Russian Journal of Economics and Law. 2022. Т. 16, № 1 / Russian Journal of Economics and Law, 2022, Vol. 16, No. 1
Переводные статьи / Translated Articles

ISSN 2782-2923

ПЕРЕВОДНЫЕ СТАТЬИ / TRANSLATED ARTICLES

Ответственные за подбор: *Дж. Шаббар, Р. А. Григорьев* /
Persons in charge of selection: *J. Shabbar, R. A. Grigoryev*

Редактор рубрики *Дж. Шаббар* /
Rubric editor *J. Shabbar*

Научная статья
УДК 342.9:004.056:316.77:33

DOI: http://dx.doi.org/10.21202/2782-2923.2022.1.136-175

О. БЕН-ШАХАР[1]

[1] *Чикагский университет, школа права, г. Чикаго, США*

ЗАГРЯЗНЕНИЕ ИНФОРМАЦИОННОЙ СРЕДЫ

Омри Бен-Шахар, Чикагский университет, школа права
E-mail: omri@uchicago.edu

Аннотация

Цель: разработка и обоснование теории информационного загрязнения, которая позволяет понять и оценить вред, который несет в себе экономика больших данных.

Методы: диалектический подход к познанию социальных явлений, позволяющий проанализировать их в историческом развитии и функционировании в контексте совокупности объективных и субъективных факторов, который определил выбор следующих методов исследования: формально-логический и социологический.

Результаты: в статье разрабатывается теория информационного загрязнения, позволяющая понять вред, который несет в себе экономика данных, и то, как следует регулировать этот вред. Автор показывает, что общественное вмешательство должно быть направлено на внешний ущерб от сбора и неправомерного использования персональных данных. В статье оспаривается преобладающая точка зрения о том, что ущерб от утечки цифровых данных является исключительно частным. Эта точка зрения привела к тому, что законодатели сосредоточиваются лишь на защите приватности. Автор, напротив, утверждает, что в основном игнорируется центральная проблема цифровой экономики: как информация, предоставляемая гражданами, влияет на других людей, как она подрывает и уменьшает общественное благо и общественные интересы.

Научная новизна: новизна концепции информационного загрязнения заключается в том, что предлагает новый взгляд на проблему низкой эффективности существующих правовых инструментов – законов о нарушении гражданских норм, контрактов и норм раскрытия информации; эти инструменты отражают историческую бесперспективность, аналогичную попыткам снизить ущерб от промышленных загрязнений. Кроме того, теория информационного загрязнения открывает широкие возможности для создания новых правовых средств – «законов об охране окружающей

Цитирование оригинала статьи на английском: Ben-Shahar O. Data Pollution, *Journal of Legal Analysis*, 2019, Vol. 11, pp. 104–159.
URL публикации: https://academic.oup.com/jla/article/doi/10.1093/jla/laz005/5578488

ISSN 2782-2923

среды в области защиты информации», которые будут направлены на регулирование указанных внешних эффектов. В статье показано, как инструменты контроля промышленных загрязнений: ограничения за производство, углеродный налог, ответственность за выбросы – могут быть адаптированы для регулирования информационного загрязнения.
Практическая значимость: основные положения и выводы статьи могут быть использованы в научной, педагогической и правоприменительной деятельности при рассмотрении вопросов, связанных с теорией информационного загрязнения.

Ключевые слова: экономика больших данных, неправомерное использование персональных данных, цифровая экономика

Благодарности: автор выражает благодарность Ronen Avraham, Oren Bar-Gill, Karen Bradshaw, Daniel Hemel, Jaime Hine, William Hubbard, Florencial Marrota-Wurgler, Jennifer Nou, Lisa Larimore Ouillette, Ariel Porat, Eric Posner, Ricky Revesz, Lior Strahilevitz, Mark Templeton, участникам семинаров в Чикагского университета, Федеральной торговой комиссии, университетов Гарварда, Стэнфорда, Тель-Авива за плодотворные обсуждения, а также Brenna Darling и Jason Grover за помощь в исследовании.

Как цитировать русскоязычную версию статьи: Бен-Шахар О. Загрязнение информационной среды // Russian Journal of Economics and Law. 2022. Т. 16, № 1. С. 136–175. DOI: http://dx.doi.org/10.21202/2782-2923.2022.1.136-175

The scientific article

O. BEN-SHAHAR[1]
[1] *University of Chicago Law School, Chicago, USA*

DATA POLLUTION

Omri Ben-Shahar, University of Chicago Law School
E-mail: omri@uchicago.edu

Abstract

Objective: to develop and substantiate the theory of data pollution, which makes it possible to realize and assess the harms the economy of big data creates.
Methods: dialectical approach to cognition of social phenomena, allowing to analyze them in historical development and functioning in the context of the totality of objective and subjective factors, which predetermined the following research methods: formal-logical and sociological.
Results: This article develops a novel framework – data pollution – to rethink the harms the data economy creates and the way they have to be regulated. The author argues that social intervention should focus on the external harms from collection and misuse of personal data. The article challenges the hegemony of the prevailing view that the injuries from digital data enterprise are exclusively private. That view has led lawmakers to focus solely on privacy protection as the regulatory objective. The article claims, instead, that a central problem in the digital economy has been largely ignored: how the information given by people affects others, and how it undermines and degrades public goods and interests.
Scientific novelty: The data pollution concept offers a novel perspective why existing regulatory tools – torts, contracts, and disclosure law – are ineffective, mirroring their historical futility in curbing the harms from industrial pollution. The data pollution framework also opens up a rich roadmap for new regulatory devices – "an environmental law for data protection" –

The article was first published in English language by Journal of Legal Analysis. For more information please contact: journals.permissions@oup.com
For original publication: Ben-Shahar O. Data pollution, *Journal of Legal Analysis*, 2019, Vol. 11, pp. 104–159.
Publication URL: https://academic.oup.com/jla/article/doi/10.1093/jla/laz005/5578488

ISSN 2782-2923

which focuses on controlling these external effects. The article examines how the tools used to control industrial pollution – production restrictions, carbon tax, and emissions liability – could be adapted to govern data pollution.
Practical significance: the main provisions and conclusions of the article can be used in scientific, pedagogical and law enforcement activities when considering the issues related to the theory of data pollution.

Keywords: Big data economy, Misuse of personal data, Digital economy

Acknowledgements: I am grateful to Ronen Avraham, Oren Bar-Gill, Karen Bradshaw, Daniel Hemel, Jaime Hine, William Hubbard, Florencial Marrota-Wurgler, Jennifer Nou, Lisa Larimore Ouillette, Ariel Porat, Eric Posner, Ricky Revesz, Lior Strahilevitz, Mark Templeton, and workshop participants at the University of Chicago, the Federal Trade Commission, Harvard, Stanford*, and Tel-Aviv University for helpful discussions, and to Brenna Darling and Jason Grover for research assistance.

For citation of Russian version: Ben-Shahar O. (2022). Data Pollution. *Russian Journal of Economics and Law, 16 (1)*, 136–175. DOI: http://dx.doi.org/10.21202/2782-2923.2022.1.136-175

Для нашего века информация то же, чем была нефть для прошлого.
Журнал *The Economist*, май 2017 г.

1. ВВЕДЕНИЕ

Цифровая информация – топливо новой экономики. Это ресурс для производства новых продуктов и компаний, новых рынков и валют, а также бесконечных новых возможностей для создания крупных общественных ценностей[1]. Но, как и углеродное топливо старой экономики, она вызывает загрязнение окружающей среды. Вредные «выбросы данных» проникают в цифровые экосистемы, разрушая социальные институты и общественные интересы. В этой статье разрабатывается инновационный подход – и*нформационное загрязнение*, – позволяющий понять вред, который несет в себе экономика данных, и возможную реакцию властей на этот вред.

Цифровая информация включает в себя любые возможные способы компиляции данных, но, вероятно, самое ценное – это персональные данные. Цифровые платформы собирают информацию о том, где находится человек в настоящее время, что он делал в прошлом и что планирует делать в будущем, что и кого он любит и как можно влиять на его решения. Повсеместный сбор таких персональных данных позволил создать новые персонифицированные общественные пространства, дающие огромные личные и социальные преимущества. Однако они также несут потенциальный вред. Один из видов такого вреда, о котором сейчас много говорят, – это потенциальный ущерб интересам приватности. С другой стороны, внешний ущерб является менее конкретным и гораздо менее заметным. Понимание масштабов этого внешнего ущерба и снижение его влияния – одна из важнейших задач нашей эпохи.

Актуальность этой задачи значительно возросла благодаря двум явлениям. Первое из них – это *намеренное обнародование* персональных данных, которое ярко проявилось во время выборов президента США в 2016 г. Для распространения фальшивой политической рекламы использовалась база персональных данных Facebook[2]. Ложь в политике – не новое явление, но информационные процессы способствуют быстрому распространению и закреплению лжи, чем многократно усиливают ее эффект, а также делают распознавание лжи более сложной задачей. Второе

[1] См. [1]; см. также [2] (цифровые технологические изменения показаны на шкале сопоставления с промышленной революцией) и [3. P. 15].

* Является нежелательной организацией в РФ с 26.03.2026 / Recognized as an undesirable organization in the Russian Federation as of 26.03.2026.

[2] Сеть принадлежит компании *Meta*, признана экстремистской организацией в РФ / The network is owned by Meta, a company recognized as an extremist organization in the Russian Federation. См. [4].

ISSN 2782-2923

явление – *ненамеренное обнародование* персональных данных, когда компании оказываются неспособны защитить свои базы данных. Ярким примером этой проблемы может служить кража финансовых досье 143 млн клиентов компании *Equifax*.

Во многих странах в настоящее время идет поиск парадигм понимания и способов предотвращения актуальных и потенциальных угроз, связанных с персональными данными. Этот поиск сосредоточен преимущественно на одном направлении. Главным и, возможно, единственным критерием оценки риска в этой сфере является *приватность*. В рамках парадигмы приватности данных сбор и использование персональных данных порождают различные риски для того, кому принадлежат эти данные. Согласно этой парадигме, если личные и частные аспекты жизни человека становятся известными или искажаются, это наносит ущерб благополучию, осуществлению прав, независимости и достоинству этого человека, т. е. сфере его личной жизни [5. P. 126]. Парадигма приватности основана на предпосылке, что ущерб от неправомерного использования персональных данных будет частным по своей природе – это «ущерб для личности», однако за счет накопления (или за счет более точного попадания) эти глубоко личные виды ущерба оказывают вторичный супераддитивный общественный эффект [6; 7. P. 300][3].

К сожалению, парадигма приватности неполна, поскольку ущерб от злоупотребления информацией зачастую намного превышает сумму частных ущербов для лиц, которым принадлежит эта информация. Если в самом деле «для нашего века информация – то же, чем была нефть для прошлого», то можно утверждать, что для нашего века информационное загрязнение – то же, чем было промышленное загрязнение для прошлого. Загрязнение – как информационное, так и промышленное – порождает общественный ущерб и разрушает общественное благо, и это помимо того влияния, которое ощущают частные лица, использующие загрязняющие продукты. При этом методы контроля загрязнения и защиты общественных интересов в корне отличаются от правовых реформ, призванных бороться с частным ущербом.

