных.

Сбор персональных данных должен осуществляться для достижения конкретных, четких и законных целей. Характер обработки и сроков хранения должен им соответствовать. Подпункт «d», касающийся требования точности, предусматривает принятие всех разумных мер, чтобы персональные данные, являющиеся неточными с точки зрения целей, для которых они обрабатываются, стирались или исправлялись незамедлительно.

Статья 10 касается обработки специальных категорий персональных данных. В п. 1 содержится общий запрет на обработку персональных данных, раскрывающих расовую или этническую принадлежность, политические взгляды, религиозные или философские убеждения, членство в профсоюзах. Обработка генетических данных, биометрических данных в целях идентификации физических лиц, данных о здоровье

или о сексуальной жизни или ориентации также запрещена. В п. 2 в подп. a–j перечислены случаи, когда приведенный выше запрет не применяется. Когда такие данные обрабатываются в режиме исключения, в отношении них должен соблюдаться режим конфиденциальности и ограниченного доступа.

Статья 11 устанавливает дополнительные требования к обработке персональных данных, относящихся к обвинительным приговорам по уголовным делам и другим правонарушениям. Обработка таких данных, а также данных, относящихся к мерам безопасности, должна осуществляться только под контролем официальных властей либо, когда их обработка разрешается правом Союза, при условии предоставления соответствующих гарантий прав и свобод субъектов персональных данных.

Статья 16 наделяет субъекта персональных данных правом на получение информации в тех случаях, когда персональные данные были получены не от субъекта. Когда персональные данные получены не от субъекта, на контроллера возлагаются следующие обязанности:

1) предоставить субъекту исходные данные:

a) наименование и контактные данные контроллера;

б) контактные данные должностного лица, отвечающего за охрану данных;

c) цели и правовые основания обработки данных;

d) категории данных, подлежащих обработке;

e) реципиенты данных;

f) намерение передать данные реципиенту в третьей стране;

2) сообщить субъекту:

a) сроки хранения данных, а если это нельзя сделать, то критерии, которыми указанные сроки будут определяться;

b) о его праве на обращение к контроллеру с просьбой о доступе, внесении исправлений или удалении персональных данных либо ограничении их обработки;

…

d) о его праве подать жалобу Европейскому инспектору по защите данных;

e) из какого источника происходят эти персональные данные и поступили ли они из общедоступных источников.

Всю эту информацию контроллер должен предоставить в разумный срок, но не позднее месяца после обращения.

Статья 17 наделяет субъекта персональных данных правом доступа к тому, какая личная информация о нем перерабатывается или хранится, с полномочиями, аналогичными тем, что предусмотрены в ст. 16.

Статья 18 предоставляет субъекту данных право требовать от контроллера исправления без неоправданных задержек неточной информации личного характера. На основании целей обработки персональных данных оно включает в себя право дополнять неполную информацию, в том числе путем направления заявления о дополнении.

Статья 19 закрепляет право на удаление (право на забвение). Согласно этой статье субъект персональных данных должен иметь право требовать от контроллера удаления своих персональных данных без неоправданных задержек при наличии одного из следующих оснований:

a) личные данные более не являются необходимыми для тех целей, для которых они были собраны;

b) субъект персональных данных отозвал свое согласие на их обработку, а других правовых оснований для такой обработки нет;

c) субъект персональных данных возражает против их обработки в связи с его особой ситуацией, а превалирующий публичный интерес отсутствует;

d) персональные данные обрабатываются незаконно;

e) персональные данные должны быть устранены во исполнение правовых предписаний, которым контроллер обязан подчиниться;

f) персональные данные были собраны в связи с предложением, поступившим от провайдера информационных услуг, в обстоятельствах, предусмотренных ст. 8 (1), где говорится об использовании личных данных ребенка.

Когда контроллер сделал персональные данные публичными и обязан в силу указанных выше положений удалить персональные данные, он с учетом имеющихся технических возможностей и стоимости исполнения обязан предпринять разумные шаги по уведомлению иных контроллеров, нежели ведомства и учреждения ЕС, которые занимаются обработкой персональных данных, о том, что субъект данных обратился с просьбой убрать все ссылки на них, их копии или реплики.