Концепция информационного загрязнения предлагает посмотреть шире и понять, каким образом сбор персональных данных влияет на общественные институты и группы, – помимо тех граждан, кто предоставляет информацию, и ущерба для их приватности. Ярким примером влияния информационного обмена на экосистему является практика компании *Facebook**, которая предоставила рекламодателям доступ к персональным данным и возможность изменять результаты голосования. Негативный эффект этого действия не ограничился частным ущербом для тех лиц, которые стали получать рекламу на основе их данных или на чье мнение при голосовании было оказано влияние (на самом деле многие из них не считают себя пострадавшими). Главный негативный эффект был гораздо шире – пострадало все окружение, связанное с выборами и политикой, включая ущерб для других членов общества и ущерб, не имеющий отношения к вопросам приватности. Даже если речь не идет о злоупотреблениях, мы все больше осознаем, что платформы, предлагающие «персонализированные новости», способствуют фрагментации и поляризации общества, а это разрушает процесс демократического обсуждения и уничтожает «социальный клей» [13, 14].

Информационный обмен вызывает загрязнение и другими, более конкретными способами. Давая разрешение веб-сайтам на сбор данных о своей электронной переписке, участии в социальных сетях и даже о своей ДНК, люди автоматически предоставляют информацию о других лицах, которые не участвуют непосредственно в этих транзакциях. В персонализированных средах опыт каждого индивидуума частично зависит от того, какими данными о других людях он поделился.

Концепция информационного загрязнения служит основой для трех смелых идей, выдвигаемых в этой статье. Первая из них – охарактеризовать сущность социального ущерба от информационного обмена.

[3] См., например, [8. P. 1653] (приватность баз данных является необходимым условием демократического обсуждения общественных проблем), [9] (приватность необходима для развития гражданского общества, свободы самовыражения и комфортной общественной жизни), [10. Pp. 69–71] (приватность необходима для правильного функционирования демократической политической системы), [11] (описан ущерб для человеческого достоинства, вызванный утечкой данных; утверждается, что это может привести к «нежеланию граждан предоставлять информацию, что затруднит достижение поставленных политических целей»). См. в целом [12] (обсуждаются частная и публичная сферы защиты частной жизни).

ISSN 2782-2923

Множество научных источников описывают каждый аспект всех возможных видов частного ущерба от сбора данных, т. е. потенциальный ущерб приватности людей, чьи данные собираются. Однако зачастую игнорируется проблема внешних эффектов: как разрешение на сбор личных данных повлияет на других людей и общество в целом. В разд. 2 показаны различные грани этого внешнего, общественного эффекта. Проводится разграничение между малоизвестным общественным ущербом и широко признанным частным ущербом от распространения информации; тем самым мы начинаем создавать новое, дополненное обоснование для регулирования данных. Кроме того, обсуждение, представленное в разд. 2, помогает решить сложную задачу – как примирить повсеместное недовольство людей сбором персональных данных и всеобщую готовность «платить своими данными». Это несоответствие часто называют «парадоксом приватности» [15; 16. P. 17; 17][4]. Теория информационного загрязнения разрешает этот парадокс: люди ощущают тревогу по поводу влияния информации на общество в целом и в гораздо меньшей степени – по поводу возможного ущерба для себя лично. Они считают, что частные выгоды от предоставления информации перевешивают этот ущерб.

Вторая идея настоящей статьи – объяснить причины неэффективности существующих правовых инструментов борьбы с информационным загрязнением. В разд. 3 показано, что частное право и правоприменение неспособны контролировать информационное загрязнение по тем же самым причинам, по которым они не контролируют промышленное загрязнение. Неэффективность частных оснований для предъявления исков объясняется в первую очередь публичным характером ущерба. Загрязнение относится к внешним эффектам; оно затрагивает окружающую среду в целом, а не только тех лиц, с которыми взаимодействует источник загрязнений или владелец информации. Информационное загрязнение, как и его промышленный предшественник, приносит вред всему сообществу; к тому времени, когда затронуты конкретные индивидуумы, оказывается уже сложно установить причину или полный масштаб общественного вреда. В контексте промышленного загрязнения истцы исторически испытывали трудности с привязкой роста заболеваемости к конкретным случаям выбросов; так же и нынешним жертвам злоупотребления информацией сложно доказать, какие именно утечки данных им навредили [20. P. 429]. Даже если причинная связь установлена, объем ущерба для отдельной жертвы загрязнения – как в промышленной, так и в цифровой сфере – зачастую слишком умозрительный, чтобы его можно было оценить с помощью инструментов частного права.

Далее в разд. 3 показано, что неспособность частного права регулировать информационное загрязнение объясняется не только ограничениями деликтного права, это также недостаток контрактной системы. Добровольные транзакции с загрязняющими продуктами оказались неспособны адекватно снизить выбросы в промышленности; по тем же самым причинам рынки цифровых продуктов не уделяют существенного внимания снижению информационного загрязнения. Потребители покупают продукты с огромным углеродным следом; аналогичным образом они оставляют огромный информационный след на цифровых площадках. Как в промышленности, так и в цифровой сфере люди не заключают оптимальных договоров о загрязнении по целому ряду причин, но в первую очередь потому, что сокращение загрязнения – это общественное благо. Изначально ошибочно мнение, что контракты и система информированного согласия помогают людям принимать разумные решения относительно обмена информацией и снижают уровень информационного загрязнения, поскольку механизм частных двусторонних контрактов не способен предотвратить ущерб, наносимый третьим сторонам. Не столько отдельных граждан нужно защищать от ловушек контрактов, связанных с передачей данных, сколько э*косистему в целом нужно защищать от* подобных контрактов, бесконечно заключаемых гражданами.

Таким образом, в разд. 2 предлагается новое понимание ущерба в сфере данных, в разд. 3 объясняется неэффективность существующих подходов к снижению этого ущерба, а в разд. 4 представлена третья идея настоящей статьи, наиболее амбициозная из всех: создание альтернативной системы правового контроля над информационным загрязнением. Метафора загряз-

[4] Попытки объяснить парадокс приватности с точки зрения проблемы асимметричности информации см. [18. Pp. 1732–1735; 19] (обсуждается неопределенность и сложность решений по поводу приватности как причина поведения, не предусматривающего защиту приватности).

ISSN 2782-2923

нения позволяет предложить широкий спектр правовых средств и упорядоченный набор рекомендаций, которые до сих пор оставались незадействованными или имели иные обоснования для применения[5].

Основным методом регулирования загрязнений является установленный комплекс ограничений производства, чаще всего в форме количественных лимитов и квот. Деятельность, вызывающая загрязнения, может быть ограничена за счет необходимости получать лицензии на выбросы или выполнять законные требования по объему производства. Информационное загрязнение также можно контролировать путем ограничения информационных услуг по нескольким направлениям: какие данные можно собирать, кто может это делать, в каких объемах и по каким основаниям, каким образом можно использовать или передавать данные, когда их необходимо уничтожать, как сохранять и т. д. Такие предупреждающие методы все шире применяются в европейском частном праве[6] и в некоторых узких областях американского частного права – например, в ситуациях с участием детей[7]. Количественное регулирование относится к традиционным методам контроля, и оно способно эффективно снижать загрязнение, но зачастую ценой значительных издержек. При этом снижаются не только негативные последствия, но также и позитивные; кроме того, происходит торможение инноваций. В сфере работы с данными особенно сложно применять анализ эффективности затрат при ограничениях на информацию, поскольку затраты и выгоды очень сложно оценить.

В разд. 4 мы описываем сложности, связанные с количественными ограничениями, и рассматриваем другой ключевой метод контроля загрязнений: определение стоимости общественных издержек. Считается, что «налог Пигу» на деятельность, на вложения в эту деятельность или на ее результаты способен скорректировать деформации, вызванные негативными внешними эффектами. В промышленном производстве этот подход привел к появлению углеродного налога, а в цифровой экономике он предполагает появление налога на информацию. Общественные издержки от сбора личных данных могут быть интернализированы через налог на деятельность с информацией. В разд. 4 рассматриваются некоторые основные проблемы, связанные с налогом на информацию: кто должен его выплачивать, как его установить, каковы могут быть преднамеренные и непреднамеренные результаты его введения. Также показано, что информация может производить некоторые нейтрализующие положительные эффекты, которые могут влиять на размер налога. Важно отметить, что предлагаемый подход отличается от недавних предложений (и даже

[5] Ряд авторов уже использовали контекст охраны окружающей среды как модель для изучения проблемы регулирования оборота информации. Однако в отличие от настоящей статьи они фокусировались на частном ущербе и законодательстве о защите частной жизни, а именно как сбор данных вызывает вред для тех лиц, чьи данные собираются. Наиболее близкими к точке зрения автора настоящей статьи являются работы [21, 18, 10]. Как и в настоящей работе, эти авторы изучали так называемые внешние эффекты сбора данных, но определяли их как снижение уровня приватности, вызываемое практиками надзора со стороны сборщиков данных. См., например, [18. P. 1732] («Если стороны, над которыми проводится наблюдение, заботятся о своей приватности, то наблюдающая сторона налагает на них дополнительные расходы для достижения собственных целей. Независимо от того, совпадает ли эта ситуация с классической моделью внешних эффектов, ее, несомненно, можно смоделировать таким образом»), [21. P. 28] («Компании получают выгоду от собираемой информации, но не несут затрат, которые они тем самым вызывают... (т. е. нарушение приватности клиентов... В экономических терминах – компании, собирающие персональную информацию, налагают отрицательные внешние эффекты на потребителей»), [22. P. 375] («Большие данные... делают социальную среду менее благоприятной для развития человеческой личности»). При решении вопроса о регулировании ущерба в сфере информации Hirsch [21, 22] и Froomkin [18] обращаются к командно-административным средствам регулирования, используемым в законодательстве об охране окружающей среды, однако, поскольку они рассматривают этот ущерб исключительно как частный (используя термины «внутренняя среда», «нарушение приватности», «человеческая личность»), их анализ методов регулирования приводит к иным выводам, чем те, что обсуждаются в настоящей статье. Напротив, Nehf [10] изучал общественную ценность приватности. Хотя он фокусируется в основном на социальных последствиях нарушения частной жизни («отчуждение» и утрата власти по отношению к «крупным институтам») (Там же. Pp. 69–71), он также признает существование «внешних издержек, помимо прямого ущерба для участвующих лиц», таких как переложение на потребителя общественных издержек от нарушения конфиденциальности (Там же. Pp. 79–80).

[6] European Directive on Data Protection, 95/46/EC of the European Parliament and of the Council, Art. 25, OJ L 281, 23 November 1995, 56-57 (1995); General Data Protection Regulation (GDPR), 2016/679 of the European Parliament and of the Council, OJ 119, 4 May 2016, 60–62 (2016).

[7] Children's Online Privacy Protection Act, 15 U.S.C. § 6501 (1998).

ISSN 2782-2923

противоречит им) сделать обязательными выплаты гражданам от компаний за их персональные данные [24; 25. Pp. 246–249]. Оплата за данные – это сделка с нулевой суммой между двумя сторонами, которые совместно производят информационное загрязнение, следовательно, она не снижает уровень соответствующей деятельности и не способствует инвестициям, снижающим загрязнение.

Третий подход к контролю над загрязнениями состоит в разработке режима ответственности за ущерб, наносимый информацией, в особенности для борьбы с непреднамеренными утечками данных. Как и выбросы токсичных отходов в промышленности, утечки данных становятся основным внешним эффектом, с которым пытается бороться частное право. В законах об охране окружающей среды содержится ряд инструментов, позволяющих перенаправить ущерб от токсичных отходов на тех, кто ответственен за их утечку; аналогичным образом, закон об информационном загрязнении может сфокусироваться на вопросах ответственности и предотвращения вреда. Очищение после утечки данных по большей части невозможно; однако ущерб можно уменьшить за счет адекватной подготовки к таким ситуациям и к действиям после утечки. Предполагаемый вред можно снизить с помощью надлежащей системы сдерживания. Если масштаб ответственности будет соответствовать социальным издержкам (а этому может способствовать обязательное страхование ответственности), то это приведет к развитию системы мер предосторожности и саморегуляции. В разд. 4 изложено предложение по переходу к режиму пропорциональной ответственности.

Некоторые из указанных методов регуляции уже рассматривались ранее, но лишь через призму защиты частной жизни. Этот аспект рассмотрения сразу привлекает внимание, поскольку базы данных, приводящие к информационному загрязнению, состоят из персональной, а иногда приватной информации. Но чем более привлекателен аспект защиты частной жизни, тем в большей степени он кажется единственно важным аспектом изучаемой проблемы – и тем яснее становится, что законодатели и сторонники такого подхода не учитывают широкомасштабное общественное влияние, выходящее далеко за пределы интересов любых частных сторон, чья персональная информация включается в базы данных. Раздел 4 рассматривает способы преодоления этого узкого подхода и предлагает такие принципы создания законодательства об информационном загрязнении, которые могли бы минимизировать внешние общественные издержки.

Законодательство о защите окружающей среды зародилось в индустриальную эпоху, поскольку частное право имело дело лишь с частным ущербом и было неспособно защитить общественное благо и окружающую среду [26. P. 149]. Сегодня нам необходима современная версия законодательства о защите окружающей среды – законодательство об информационном загрязнении, которое расширило бы понимание проблемы защиты информации и смогло бы противостоять *общественному* ущербу от сбора персональных данных. Настоящая статья предлагает план такой трансформации.

2. ИНФОРМАЦИОННЫЙ УЩЕРБ: ЧАСТНЫЙ ИЛИ ОБЩЕСТВЕННЫЙ?

В течение многих десятилетий охрана частной жизни рассматривалась как основная проблема в развитии информационных технологий. В рамках парадигмы охраны частной жизни сбор персональных данных коммерческими организациями может создать ущерб для тех, чья информация собирается и используется. Компании, собирающие персональные данные, могут многое узнать о людях и использовать эти знания для блага, но также могут и вызывать риски и вред.

Определению границ этого вреда посвящена обширная литература. Иногда эмоциональный ущерб жертв очевиден; например, если взламывается сайт, на котором люди ищут партнеров для внебрачных связей [27]. В других случаях люди ощущают вред, когда алгоритм работы с данными представляет их миру с ущербом для их репутации или финансовых возможностей [28]. Случаи прямого эмоционального и репутационного вреда поддерживают широко распространенное мнение о том, что базы данных, собирающие персональную информацию, могут нанести персональный ущерб. Ряд специалистов по проблеме охраны частной жизни отмечают, что этот внутренний ущерб может перейти в общественную плоскость – например, деморализуя людей и тем самым препятствуя «демократическому процессу принятия решений» или подрывая «развитие гражданского общества» – однако те виды общественного вреда, которые они указывают, являются лишь производными от персо-

ISSN 2782-2923

нального ущерба: деморализуются те индивиды, чья персональная информация была собрана (например, [8. P. 1653; 9; 12; 10. Pp. 69–71; 11].

Такое представление (что проблема с информацией лежит в плоскости частной жизни, а ее решение – защита приватности) является очень привлекательным, так как базы данных компаний состоят в основном из частной информации, которую люди обычно не обнародуют. Множество данных собирается путем процедур, которые критики характеризуют как «надзор» и говорят о «постоянном присутствии наблюдения в домах людей» [29]. Если проблема состоит в том, что умные устройства и приложения «шпионят за нами (даже в нашем собственном доме» [30], то мы сразу задумываемся о личном ущербе, и очевидным средством противодействия этому потенциальному ущербу становится защита личной информации.

Однако это главенствующее мнение – что информационные технологии наносят частный ущерб – наталкивается на неприятное явление, которое иногда называют «парадоксом приватности». Несмотря на большое внимание, уделяемое рискам и защите приватности со стороны законодателей и юристов, несмотря на широко распространенное и документально подтвержденное мнение о важности защиты персональной информации, реальное поведение людей противоречит этому [31][8]. Люди утверждают, что понимают огромную важность своих персональных данных, и тут же отдают их за самую незначительную цену [35, 36, 17]. Исследования показали, что реальный уровень заботы о своей информационной безопасности существенно уступает ее декларируемой ценности. Иными словами, у нас нет достаточных оснований утверждать, что сбор цифровых данных наносит явный и измеримый ущерб тем аспектам личности, о которых обычно упоминают в этом контексте – эмоциональному благополучию, личному достоинству, независимости, репутации.

И все же тревога по поводу вреда, вызываемого информационными технологиями, неуклонно растет. Американская политическая система была до основания потрясена сведениями о возможных злоупотреблениях, связанных с огромной базой данных *Facebook**, что, возможно, повлияло на результаты выборов. Одновременно в американской финансовой системе произошла массовая утечка личных и финансовых данных потребителей и стало известно о вероятном мошенническом использовании этой информации. Крупнейшие страны мира проводят масштабные реформы, широко одобряемые населением, с целью затруднить сбор данных[9]. Громче чем прежде звучат опасения по поводу нарушений приватности.

Как же примирить эти противоречивые эмпирические наблюдения – всеобщую озабоченность властью информации и всеобщее равнодушие при передаче собственных данных? Это фундаментальный вопрос в сфере законодательства об охране частной жизни, и на него предложено несколько различных ответов (например, [19; 18. Pp. 1732–1735; 37]. Однако на один аспект обычно не обращают внимания, а именно на тот, которому посвящена наша статья, – природу причиняемого ущерба. Если значимый компонент информационного ущерба является общественным, тогда указанное противоречие исчезает. Люди беспокоятся о том, что информация способна причинить общественный ущерб. При этом они не беспокоятся о своем частном ущербе и поэтому продолжают делиться своими данными.

Автор не задается вопросом, значительны ли частные ущербы, связанные с информацией; в настоящей статье автор развивает тезис, что обоснование законодательства в области информации должно формироваться относительно внешних ущербов. Наличие баз данных с личной информацией сказывается на всей экосистеме, а не только на тех лицах, чья информация была обнародована или подверглась злоупотреблениям. Соответственно, в оставшейся части данного раздела мы рассмотрим виды влияния сбора персональных данных на общество – способы информационного загрязнения.

2.1. Влияние на общественные интересы

Промышленное загрязнение снижает уровень общественного блага. Оно является квинтэссенцией отрицательного внешнего эффекта, так как затрагивает многих лиц, не являющихся сторонами деятельности, вызывающей загрязнение. Оно влияет на экосистему в целом, а также на здоровье многих третьих лиц.

[8] См. [32–34] («85 % потребителей считают, что компании должны предпринимать больше усилий для защиты их данных»); см. в целом [31].

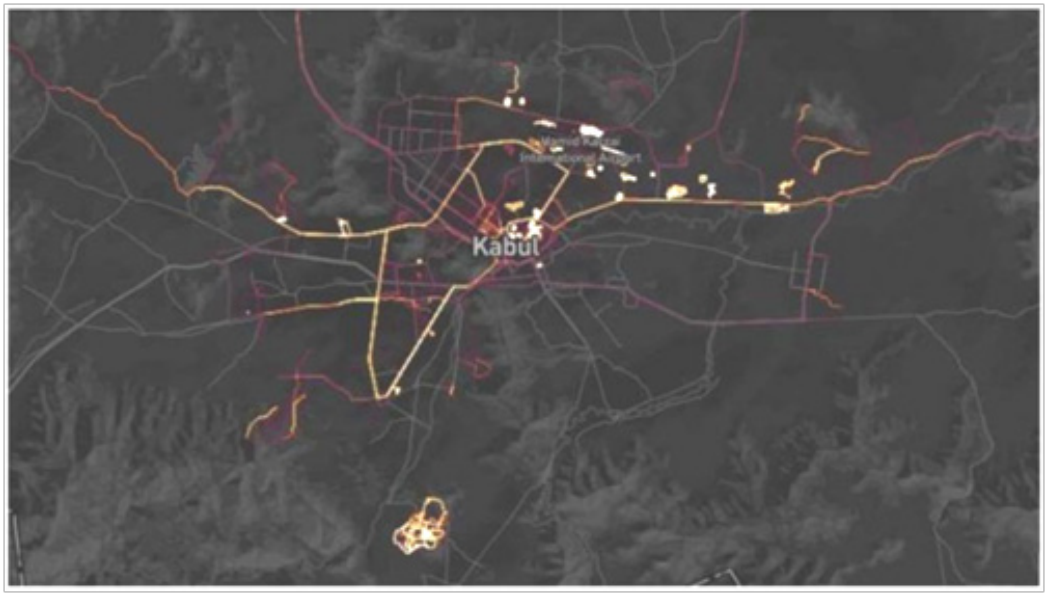
[9] Например, California Consumer Privacy Act of 2018, AB 375.

ISSN 2782-2923

Утечки информации сходны с утечками других загрязняющих веществ; издержки часто являются внешними, т. е. затрагивают общественные интересы. Цифровая база данных не похожа на библиотечный каталог прошлых поколений; это просто проиндексированная сумма отдельных кусочков информации. Цифровая база данных обладает свойством супераддитивности; из нее можно узнать то, что не было известно в момент разделения информации, в том числе то, что затрагивает общественные интересы. При агрегации информации возникает новое знание, включая сведения о лицах, чья персональная информация никогда не заносилась в эти базы; в дальнейшем эти сведения могут использоваться во вред этим индивидуумам или обществу в целом. Приведем несколько примеров для иллюстрации таких негативных внешних эффектов.

Первый пример – сеть *Facebook**. Когда владельцы этой гигантской социальной сети дали разработчикам приложений и другим сторонам доступ к базе данных своих пользователей, влияние этого действия лишь частично отразилось на отдельных гражданах. Если бы использование данных для распространения политической лжи и фейков было более эффективным, как это произошло в деле *Cambridge Analytica*, то результатом стало бы нарушение целостности процесса голосования. Такое нарушение выходит далеко за пределы частных интересов сторон. (Фактически вполне вероятно, что лица, чьи данные были использованы, остались вполне удовлетворены своими действиями и не чувствуют никакого персонального вреда.) Первостепенной угрозой общественному благу является новая возможность, порожденная цифровизацией, – возможность для правительств враждебных стран разворачивать цифровые платформы и искажать результаты демократического процесса.

Второй пример, иллюстрирующий влияние раскрытия информации на общественные интересы, помимо приватности пользователей, – это приложение для фитнеса *Strava*, провозгласившее себя «социальной сетью для спортсменов». Приложение позволяет миллионам пользователей обозначать на карте места своих тренировок; затем все могут видеть «тепловую карту» спортивной активности. Крупные скопления пользователей могут указывать на секретные места военных операций США по всему миру [38, 39]. Чем иным может быть кластер физической активности в пустыне Сахара или в окрестностях крупного афганского города? Метаизображение возникает в результате агрегации персональных данных, угрожая общественным интересам – национальной безопасности, а не частной жизни индивидуального владельца данных (рис. 1).