Указанные положения не должны применяться в той мере, в какой обработка персональных данных необходима для следующего:

a) осуществления права на свободу слова и информации;

b) выполнения обязательств, вытекающих из требований закона, которым подчиняется контроллер, либо для решения задач, выполняемых им в общественных интересах или при осуществлении возложенных на контроллера властных полномочий;

c) охраны публичных интересов в сфере здравоохранения;

d) достижения общественно полезных целей в области научных, исторических исследований или в области статистики, когда осуществление права на забвение сделает их проведение невозможным или серьезно им помешает;

e) установления, осуществления или защиты правовых требований.

Приведенный выше перечень показывает зарождение нового поколения прав человека, которые будут все более востребованными по мере становления метавселенной и возникновения присущих ей информационных прав.

## ДРОБЛЕНИЕ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА НА СЕКТОРА С УВЕЛИЧЕНИЕМ ЧИСЛА РЕГУЛЯТОРОВ

Принятие 14 декабря 2022 г. новой Директивы о кибербезопасности [12], направленной на повышение защищенности критических инфраструктур в ЕС, усиливает регуляторный надзор и правовой механизм принуждения к выполнению требований кибербезопасности в соответствии с более высокими стандартами применительно к деятельности широкого спектра компаний и правительственных учреждений.

Директива предусматривает единообразную процедуру реагирования на инциденты в области безопасности, задает стандарты соблюдения информационной безопасности в цепочках поставок, шифрования и выявления уязвимостей. Новые требования будут распространяться на инфраструктурные объекты в области энергетики, транспорта, банковского дела, здравоохранения, космической отрасли, цифровой инфраструктуры государственной администрации, пищевой промышленности, медицинских изделий, автомобилей, переработки мусора и канализации, почтовой службы, химической промышленности и поставки комплектующих, используемых в электронике. В Европарламенте полагают, что новые требования затронут 160 тыс. организаций на территории ЕС.

Регулирование вопросов, связанных с информацией, распадается на дискретные области. Каждая из них регулируется самостоятельно в соответствии с ее полезностью, известной на момент издания нормативного акта. Латентные свойства информации не могут являться объектом регулирования, что ведет к необходимости периодического обновления регуляторной ткани и корректировки полномочий регуляторов.

При этом все в большей степени проявляет себя конкуренция между регуляторами. Для стран романо-германской правовой семьи характерна обязательная инкорпорация в контракты между хозяйствующими субъектами стандартных предписаний (standard contractual clauses, SCCs), действующих в данной сфере. В условиях, когда наряду с национальным законодательством действует интеграционное право, учащается обновление стандартных положений как проявление конкуренции между национальными регуляторами и Комиссией ЕС.

Предприятиям и публичным учреждениям, пользовавшимся предшествующими стандартными предписаниями, автоматически включаемыми в хозяйственные договоры, чтобы выполнить требования законодательства о защите персональных данных, необходимо было учесть новые обновления стандартных положений ЕС до 27 декабря 2022 г. Пропуск этого срока влечет штрафные санкции. Это обусловлено тем, что новые стандарты соответствия касаются главным образом передачи персональных данных за пределы ЕС.

## ОТГОРАЖИВАНИЕ ОТ ФИЗИЧЕСКИХ И ЮРИДИЧЕСКИХ ЛИЦ ИНЫХ ЮРИСДИКЦИЙ С ПОМОЩЬЮ ПОНЯТИЙНОГО АППАРАТА, СВОЙСТВЕННОГО ТОЛЬКО ПРАВУ ЕС

В русле постепенной федерализации Европейского Союза Комиссия ЕС выступила с проектом регламента о создании Общеевропейского пространства данных здравоохранения [13]. Его необходимость обосновывается потребностью предусмотреть возможность доступа граждан к данным, касающимся их здоровья (первоначальное использование), а также облегчить повторное использование таких данных в социальных целях на территории ЕС (вторичное использование).