Тепловая карта *Strava* в окрестностях Кабула (Афганистан) показывает активность к югу от города
Strava heatmap of Kabul, Afghanistan, displaying a patch of activity south of the city

ISSN 2782-2923

Озабоченность по поводу общественной угрозы, вызванной агрегацией информации, отражена в попытках правительства ограничить передачу коммерческих баз данных через границы государства путем введения выходного контроля и требования «локализации данных» [40. P. 107]. Аргументация в пользу таких мер простирается от требований национальной безопасности и обеспечения правопорядка до защиты торговли и промышленности страны. Например, правительство Китая объявило, что «информация стала одним из основных национальных стратегических ресурсов», и постановило, что персональные данные китайских граждан могут храниться только внутри страны[10]. Утверждается, что утечка или обнародование огромных объемов персональных данных с таких сервисов, как *Alibaba*, является «серьезной угрозой для национальной безопасности» [41].

Возможности использования баз данных для причинения вреда общественному благу или общим ценностям можно продемонстрировать также на примере персонализации обращения с информацией и соответствующих новых форм опасной дискриминации. Связи, которые можно извлечь из баз данных, дают информацию помимо той, что содержится в них непосредственно, и для ее получения можно создать необходимые алгоритмы. Такие подходы лежат в основе персонализированного маркетинга и множества других сервисов. Они дают огромные общественные выгоды – например, используя цифровые истории болезней, больницы могут предоставлять более качественное и быстрое обслуживание с меньшими затратами[11].

Однако те же корреляции, извлекаемые из цифровых баз данных, могут приводить к дискриминации против некоторых групп лиц. Например, онлайн-реклама реже предлагает рабочие места в сфере инжиниринга и математики женщинам, чем мужчинам [43, 44]; сообщения, предполагающие прошлую судимость, при запуске онлайн-поиска предлагаются чаще лицам, чьи имена звучат как имена чернокожих [45]. Такие дискриминационные явления могут иметь негативное влияние на общество. Стремясь оптимизировать свои затраты, компании, рекламирующие позиции в сфере инжиниринга и математики, ограничивают показы своей рекламы для женщин; при поиске лиц с судимостью также запускается «оптимизация» в пользу страниц, содержащих имена чернокожих. Такие вещи становятся возможными с помощью аналитики персональных данных; они просто соответствуют информационным запросам людей [46]. Однако максимизация частной прибыли от рекламы в обществе, где существуют дискриминация и неравенство, не гарантирует общественно оптимальной передачи информации. Напротив, такое положение может способствовать усилению дискриминации, так как выявляет дискриминационные схемы, которые в мире «малых данных» не могли бы существовать.

Провести границу между вредоносной дискриминацией и желательной персонализацией не всегда легко, поскольку и то и другое основывается на работе с данными и индивидуальными особенностями отдельного человека. Персонализированные медицина, обучение, питание помогают лечить, учить, кормить людей более эффективно. Даже персонализированная реклама помогает людям получать более полезную информацию. Вполне возможно, что выгоды от персонализации на основе данных намного превосходят негативное влияние соответствующей дискриминации – то есть что нужно говорить скорее о «защите окружающей среды в сфере информации», чем об информационном загрязнении. Однако выгоды от владения данными часто присваиваются и интернализируются: компании, создающие такие выгоды, имеют как мотивы, так и технические инструменты для их коммерциализации и монетизации (пока конкуренция не лишит их этих преимуществ). Напротив, негативные внешние эффекты остаются всеобщими. Они затрагивают слишком обширные и раздробленные группы и вызывают слишком абстрактный ущерб, чтобы можно было эффективно влиять на них частными средствами.

Дискриминация – это главный, но не единственный общественный вред, вызванный цифровой средой. Быстрое распространение ненавистнических, манипулятивных, поляризующих новостей и мнений в социальных сетях, сегрегация информационных сообществ, исчезновение оснований для общего опыта – то, что Sunstein [13] назвал «эхокамерами» и «информационными коконами», – это явление, которое многократно усилила цифровизация (см. также [47].

[10] Cybersecurity Law of the People's Republic of China, Art. 37.

[11] См., например, [42. Pp. 51–54] (показано, что ведение цифровых медицинских карт снижает неонатальную смертность).

ISSN 2782-2923

2.2. Влияние на других лиц

Загрязнение может оказывать негативный внешний эффект не только на экосистему или на общественное благо, но и на конкретных частных жертв. Например, загрязнение асбестом влияет на здоровье отдельных лиц. Аналогичным образом экстернализация ущерба от цифровых данных может происходить через механизмы, затрагивающие не только систему в целом, но конкретных лиц, но не тех, кто предоставил информацию.

Самый распространенный механизм такого рода – предоставление пользователями определенной информации о других лицах. Например, *Google* собирает и использует персональные данные, сканируя тексты сообщений, пересылаемых через *Gmail*. Любые последствия этого на отдельных пользователей *Gmail* интернализируются, т. е. относятся на счет взаимодействующих сторон. Пользователи платят за услуги электронной почты не деньгами, а данными (у них есть выбор). Но что по поводу тех, кто не использует Gmail, но посылает письма владельцу аккаунта *Gmail*? Содержание их писем также просматривается и используется «Гуглом» в соответствии с соглашением для пользователей *Gmail*. Все неудобства, испытываемые этими пользователями, – возможно, именно те неудобства, которые заставили их отказаться от бесплатного аккаунта *Gmail*, – это внешний эффект транзакции с *Gmail*. Если бы эти лица могли заключить договор с пользователями *Gmail* (и другими пользователями электронной почты, которые используют сервисы, размещенные на платформе *Google*) и «выставить счет» за испытываемые неудобства, то этот внешний эффект был бы интернализирован. Но заключение такого «контракта Коуза» невозможно из-за множества транзакционных издержек.

Другой пример обмена данными, при котором затрагиваются третьи стороны, – это информация о ДНК, которую люди предоставляют сервисам по генетической проверке, например, *23andMe* или *ancestry.com*. Информация, хранящаяся в их базах данных, содержит множество важных фактов о третьих лицах из круга биологических родственников пользователей, которые никогда не давали согласия на участие в таких исследованиях. Возможно, эта информация может спасти жизнь этих родственников. Она может также оказаться социально полезной для раскрытия преступлений или воссоединения семей[12]. Однако она может вызвать и негативные последствия, особенно в случаях, когда требуется генетическая анонимность [50].

Наконец, рассмотрим социальную сеть, которая имеет законный доступ к данным своих пользователей, включая ценную информацию об их «друзьях» (в том числе тех, кто пытается ограничить свою публичность)[13]. Помимо полного выхода из социальных сетей, эти лица практически ничего не могут сделать. Все их усилия оставаться анонимными будут сведены на нет, если данные собираются через порталы других людей. Другими словами, все меры предосторожности должны приниматься совместно; если некоторые члены социальных сетей не выполняют их, они уничтожают все усилия других.

Оказывает ли информационное загрязнение негативные эффекты на всю экосистему или только на определенный круг третьих сторон, будет зависеть от структуры регулятивного отклика. Такие инструменты публичного законодательства, как количественные ограничения или налоги, могут быть эффективными для обеих категорий внешних эффектов, что будет обсуждаться в разд. 4. Напротив, решения, предлагаемые частным законодательством, не позволяют исключить ущерб для общественного блага. Возможно, некоторые частные инструменты могли бы помочь, когда внешний эффект затрагивает конкретные и определяемые третьи стороны. Но эти инструменты оказываются неэффективными, если операторы баз данных ограждены от ответственности.

2.3. Внешние эффекты мер предосторожности и страхования

Общественное влияние ущерба включает в себя затраты на меры предосторожности. Некоторые из внешних эффектов в сфере информации оказыва-

[12] См., например, [48] (примеры раскрытых преступлений), [49] (пример воссоединения семьи).

[13] Зачастую сторонние приложения позволяют пользователям регистрироваться через их аккаунт в *Facebook**. До 2015 г. при использовании логина *Facebook** пользователь, часто не догадываясь об этом, передавал разработчику приложения всю информацию со своего профиля в *Facebook**, например, свои имя, месторасположение, адрес электронной почты, список друзей. В 2015 г. *Facebook** приостановил эту практику, однако не потребовал от третьих сторон удалить ранее собранные данные. См. [51, 52].

ISSN 2782-2923

ются преодолимыми, но ценой неких издержек. Эти издержки также имеют аспект общественного блага. Нет ничего удивительного в том, что сокращение загрязнения является общественным благом. Жертвы загрязнения часто входят в широкий круг лиц, подверженных одному и тому же виду ущерба, который, в свою очередь, зависит от вклада каждого члена этого круга. В контексте охраны окружающей среды лица, применяющие частные меры против выбросов, не могут достичь оптимальных уровней защиты, поэтому положительный эффект от их усилий оказывается дискредитированным. Вспомним, что одна из задач политики в области климата – заставить борцов-одиночек действовать в соответствии с официальными усилиями [53. P. 376].

Проблема общественного блага может возникнуть даже тогда, когда превентивные меры приносят только частную, но не внешнюю выгоду – через внешний эффект страхования. Если потребители защищены от ущерба страховкой, они могут меньше беспокоиться о нем (типичная проблема морального ущерба)[14]. Эта проблема стимулирования становится внешним эффектом, когда издержки на покрытие возникшего ущерба распределяются между всеми членами страхового пула. В контексте охраны окружающей среды кумулятивный рост заболеваемости в результате выбросов загрязняющих веществ распределяется на весь пул граждан, имеющих медицинскую страховку.

В контексте информационного загрязнения также присутствуют внешние эффекты как от мер предосторожности, так и от страхования, причем последние в особенно острой форме. Если возникает взлом системы безопасности и огромные объемы важных персональных данных оказываются доступными, люди могут серьезно пострадать от кражи личности, финансового мошенничества, а также от издержек, связанных с восстановлением безопасности данных. Однако в основном они застрахованы от этих частных ущербов от мошенничества через различные предусмотренные законодательством программы страхования, а остаточные потери покрываются стандартными страховками для домовладельцев[15]. Экономические издержки от утечки данных значительны[16], но только малую их долю несут потребители, чьи данные подверглись краже.

Отдельно следует отметить, что компании, подвергшиеся взлому данных, часто испытывают враждебное отношение, от них требуют «покарать» взломщиков. Кроме того, от них требуют возместить ущерб, при этом не учитывая внешние эффекты от таких действий, а именно поощрение хакеров на повторение взломов. Действительно, ФБР рекомендует не идти на возмещение цифрового ущерба, однако компании продолжают частным образом оплачивать киберстраховки, покрывающие подобные выплаты[17].

Потребители косвенно платят за защиту. Например, они покупают страховку против мошенничества с кредитными картами или платят более высокие цены за обслуживание кредитных карт и продуктов, которые выступают как скрытые страховые премии на покрытие утечек данных. Важнее всего то, что издержки отдельного потребителя не зависят от его личных мер предосторожности. Предусмотрительный потребитель может подписаться на услугу, предоставляющую лучшую защиту от утечки данных, но эта дополнительная и зачастую недешевая мера предосторожности не снижает скрытых платежей за страховку, которые он платит. Стимулы для участия в программах, направленных против утечек информации, оказываются неэффективными.

Аспект общественного блага при предотвращении информационного загрязнения очевиден не только в контексте утечки данных. В целом люди, пользующиеся информационно насыщенной средой компьютерных сетей, имеют некоторую степень настороженности относительно влияния потенциального раскрытия своей частной информации [31]. Но какие бы меры защиты они ни предпринимали, все перекрывается (верным) пониманием того, что

[14] Договоры страхования могут смягчить и даже преодолеть проблему морального вреда путем создания соответствующих стимулов. См. в целом [54]. Ниже будет показано, как определенные формы страхования могут заменить государственное регулирование в вопросе информационного загрязнения.

[15] Стандартная политика страхования домовладельцев предусматривает несанкционированное использование кредитных карт или денежных переводов, включая подделку. См. [55]. Страхование от кражи личности представляет собой дополнительный инструмент в рамках прав домовладельцев; см., например, [56].

[16] См. [57]; см. также [58] («по осторожным оценкам, ущерб может составить 375 млрд долларов, по максимальным – до 575 млрд долларов»), [59].

[17] См. [60].

ISSN 2782-2923

информация тем или иным путем все равно станет общедоступной через действия других лиц. Если персональные данные все равно будут собираться из других источников – от друзей, провайдеров услуг, из предсказательной аналитики, – то частные лица не будут вкладываться в защиту информации.

Таким образом, в данном разделе мы попытаемся аргументированно показать, что существенная доля информационного ущерба является общественной, причем не только в производном, вторичном аспекте, как описано в литературе по частному праву, а именно что глубоко личные виды ущерба оказывают деморализующее и разлагающее воздействие на гражданскую деятельность отдельных людей, тем самым истощая общественные сферы и институты[18]. Напротив, мы покажем, что ущерб наносится непосредственно общественным экосистемам и зачастую не имеет никакого отношения к воздействию на тех конкретных лиц, чья информация при этом используется. Цифровая экономика производит цифровой смог, вопрос в том, что с этим делать.

3. НЕЭФФЕКТИВНОСТЬ ЧАСТНОГО ПРАВА

В разд. 2 была поставлена проблема информационного загрязнения, и в разд. 3 и 4 мы попытаемся ее решить. В начале разд. 3 мы показываем, чего делать НЕ следует – какие юридические подходы неэффективны в борьбе с информационным загрязнением. Это необходимый первый шаг, поскольку выясняется, что огромная доля существующих нормативных инструментов неэффективна. А именно мы покажем, что частное право не позволяет оптимально контролировать информационное загрязнение, как и те законодательные акты, которые призваны заставить людей осторожнее делиться своими персональными данными. Это обсуждение закономерно приводит к ряду более эффективных решений, описанных в разд. 4.

Неэффективность частного права в борьбе с информационным загрязнением представляет собой интересный феномен, поскольку права в отношении персональных данных всесторонне определены во множестве законодательных актов и являются предметом тщательно разработанного частного договорного права. Возникновению и реализации частных прав в области данных посвящена целая отдельная область права – законодательство о неприкосновенности данных. А самый распространенный тип потребительских контрактов – «политика конфиденциальности» на веб-сайтах и в приложениях, управляющая транзакциями с частными правами в области информации [61. Pp. 25–30]. Если базовые права настолько четки, а договорные отношения в этой сфере настолько широко распространены, почему же частное право оказывается неэффективным? Причины этого поясняются ниже, и они в точности соответствуют неэффективности частного права при регулировании промышленных загрязнений.

3.1. Неэффективность контрактации

Люди заботятся об экосистеме своих данных [32]. Обычно, если потребителей заботит какое-либо свойство продукта, компании конкурируют в стремлении предложить это свойство. Тогда перед нами загадка: почему информационное загрязнение не становится предметом преференциальных контрактов? Почему никто не торгуется за предотвращение выбросов данных?

Это тем более удивительно, что законодательство о неприкосновенности данных во многом ориентировано на поощрение договорных отношений между сторонами. Множество положений устанавливает возможность для компаний собирать и использовать персональные данные только в результате разрешения после заключения договора[19]. Ключевым положением Общего регламента ЕС по защите персональных данных (*Europe's General Data Protection Regulation, GDPR*) является требование к организациям, собирающим данные, предоставлять потребителям больше контроля над их персональными данными и дать им

[18] См. выше сноску 1.

[19] См., например, Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2018); Health Coverage Availability and Affordability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936; 45 C.F.R. § 164.502 (2018); Personal Information Protection Act, 815 Ill. Comp. Stat. 530/1 (2006); California Financial Information Privacy Act, Cal. Fin. Code. §§ 4050–4060 (законодательство запрещает финансовым институтам без согласия клиента распространять или продавать непубличную информацию, для которой можно идентифицировать личность владельца); California Online Privacy Protection Act, BPC § 2275.

ISSN 2782-2923

возможность ограничить и персонализировать их сбор.

Действительно, многие компании предлагают своим клиентам различные варианты контроля над данными. Например, некоторые предлагают «премиальное» обслуживание, за которое клиенты платят деньгами, а не данными [62]. У других имеются «пульты управления приватностью», где объясняется, какие данные собираются и с какими целями, а также предоставляется возможность отключить некоторые позиции[20]. Каждый веб-сайт, приложение и магазин имеют «политику обработки данных», объясняющую клиентам, какие данные собираются и как используются. Рыночная среда бурлит от заключения контрактов на обработку данных и наличия бесконечных возможностей для защиты персональной информации. Почему же в таком случае так распространено информационное загрязнение? По той же причине, по которой граждане не заключают достаточно контрактов по поводу промышленных загрязнений. Неспособность рыночной экономики производить контракты на общественно оптимальные уровни загрязнения объясняется тремя основными недостатками рынка: это внешние эффекты, дезинформация, ограниченная рациональность. Каждый из этих факторов в достаточной степени обсуждался в прошлом при объяснении неэффективности контрактации в сфере промышленных загрязнений (и в сфере общественного блага в целом), поэтому сосредоточимся на приложении этих факторов к контексту информационного загрязнения.

3.1.1. Внешние эффекты

Загрязнение наносит вред лицам, которые не являются сторонами транзакции. Например, при производстве мяса возникают токсичные отходы, но это никак не отражается на покупательских решениях, пока негативные внешние эффекты не станут ощущаться производителями и потребителями мяса и влиять на цену [64. Ch. 4; 65]. Даже при возникновении отдельных вспышек озабоченности, когда токсичность для окружающей среды слишком явно ассоциируется с конкретным продуктом и покупатели отказываются от него, реакция редко достигает такой силы, чтобы сравниться с величиной ущерба.

В разд. 2 мы показали, что выбросы информации подобны выбросам загрязняющих веществ – издержки часто являются внешними. Эти внешние эффекты относятся к фундаментальным недостаткам рынка, которые показывают, почему частные контракты не решают проблему информационного загрязнения. Действительно, люди постоянно заключают контракты в области информации, но с полным безразличием к проблеме информационного загрязнения. У них есть возможность предоставлять меньше данных – платить деньгами, а не личной информацией, – но они редко используют эту возможность, а также редко проявляют интерес к мерам по сокращению информационного загрязнения. Стандартные юридические нормы, запрещающие компаниям собирать персональные данные, методически оспариваются и отменяются – потому что потребители не склонны беспокоиться о потенциальной угрозе для своей частной жизни и не имеют никаких стимулов противодействовать общественному вреду.

В самом деле, исключения лишь подтверждают правило; в тех особых случаях, когда вред от утечки данных *не* является внешним, когда угроза частной жизни становится явной и острой, потребители проявляют больше склонности к заключению контрактов, направленных на сокращение информационного загрязнения. Как потребители не желают приобретать керосиновые обогреватели для домашнего применения, потому что они испускают загрязняющие вещества (ведь вред будет в первую очередь частным), так же они тщательно следят за наиболее чувствительными персональными данными и требуют для них большей защиты. Когда персональные данные собираются определенными «неудобными» сайтами – например, история поисков на сайтах для взрослых, – процесс регулируется более строгими стандартами в сфере защиты информации [66. P. 13]. Аналогично сервисы облачного хранения, которые предлагают удаленное хранение любых данных, применяют более жесткие меры безопасности (Там же. Pp. 30–35). Таким образом, когда ущерб является полностью частным, контракты составляются так, чтобы обеспечить более эффективную защиту данных (и снизить информационное загрязнение).

[20] Например, *Google's Privacy Checkup* [63] позволяет пользователям управлять настройками своих данных и ограничивать отслеживание данных через Google.

ISSN 2782-2923

3.1.2. Информация

Даже если ущерб является внутренним, контракты для оптимизации загрязняющих выбросов могут оказаться неэффективными из-за дезинформации[21]. Эта проблема, несомненно, гораздо шире, чем выбросы загрязняющих веществ. Вред от продуктов или их плохое функционирование различного рода может обнаружиться только после употребления. Два широко известных примера – употребление трансжиров и массовое использование грудных имплантатов. Поскольку многие опасные последствия (или гарантированные преимущества) от применения продуктов проявляются не сразу, их истинные причины оказываются неопределенными, что ведет к неэффективности контрактации.

Безопасность данных есть благо на доверии. Потребители не могут знать, насколько широко распространяются данные и насколько надежны меры защиты, пока не настанет кризис безопасности. Также они обычно не знают, какие именно данные собираются и кем [67. Pp. 1501–1502]. Если происходит утечка персональных данных, потребители часто не понимают, опасно ли это, и действительно, многие утечки не наносят вреда. Оценивая опыт своего взаимодействия с компанией, клиенты редко или вовсе никогда не рассматривают практику компании по обращению с данными, поэтому другие лица не могут основывать свои решения на этих факторах. Даже если потребители на своем опыте понимают вред, связанный с информацией, то обычно это частный вред. Люди по большей части не догадываются об общественном ущербе в этой области.

Во многих секторах рынка потребители пытаются компенсировать недостаток информации путем обращения к посредникам. Те, кого волнует загрязнение окружающей среды, запрашивают сертификаты и рейтинговые показатели вроде *ISO*, а те, кто заботится об утечке данных, могут получить подобную консультацию компании *TRUSTe*[22]. Однако такие сервисы предоставляют лишь часть информации. Они могут сообщить, какие данные собираются и охраняются, но они не указывают на возможные внешние риски. Кроме того, при формировании рейтингов они используют множество факторов, и потребители обычно не знают, каким весом обладает каждый из факторов. Например, иногда при оценке мер защиты приватности больший вес придается *обещаниям* компаний, собирающих данные, а не их реальным *действиям*[23]. Гораздо проще прочитать и оценить декларации о защите персональных данных, публикуемые компаниями, чем отслеживать реально применяемые меры защиты и реальные практики передачи данных[24]. Не зная, как в действительности определяется рейтинг, люди получают ложное чувство безопасности. Другими словами, рейтинговые сервисы также являются благом на доверии.

Наконец, если потребители плохо информированы относительно общего уровня риска какого-либо продукта, то гораздо менее вероятно, что конкуренция заставит компании заключать контракты, направленные на снижение этого риска. Выгоднее инвестировать в те очевидные качества продукта, которые создают конкурентные преимущества, чем тратить деньги на улучшение скрытых свойств. Кроме того, компании обычно не конкурируют в области тех рисков, которые потребители недооценивают, даже если снижение этих рисков эффективно. Например, компания, предлагающая высококачественную защиту против утечки данных, не будет рекламировать это преимущество, чтобы не насторожить потребителей относительно рисков, о которых они раньше не беспокоились. Эта настороженность может и вовсе отвратить потребителей от всего класса продукции. При этом компания

[21] Froomkin [18. Pp. 1732–1737] описывает «слепоту» относительно долгосрочного частного ущерба от раскрытия личной информации и неспособность людей признать истинную ценность информации для тех, кто ее собирает.