Проект регламента может легко затеряться в лабиринте законодательных предложений, регулирующих использование данных, которые исходят от Комиссии ЕС. Однако именно в сфере здравоохранения, где идея широкой доступности данных пользуется поддержкой напуганного ковидом населения, прорабатываются механизмы ускоренного получения принудительных лицензий. Общеевропейское пространство данных здравоохранения предусматривает упрощенный режим принудительного лицензирования данных здравоохранения в пользу третьих лиц. От бизнеса это потребует дополнительных усилий по защите прав интеллектуальной собственности на данные медицинского характера и их сортировке по назначению и степени доступности. Это касается в первую очередь права доступа к информации о состоянии здоровья, хранящейся в электронном виде, и степени контроля над повторным использованием собранных данных в дополнение к субъективным правам в отношении персональной информации, предус-

мотренным Директивой ЕС о защите персональных данных (GDPR) [5].

Регламент требует, чтобы организации, занимающиеся хранением и обработкой данных о здоровье, обеспечили операционную совместимость используемых систем, а также выполнение требований безопасности, предъявляемых к электронным документам. Европейской комиссии будут выделены средства на создание интернет-платформы MyHealth@EU, обеспечивающей трансграничный обмен данными о здоровье на территории ЕС. Хозяйствующие субъекты, включая изготовителей, импортеров и дистрибьюторов систем электронного хранения информации о здоровье, должны будут нанести соответствующую маркировку ЕС в подтверждение соблюдения технических требований регламента.

Общеевропейское пространство данных о здоровье EHDS создает техническую и правовую основу для доступа академических учреждений, бизнеса, политиков и регуляторов к обезличенным данным о здоровье непосредственно от организаций, хранящих данные о здоровье, или через посредство учреждения, обеспечивающего доступ к данным о здоровье, которое должно быть создано во всех государствах-членах. Для повторного использования данных о здоровье потребуются получение разрешения и оплата сбора в зависимости от вида использования.

## ДАННЫЕ КАК АКТИВ, КОТОРЫМ НИКТО НЕ ДЕЛИТСЯ БЕСПЛАТНО

Специалисты практически единодушны в том, что важными драйверами многих сделок слияния и поглощения являются коммерческая ценность информации и перспективы реструктурирования ее использования и лицензирования. Данные как актив обычно рассматриваются с нескольких позиций:

- в частном секторе учитывается полезность или степень коммерческой ценности данных (например, когда речь идет о клиентской или пользовательской базе, оцениваемой исходя из числа обращений или пользователей);
- в публичном секторе регулируется доступность данных, что позволяет повысить эффективность управленческих решений публичных властей и бизнеса, чего нельзя добиться в рамках узкоотраслевого дробления информации. Обычно приводят пример Нью-Йорка, где расширение доступности данных, собираемых офисом мэра города (NY Open Data), позволило существенно сократить время ожидания медицинской помощи;
- обладание данными создает риски привлечения к ответственности по разным основаниям. Утечка данных может нанести имущественный ущерб в виде потери ценного акта, вызвать применение штрафных санкций со стороны регулятора, привести к нарушению контрактных обязательств, вызвать недоверие имеющихся и потенциальных клиентов, нанести репутационный ущерб;
- в зависимости от используемых режимов обеспечения безопасности данных информация может охраняться как конфиденциальная, служебная и даже государственная тайна, секрет производства, коммерческая тайна, что предопределяет возможности и пределы ее использования в гражданском обороте. Сбор и организация данных коммерческого характера приведут к появлению баз данных, коммерческой тайны, где использование хранимой информации варьируется в зависимости от особенностей национального законодательства, а также контрактных ограничителей доступа и условий использования;
- повышенные сложности вызывает обращение с носителями персональной информации, стандарты требований к условиям хранения и передачи их для обработки третьим лицам меняются так часто, что административная отчетность по ним ложится бременем на бизнес, который включает его в цену товаров и услуг;
- борьба за контроль над некоторыми видами чувствительных данных может спровоцировать расследования антимонопольных органов, призванных пресекать злоупотребление доминирующим положением на рынке.