[22] Компания *TRUSTe* занимается оценкой и сертификацией рисков в сфере частной жизни. См. URL: https://www.trustarc.com/prod-ucts/enterprise-privacy-certification/

[23] Например, один из самых объективных сервисов такого рода – PrivacyGrade.org, разработанный университетом *Carnegie Mellon*. Он измеряет «разницу между ожиданиями людей по поводу работы приложения и его реальной работой» [68]. При этом высокие баллы по этому показателю получают приложения, в наибольшей степени загрязняющие информационную среду. Например, *Facebook** и *Strava* получили высшие баллы – возможно, причина в том, что у пользователей настолько низкие ожидания относительно охраны частной жизни в приложениях *Facebook** и *Strava*?

[24] Многие рейтинговые сервисы не проводят аудит вебсайтов относительно выполнения заявленных обещаний или стандартов [10. P. 65].

ISSN 2782-2923

с низким риском утечки данных может получить преимущество от возрастания своей доли рынка, превышающее потери от сокращения размера рынка.

3.1.3. Ограниченная рациональность

Еще одна причина неэффективности контрактов в сфере загрязнений – это неверные суждения. Ущерб от загрязнения окружающей среды – это классический случай неопределенного исхода со множеством когнитивных искажений. При оценке этого ущерба люди бывают чрезмерно оптимистичными или пессимистичными; они слишком бурно реагируют на отдельные события и затем забывают о них; они недооценивают отдаленные выгоды, но делают это непоследовательно; они становятся жертвами манипулирования; они иррационально стремятся сохранить статус-кво; они не любят узнавать или делать что-то новое и т. д. [69. P. 1597]. Достаточно сложно сделать правильный выбор, который действительно соответствует личным целям; часто для этого требуется тщательная оценка по многим параметрам. И эта задача становится непосильной, если другой стороной транзакции является умудренная организация, которая знает обо всех когнитивных искажениях и сознательно умножает их, чтобы извлечь выгоду из неверных представлений отдельного человека.

Подобные уровни неопределенности возникают и в случае принятия решений относительно персональных данных, и такие решения также принимаются под влиянием ограниченной рациональности. Четко определить цифровые риски еще сложнее, чем токсичность химических соединений [10. P. 62]. Они не вызывают цифровых болезней или смертей; риски от утечки данных многочисленны, разноплановы и могут вызвать бесконечное число поведенческих отклонений [19. P. 509; 70]. Зачастую проявления вреда в этой сфере малозаметны и их легко недооценить; в иных случаях они бросаются в глаза и их можно переоценить. Даже если бы компании писали свою документацию о работе с персональными данными простым и понятным языком (что случается редко, а если случается, то текст обычно скатывается на уровень детей школьного возраста [71. P. 471], и тогда аспекты этой работы оставались бы сложными, запутанными, а также постоянно меняющимися. Как ни парадоксально, исследователи отмечают, что само наличие «предупреждения о защите приватности» на веб-сайте успокаивает тревогу клиента и повышает его доверие к сайту [71. Pp. 331–338]. И это несмотря на то, что такие предупреждения не несут какой-либо новой информации для клиентов и практически всегда устанавливают меры защиты ниже уровня стандартных правил, которые действовали бы по умолчанию при отсутствии такого предупреждения.

Потребители часто полностью игнорируют проблему защиты информации из-за трудности принятия рациональных, информированных решений. Является ли такое массовое безразличие иррациональным? Или, напротив, оно рационально, учитывая непомерную сложность таких решений? Даже если бы люди хотели заключать продуманные контракты в сфере данных, уделять пристальное внимание управлению личной информацией, они не смогли бы этого делать по причине, которую автор вместе с Карлом Шнайдером (Carl Schneider) в другой работе назвали «проблемой количества»: каждое посещение сайта, каждое использование приложения, даже каждая физическая сделка ставят перед потребителем свой огромный объем проблем, связанных с информацией[25]. Проблемы нагрузки при каждой отдельной транзакции и их накопление при множественных транзакциях остаются неразрешимыми в рамках частной контрактации. И эти проблемы экспоненциально возрастают от того, что такое же внимание приходится уделять другим повседневным ситуациям заключения контракта, иногда гораздо более насущным. В современном мире, где техническая информация нарастает слой за слоем, кто может утверждать, что незнание и невнимание иррациональны?

Таким образом, контрактация неэффективна, и пути решения этой неэффективности не могут лежать в сфере контрактного права. Можно было бы предложить скорректировать неэффективность контракта «выбором архитектуры» – т. е. предположить, что поведенческая экономика может быть не проблемой, а решением. Однако такие половинчатые решения сталкиваются с серьезным противником, а именно компаниями, которые получают выгоду от доверчивости людей в вопросах передачи данных.

[25] См. [73]. По оценкам, средний гражданин ежегодно сталкивается с таким количеством документов о раскрытии информации, что для их прочтения понадобилось бы 76 дней, а денежные потери составили бы 781 млрд долларов. См. также [74].

ISSN 2782-2923

В конечном счете передача происходит на платформах, созданных теми, кто получает выгоду от владения информацией и в чьих интересах противодействовать любым законным требованиям, направленным против ее распространения. Стандартные нормы, направленные против таких компаний, оказались во многом неэффективными потому, что их очень легко отклонить, и многие компании хотели бы сделать это руками своих клиентов [75–77].

Нормы защиты данных были бы эффективными, если бы были обязательными, но это означает (парадоксальным образом), что единственный способ для контрактного права преодолеть неэффективность контракта – это полностью вывести этот аспект за рамки допустимой контрактации. В разд. 4 мы рассмотрим возможности создания таких обязательных норм. Чтобы частное право могло по-прежнему влиять на сферу обязательных норм защиты данных, жертвам необходимо дать полномочия по правоприменению. Поэтому далее мы рассмотрим, почему частное правоприменение неэффективно в сфере неотторжимых прав на нераспространение информации.

3.2. Неэффективность деликтного права

В разд. 3.1 было показано, почему контракты и рынок не способны обеспечить оптимальные уровни контроля над информационным загрязнением. Однако частное право может преодолеть неэффективность рынка с помощью иных инструментов. Он может перевести некоторые выбросы в категорию случаев, дающих основание для судебного иска, и предоставить частному правоприменению свободу действия. Информационное загрязнение может стать незаконным и в ряде случаев уже является таковым – например, когда компании собирают персональные данные без согласия их владельцев, используют данные недопустимым образом, допускают халатность при их хранении или участвуют в мошенничестве. Все это нарушает права граждан в отношении их личных данных и находится в сфере влияния деликтного права.

Однако деликтное право не способно справиться с этими правонарушениями, и причина этого та же, что и в случае его традиционной неспособности справиться с нарушениями в области охраны окружающей среды. Теоретически в случае промышленных загрязнений можно применять законодательство о причинении собственнику недвижимости помех и неудобств в пользовании ею [*nuisance law*]. Однако широко известно, что это законодательство оказалось неэффективным [26. P. 149]. Деликтное право оказалось неэффективным для предотвращения и компенсации ущерба от промышленных загрязнений по трем основным причинам: причинная обусловленность, оценивание, общественные внешние эффекты. Мы утверждаем, что те же причины являются ключевыми факторами неэффективности деликтного права для контроля информационного загрязнения.

3.2.1. Причинная обусловленность

Деликтное право эффективно в тех случаях, когда можно непосредственно и явно увидеть ущерб. Ущерб от загрязнения не является непосредственным: актуальной проблемой в делах о защите окружающей среды являются «отсроченные последствия» – скрытый ущерб, который трудно увязать с конкретными нарушениями [78. P. 919; 79. Pp. 293–294; 80. P. 131]. Нельзя назвать его и явным: можно доказать, что на территории загрязнения появились новые *риски*, но трудно доказать, что был нанесен реальный *вред* [20. P. 429].

Случаи утечки данных часто связаны с подобной проблемой неопределенности причинно-следственных связей. Рассмотрим нарушение безопасности, при котором финансовая информация о миллионах потребителей оказывается украденной с веб-сайта из-за халатности компании[26]. Несомненно, как только эта информация попадет в руки «воров идентичности», будет установлен частный ущерб конкретных лиц. Однако кто именно из этих миллионов людей станет реальной жертвой? Суды, да и сами жертвы могут никогда не получить необходимой информации об этом. Как правило, судебные дела начинаются сразу после утечки данных и до момента определения реальных жертв (и действительно, в таких делах зачастую – и обычно безуспешно – требуют компенсации

[26] Информационные выбросы отличаются от выбросов загрязняющих веществ тем, что основной причиной первых является намеренный взлом. Таким образом, ответственность компаний за утечку данных отходит на второй план. Тем не менее сбор и хранение чувствительных данных без адекватной защиты от хакеров может расцениваться как халатность, аналогично тому, как расценивают непреднамеренные предотвратимые утечки загрязняющих веществ.

ISSN 2782-2923

за возросший *риск*)[27]. Злоупотребление информацией может произойти спустя годы, а к тому времени будет сложно связать ущерб с конкретной утечкой данных. Нельзя будет выделить какой-либо один источник информации, который «с бо́льшей вероятностью» вызвал ущерб; многие утечки уже забудутся.

Любые попытки применить положения законодательства о халатности разобьются об отсроченное проявление вреда и неопределенность причинно-следственных связей. Те же причины блокируют и более амбициозные предложения по распространению действия деликтного права на сферу информационного загрязнения. Например, иногда утверждают, что установление более строгой ответственности за халатность заставит компании более тщательно следить за утечками данных. Если жертвам не придется собирать доказательства халатности компании, то им будет проще получить компенсации по гражданским правонарушениям, что, в свою очередь, «заставит операторов баз данных полностью интернализировать издержки от своей деятельности» [82. Pp. 241, 266]. К сожалению, введение строгой ответственности по гражданским правонарушениям не отменяет доказательства причинно-следственных связей. Если не удается установить причинно-следственную связь между конкретной утечкой данных и конкретными жертвами, то не будет и желаемых превентивных и регулирующих эффектов от введения строгой ответственности. В деликтном праве наступлению ответственности препятствует неадекватное доказательство ущерба, а не халатности.

В принципе, в рамках деликтного права можно добиваться компенсации жертвам за подвергание риску ущерба, а не за сам ущерб – если будет доказана общая вредоносность от утечки информации. Таким образом, речь будет идти о компенсации рисков от информационного загрязнения, а не реально возникшего вреда. Однако зачастую в судебном процессе оказывается невозможно представить информацию такого рода, поскольку причиняемый вред является скрытым [83. P. xi; 84. P. 601; 85. P. 1452]. Если бы такую информацию было несложно представить (а в контексте нарушения безопасности данных это, вероятно, можно осуществить, поскольку лица, чьи данные украдены, подвергаются известному риску кражи идентичности). Тогда можно было бы воспользоваться статистическими данными для оценки совокупного ущерба всех пострадавших и присудить пропорциональные доли компенсации каждому. Будучи основанной на надежной статистической информации, такая схема могла бы стать оптимальной превентивной мерой [86. Pp. 115–118]. Например, по оценкам Департамента юстиции, в среднем ущерб от кражи идентичности составляет 1500 долларов на человека [87]. Чтобы вынести решение по деликтному делу о нарушении безопасности веб-сайта, суду понадобится экспертное заключение для оценки прироста вероятности кражи идентичности среднего члена всего пула пострадавших. Имея такую оценку, можно назначить компенсацию для всех пострадавших.

Однако такие иски о компенсации рисков, вероятно, не будут успешными в контексте информационного загрязнения по тем же причинам, что и в случае промышленного загрязнения[28]. Такие иски уже подавались и безуспешно[29]. Суды чрезвычайно редко выносят решения в рамках деликтного права о компенсации ожидаемого вреда[30], чаще это встречается в публичном праве (например, штрафы за превышение скорости). Для частных истцов упреждающие обе-

[27] См., например, Indep.Cmt. Bankers of Am. V. Equifax, Inc. 1:17-cv-04756-MHC (N.D. Ga. Feb 20, 2019). См. также [81].

[28] Дальнейшее объяснение см. [88. Pp. 491–493] («Суды обеспокоены практикой вероятностного определения причинно-следственных связей в вопросах, касающихся ущерба от опасных веществ... Суды опираются на механистические определения причинно-следственных связей, а вероятностные определения могут вводить их в заблуждение»). Однако см. Norfolk & Western Railway Company v. Ayres, 538 U.S. 135 (2003).

[29] Этот аспект является ключевым для определения исковой правоспособности в федеральном суде, однако решения судов по вопросу актуального и будущего вреда в делах об утечках информации были непоследовательными. Истцы утверждают, что утечка данных «создает риск ущерба в будущем, например, кражи идентичности, мошенничества, репутационного вреда» и что они ощущают обеспокоенность по поводу таких рисков [89]. Анализ судебных решений по поводу возрастания риска будущего вреда см. [90. P. 226].

[30] Некоторые суды отказываются принимать какие-либо статистические данные в деликтных исках. См. [78. P. 857]. См., например, Smith v. Rapid Transit, Inc., 58 N.E.2d 754 (Mass. 1945) (вынесено решение, что статистические данные сами по себе не являются доказательством вины автобусной компании). См. также [91. P. 374].

ISSN 2782-2923

спечительные меры имеют небольшое значение, они чаще используются такими структурами, как Федеральная торговая комиссия (*FTC*) или генеральные прокуроры штатов. Поэтому главной целью разд. 4 будет разработка схемы обеспечительных мер для компенсации возросших рисков в случае утечки данных; таким образом, мы предлагаем решать проблему информационного загрязнения на основе публичного права.

3.2.2. Оценивание

Вторая проблема, возникающая при определении деликтной ответственности за загрязнения, – это проблема оценивания. Даже когда влияние загрязняющего выброса доказано, оценить его можно лишь количественно, а не в денежном выражении. В области экологических загрязнений проблема оценивания привела к тому, что в деликтном праве появились произвольные исключения, основанные на доказательствах правомерности оплаты убытка[31]. Явные *физические* проявления вреда позволяют получить компенсацию за некоторые виды убытков, потому что их можно оценить. Кроме того, проблемы оценивания можно преодолеть, если решения направлены на восстановление, а не на компенсацию [93. P. 1901]. И даже если некоторые убытки от загрязнения можно подсчитать (например, убытки рыбаков из-за разлива нефти), другие крупные потери возникают из-за вреда всей окружающей экосистеме и подсчитать их труднее.

В контексте информационного загрязнения проблема измерения ущерба еще сложнее. Люди заявляют, что безопасность данных важна для них, но часто действуют вразрез с этими заявлениями – это парадокс приватности[32]. Должно ли деликтное право компенсировать им ущерб на основе их заявлений или их поступков? Эта проблема с частным оцениванием возникает из-за глубокой неопределенности относительно частных последствий утечки персональных данных – кто и как воспользуется такой утечкой, каковы будут последствия незаконного использования данных. Даже если ущерб удастся проследить (как в случае кражи идентичности в результате конкретного эпизода утечки), восприятие финансового ущерба может кардинально отличаться от реальности.

Дела об утечках данных регулярно сталкиваются с проблемой демонстрации доказуемого ущерба. В типичном деле о нарушении безопасности данных истцы указывают на причинение эмоционального вреда, а также на риск частного ущерба в будущем, однако многие суды расценивают такой ущерб как слишком умозрительный, чтобы его компенсировать, и отказывают в иске [94. Pp. 960–962][33]. Даже издержки жертв нарушений безопасности данных на мониторинг их финансовой информации были расценены как недостаточные для рассмотрения дела, поскольку «затраты на рассмотрение спекулятивной цепочки будущих событий, основанной на гипотетических будущих преступных деяниях, являются не в большей степени “реальным” ущербом, чем предполагаемый “возросший риск ущерба”»[34].

Трудность оценивания индивидуального ущерба и распределения денежной компенсации между жертвами можно не принимать во внимание, если целью деликтного права является не столько компенсация, сколько предотвращение вреда. Виновника загрязнения можно заставить платить, даже если жертвы не смогли объединиться. Такое разделение ответственности и компенсации можно осуществить, например, с помощью схемы *cypres* [лат. «близко к этому», т. е. настолько близко к желанию учредителя доверительной собственности, насколько это возможно. – Прим. переводчика], когда в рамках группового иска суд назначает не подлежащие распределению доли компенсации третьим сторонам – бенефициарам, представляющим интересы своей группы[35]. Однако такие методы являются исключением и применяются короткое время. Считается, что они недопустимым образом раздвигают границы конституционных полномочий суда в области вынесения решений по

[31] Для исключения некоторых видов ущерба суды используют стандартные критерии доказанности. См. [92. Pp. 319–321] (приводится обзор относительно низких значений общих компенсаций, присужденных за ущерб в сфере экологии).

[32] См. выше сноску 2.

[33] См., например, Beck v. McDonald, 949 F.3d 262 (4th Cir. 2017); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo 2009).

[34] Reilly v. Ceridian Corporation, 664 F. 3d 38 (3d Cir. 2011).

[35] Nachshin v. AOL, LLC, 663 F.3d 1034, 1038 (9th Cir. 2011); [95, 96] (приводятся примеры дел).

ISSN 2782-2923

частным делам[36]. Действительно, именно в контексте дела об информационном загрязнении Верховный суд рассматривал законность такой модели частного правоприменения[37].

По существу, проблема оценивания возникает из-за внешних, общественных воздействий информационного загрязнения. Вред, наносимый различным общественным благам, который обсуждался в разд. 2, сложно перевести в плоскость денежных компенсаций, присущую частному праву. Остается неясным, кто именно должен заявлять иски, каков конкретный ущерб, и в конечном итоге сложно оценить общий вред.

3.2.3. Общественный вред

Третье значительное препятствие для регулирования информационного загрязнения средствами деликтного права состоит в широте общественного воздействия будущего вреда. Существование общественных внешних эффектов – ключевой фактор нашей позиции о неспособности контрактации оптимально решить проблему информационного загрязнения. В целом внешние эффекты не обязательно приводят к неэффективности деликтного права – напротив, деликтное право является первоочередным социальным инструментом для интернализации негативных внешних эффектов. Однако загрязнение представляет собой особый тип внешних эффектов, слишком широко распространенный, чтобы контролироваться деликтным правом[38].

В контексте охраны окружающей среды вред, нанесенный воздуху, общественным землям или водам, не приводит к конкретным реакциям в форме частных компенсаций. На самом деле деликтное право не всегда оказывается неэффективным: доктрины о нарушениях частного и общественного порядка, доктрина общественного доверия, урегулирование по системе *cy pres* позволяют в рамках деликтного права добиться возмещения общественного вреда[39]. Кроме того, ученые предлагают инновационные пути распространения деликтной модели возмещения частного ущерба на общественный вред[40]. Несмотря на это, деликтное право по-прежнему ограничивает частные иски областью частного ущерба [101; 20. P. 428]. Например, чтобы получить возмещение за нарушение общественного порядка в рамках доктрины общественного доверия, по-прежнему необходимо частное правоприменение [99. P. 1093]. В контексте охраны окружающей среды деликтоподобное возмещение за ущерб, нанесенный природным ресурсам, потребует огромных сумм на восстановление поврежденных природных ресурсов, но это возможно только для общественных организаций в рамках доктрины общественного доверия [102]. В целом общепризнано, что «законодательство об охране общественного порядка не способно выполнить задачу защиты окружающей среды» [20. Pp. 428–429; 26. P. 149][41].

Как и экологические загрязнения, выбросы данных наносят общественный вред. Это негативные внешние эффекты, которые обсуждались в разд. 2, – ущерб от баз данных и аспекты вреда для общественного блага, происходящие от торговли информацией. Вред, нанесенный целостности американских выборов в результате действий с данными *Facebook**, был чисто общественным – он отразился не столько на каком-либо отдельном пользователе, сколько на политической экосистеме. Какое из средств деликтного права могло бы возместить его? Ущерб жертв утечки финансовой информации выражается главным образом в возрас-

[36] Спорность конституционных оснований распределения компенсации по принципу *cy pres* была отмечена председателем Верховного суда John Roberts, который заявил о «фундаментальных сомнениях по поводу использования таких средств при рассмотрении групповых исков». Marek v. Lane, 134 S. Ct. 8, 9 (2013), cert. denied (No. 13–136).

[37] См., например, Frank v. Gaos, 139 S. Ct. 1041, No. 15–15858. В этом деле *Google* выступал ответчиком за передачу поисковых данных пользователей третьим сторонам.

[38] В индустриальном контексте такие внешние эффекты, как загрязнение, послужили первоочередной причиной, по которой правоприменение законодательства об охране окружающей среды перешло из системы деликтного права в публичное право. См. [97. P. 379, N. 2; 98. P. 29].

[39] Обсуждение истории и применения доктрин общественного доверия и нарушения общественного порядка по отношению к охране окружающей среды см. [99].

[40] Например, новая мера ущерба – «общественный ущерб» – может быть отнесена (как часть частного деликтного иска) на не истцов, чтобы компенсировать ущерб жертвам того же правонарушения, которые не являются членами судебного процесса, или чтобы способствовать общественным интересам, пострадавшим от данного правонарушения. См. [100].

[41] Аналогичным образом, доктрина нарушения общественного порядка оказалась неэффективной для охраны окружающей среды в Великобритании в XIX в.

ISSN 2782-2923

тающем ощущении небезопасности; это также такой тип ущерба, для которого деликтное право не предлагает средств возмещения, и он уже неоднократно отклонялся судами. А ущерб от стереотипов и дискриминации, которые испытывают люди с именами, похожими на имена чернокожих, когда при поиске получают ссылки на информацию, связанную с тюрьмами, – это такой глубоко общественный ущерб, что трудно даже представить, как его можно возместить средствами деликтного права. Как и в случае ущерба для природных ресурсов, схема компенсаций при информационном загрязнении должна основываться на публичном правоприменении.

3.3. Неэффективность обязательного раскрытия информации

Между этими двумя столпами частного права – контрактами и деликтами – располагаются многочисленные нормы публичного права, призванные помочь людям самим защититься от злоупотребления информацией. Множество федеральных законов и законов уровня штатов требуют от компаний, собирающих и обрабатывающих персональные данные, раскрывать детали своих практик клиентам. Такое обязательное раскрытие информации опирается на широко распространенную, но нереалистичную веру в то, что люди смогут дать свое «информированное согласие» на эти практики. Например, Закон о защите конфиденциальности пользователей видеоматериалов (*the Video Privacy Protection Act*) запрещает провайдерам услуг распространять персональные данные клиентов без их письменного согласия (штраф составляет 2 500 долларов за каждое нарушение), в результате чего документы о раскрытии информации скрупулезно включаются во все членские соглашения[42].