В сделках слияния и поглощения соблюдение требований относительно безопасного хранения, использования и передачи персональных данных третьим лицам, резидентам и нерезидентам ЕС и ЕАЭС соответственно может обернуться головной болью. Быстро развивается такое направление деятельности, как аутсорсинг проверки соблюдения требований и ограничений, предъявляемых к работе с чувствительными данными, в рамках процедуры должной предусмотрительности (due diligence). В этой связи возникают вопросы достаточности контрактных средств предосторожности, таких как:

- требование возмещения штрафов, наложенных регулятором за несоблюдение регламентных или контрактных условий обработки информации;
- аудит интеллектуальных прав в связи со сбором и использованием информации;
- требование предоставления лицензии на производные произведения, патентоспособные усовершенствования, дизайнерские решения, то есть перекрестного лицензирования охраняемых результатов интеллектуальной деятельности;

- включение условий, связанных с используемыми алгоритмами, и права собственности на результаты, полученные благодаря применению искусственного интеллекта;
- соблюдение требований этики и санкционных ограничений.

Неясным остается вопрос, в какой мере страхование рисков, связанных с профессиональной деятельностью, распространяется на собственную и сопутствующую деятельность по производству и обработке расширяющегося потока информации. Хозяйствующие субъекты беспомощно барахтаются в информационном потоке, надеясь, что юристы и страховщики позволят им справиться с этой напастью с минимальными издержками. В результате фрагментация информационного пространства на автономные блоки получает правовое признание и юридическое закрепление.

## СПИСОК ИСТОЧНИКОВ/ REFERENCES


1. URL: https://clermont-filmfest.org (data obrascheniya 26.07.2023).
2. Code de la propriété intellectuelle — Légifrance (legifrance.gouv.fr) art. L 122-4.
3. Code de la propriété intellectuelle — Légifrance (legifrance.gouv.fr) art. L335-3.
4. The legal framework to address "fake news": possible policy actions at the EU level, Policy Department for Economic, Scientific and Quality of Life Policies Author: Andrea Renda (CEPS — Centre for European Policy Studies and College of Europe) Directorate-General for Internal Policies PE 619.013 — June 2018.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 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). Text with EEA relevance.
6. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/ECText with EEA relevance.
7. Article18 (ex Article 12 TEC) Within the scope of application of the Treaties, and without prejudice to any special provisions contained therein, any discrimination on grounds of nationality shall be prohibited. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may adopt rules designed to prohibit such discrimination. [Электронный документ]. — URL: EUR-Lex — 12012E/TXT — EN — EUR-Lex (europa.eu) (data obrashcheniya: 26 июля 2023 г.)
8. Article 19.1 (ex Article 13 TEC) Without prejudice to the other provisions of the Treaties and within the limits of the powers conferred by them upon the Union, the Council, acting unanimously in accordance with a special legislative procedure and after obtaining the consent of the European Parliament, may take appropriate action to combat discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. [Elektr. dokument]. — URL: EUR-Lex — 12012E/TXT — EN — EUR-Lex (europa.eu) (data obrashcheniya: 26.07.2023).
9. EU Charter of Fundamental Rights (europa.eu) (data obrashcheniya: 26.07.2023).
10. Consolidated version of the Treaty on the Functioning of the European Union [Elektr. dokument]. — URL: http://data.europa.eu/eli/treaty/tfeu_2012/oj (data obrashcheniya: 26.07.2023).
11. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) [Elektr. document]. — URL: http://data.europa.eu/eli/reg/2018/1725/oj (data obrashcheniya: 26.07.2023).
12. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Text with EEA relevance.
13. The European Health Data Space (EHDS) [Elektr. dokument]. — URL: http://european-health-data-space.com (data obrashcheniya: 26.07.2023).