Подобным же образом обязательное раскрытие выступает основным ответом на все нарушения безопасности в сфере информации. Как только происходит утечка, пользователи, которых это касается, получают уведомление в надежде, что они смогут принять меры предосторожности и снизить ущерб. Например, в штате Калифорния требуется производить раскрытие информации «в наиболее целесообразное время», сообщение должно иметь заголовок «Уведомление о нарушении безопасности в сфере данных» и включать четко озаглавленные разделы, такие как «Что произошло», «Какие данные затронуты», «Какие меры мы предпринимаем» и «Что вы можете сделать», оно должно преподноситься в формате, который бы «привлекал внимание к сути и значению содержащейся информации»[43].

Без сомнения, обязательное раскрытие информации является основным регулятивным подходом в американском законодательстве о неприкосновенности данных [103]. Будучи само по себе общественной формой регулирования, обязательное раскрытие информации также широко известно как обязательное условие частной контрактации и частного контроля, а его нарушение часто является деликтом.

Ничто не указывает на то, что обязательное раскрытие информации о порядке обращения с данными как-то влияет на поведение людей в информационной сфере или что их согласие на обработку данных становится более информированным. Фактически имеются достаточные основания считать, что ни одна из этих задач не решена [73. P. 69; 104]. Требования об уведомлениях оказываются неэффективными потому, что они изначально используют два механизма защиты от утечек данных, которые, как мы показали выше, обречены на неудачу. Требование информированного согласия использует защиту через контракт в надежде помочь людям сохранить наилучшие достигнутые договоренности. А требование уведомления о произошедших утечках использует деликтное право, что дает возможность людям узнать о возникших рисках, принять меры предосторожности и добиваться компенсации. Однако потребители не стремятся заключать наилучшие контракты. И какими бы своевременными ни были уведомления о произошедших утечках, в распоряжении потребителей очень мало или совсем нет мер предосторожности, которые они могли бы принять после получения уведомления, а деликтные иски о возмещении ущерба, как правило, безуспешны.

Нет ничего удивительного в неэффективности раскрытия информации при утечках данных. В случаях экологических загрязнений этот метод также не внушает больших надежд. Например, законопроект 65

[42] 18 U.S.C. § 2710.

[43] Cal. Civ. Code § 1798.29, 1798.82; см. также, Cal. SB-46, Ch. 396.

ISSN 2782-2923

штата Калифорния устанавливает требование предупреждать о канцерогенах; его широко критикуют за многочисленные недостатки и сомнительные преимущества [105; 106. P. 1248]. Публичное раскрытие информации при выбросах токсичных веществ может заставить власти принять меры после случившегося, но думать, что эти уведомления способны снизить выбросы или помочь получить компенсацию по суду, было бы, как выражаются некоторые авторы, «преувеличением» [107, 108].

Согласно широко распространенному, но наивному представлению, если бы раскрытие информации было упрощено или более четко направлено, оно могло бы помочь людям делать более правильный выбор. Если документ о раскрытии информации слишком длинный – сократите его. Если он написан слишком техническим языком – сделайте его понятным для потребителя. Если его трудно читать – улучшите форматирование. Поэтому регулятивные усилия в области защиты информации во многом фокусируются на поощрении «лучших практик» презентации раскрытия данных[44]. Однако результаты вызывают разочарование. Если необходимо принять трудное решение, то упрощение формата никак не может значимо повлиять на то, насколько хорошо люди поймут все последствия такого решения. Кроме того, если вредоносный эффект наступает в результате коллективных действий всех участников процесса, а затем влияет на всю экосистему, то зачем вообще трудиться читать даже самый простой документ о раскрытии информации?

4. ОБЩЕСТВЕННОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОГО ЗАГРЯЗНЕНИЯ

Модель загрязнения, если применить ее к ущербу от выбросов данных, является мощным инструментом, который мы использовали в разд. 3, чтобы объяснить, почему частное право не подходит для решения проблемы, обозначенной в разд. 2, а именно внешнего вреда, причиняемого данными. Будет ли модель загрязнения настолько же полезной для определения путей решения в рамках публичного права? Можно ли позаимствовать модель регулирования охраны окружающей среды для конструирования законодательства в сфере информационного загрязнения? Изучим эти вопросы в следующем разделе.

По первому размышлению может показаться, что основные методы, используемые для регулирования загрязнения в экологическом законодательстве, плохо применимы к экологии данных. Между физическим и цифровым загрязнением существует принципиальная разница. Во-первых, физическое загрязнение часто поддается очистке, а цифровое, вероятно, нет. Поэтому бессмысленно создавать «суперфонды» для ликвидации последствий утечки данных[45]. Во-вторых, последствия экологического загрязнения всегда негативны (даже если оно произошло в результате положительной деятельности), тогда как выбросы данных могут быть и благотворными – информация создает также огромные положительные внешние эффекты. Экологическое законодательство запрещает использование веществ, обладающих чрезмерной токсичностью для человека; это невозможно по отношению к информации. В-третьих, влияние на экологию может быть измерено научными методами для проведения анализа затрат и выгод; в сфере же информации внешние эффекты часто являются качественными и гипотетическими. Как измерить ущерб от нарушения президентских выборов или от дискриминационных расистских предложений при поиске в Сети?

Видя эти различия, можно подумать, что принципы законодательного реагирования в сфере экологии невозможно перенести в сферу информации – например, просто создав аналог агентства по охране окружающей среды (*Environment protection agency, EPA*) для защиты данных (*Data protection agency, DPA*) с предоставлением ему тех же полномочий по борьбе с информационным загрязнением. Однако, несмотря на значительные различия, в экологическом праве существуют способы создания общественных практик для борьбы с общественным ущербом, которые мы и опишем в данном разделе. Фактически инструменты экологического права представляют собой конкретные приложения более общих регулирующих принципов,

[44] См., например, [109–111].

[45] На самом деле очистка часто неэффективна и в контексте охраны окружающей среды. Практически невозможно ликвидировать загрязняющие вещества, достигшие подземных вод, или загрязнившие большие территории, или повлиявшие на состав воздуха.

ISSN 2782-2923

применимых к любым внешним эффектам. Сочетая эти абстрактные принципы с конкретным контекстом регулирования промышленных загрязнений, мы получим организующую парадигму публичного регулирования информационного загрязнения[46].

В определенном смысле то, что будет описано в настоящем разделе, не ново. В области защиты данных уже используются отдельные правоприменительные действия публичного характера; это делают агентства, уполномоченные регулировать некоторые последствия утечек данных. Например, Федеральная торговая комиссия (*FTC*) давно занимается защитой прав на информацию и недавно выступила с иском против *Facebook**, обвинив компанию в информационном загрязнении в форме фейковой рекламы. Однако деятельность *FTC* направлена в основном против жульничества и обмана, а такие нарушения обычно не вскрываются, если компании следуют своим заявленным практикам. Аналогичным образом агентства и общественные обвинители иногда расследуют наиболее вопиющие утечки данных, однако их полномочия в основном ограничены узким кругом правонарушений, таких как несвоевременная рассылка уведомлений об утечке данных[47].

Модель борьбы с загрязнениями средствами публичного правоприменения не нова и по другой причине – она является важным дополнением к частному правоприменению в области защиты приватности. Фактически в Евросоюзе существует развитая область публичного правоприменения частного права[48]. Европейский подход, как будет показано ниже, использует ряд принципов, известных как «принципы честного использования данных» (*Fair Information Practices*) [114. Pp. 1974–1975]. Они включают в себя различные запреты на сбор, использование, передачу данных, которые реализуются через такие требования, как ограничение по необходимости и назначению, а также через запреты на укрупнение баз данных.

Модели публичного правоприменения используются в информационном праве. Однако они направлены на решение вопросов индивидуальной приватности, помогая людям контролировать их собственные персональные данные. Эти модели не могут решить проблему внешних эффектов от утечки информации. Если мы признаём, что информационное загрязнение является также общественной проблемой, так как нарушает всю экосистему, а не только личную жизнь владельцев информации, то это открывает новые богатые перспективы для существующих решений и позволяет предложить новые варианты.

В настоящем разделе описан арсенал мер публичного права по борьбе с внешними видами ущерба. Эти меры разбиты на три категории, что отражает три основных метода, используемых в экологическом законодательстве. Первый из них – командно-административное регулирование, т. е. установление строгих ограничений на загрязняющую деятельность. Второй – налоги, т. е. решение проблемы внешних эффектов по принципу Пигу. Третий подход – разработка таких мер ответственности за утечку данных, которые обеспечили бы оптимальную профилактику и компенсацию.

4.1. Командно-административное регулирование

Основной метод регулирования экологических загрязнений – это запрет деятельности, вызывающей опасные загрязнения, превышающей установленные законом пределы. Это реализуется в первую очередь путем предписания количественных ограничений, требования получать разрешения или путем обязательного внедрения передовых технологий. Эти формы регулирования *ex ante* являются стандартными командно-административными методами и обычно эффективно выполняют свои ограничительные функции, но часто ценой значительных, иногда непредусмотренных издержек. Их можно применить в борьбе против информационного загрязнения – например, установить ограничения на виды информации, которую компании могут собирать, на цели использования этой информации, на методы ее хранения, передачи

[46] Как указывалось во введении, в более ранних работах делались предложения об адаптации правовых инструментов экологического законодательства к проблемам приватности информации. Например, Hirsch [21] исследует правовые инструменты, побуждающие стороны снизить вредоносный эффект от их работы с информацией. В настоящей статье блестящий анализ Hirsch'а дополнен рассмотрением ущербов, не относящихся к защите приватности, а также рассмотрением иных правовых инструментов.

[47] См., например, [112].

[48] В ЕС были приняты два закона о защите информации: Европейская директива о защите информации (*European Directive on Data Protection*) и Общий регламент по защите данных (*GDPR*).

ISSN 2782-2923

или опубликования. Эти рычаги регулирования должны быть направлены на идентификацию рисков и снижение вредных эффектов баз данных.

С самого начала следует решить концептуальную проблему. Экологическое законодательство обычно не регулирует факторы производства так же тщательно, как его результаты. Предприятие может использовать любые факторы, пока выполняет требования по выбросам. Например, согласно Национальному стандарту качества окружающего воздуха в рамках Закона о чистом воздухе (*National Ambient Air Quality Standards of the Clean Air Act*), агентство *EPA* устанавливает, сколько миллионных долей загрязняющего вещества может выбросить предприятие[49]. Можно предположить, что информацию нельзя разделить на входную и выходную – информация на входе та же, что потенциально окажется на выходе. Поэтому придется применять ограничения по объему и виду деятельности к начальному этапу производства информации, т. е. ограничивать данные, которые компаниям разрешено собирать.

Хотя информация не является токсичной в том же смысле, что промышленные вещества, аналогия с охраной окружающей среды продолжает действовать. Даже самые опасные промышленные загрязняющие вещества несут какую-то пользу [113, 115]. Например, асбест служит хорошим теплоизолятором и снижает пожароопасность зданий, а выбросы углекислого газа способствуют повышению производства сельскохозяйственной продукции в таких холодных районах, как Сибирь. При проведении анализа затрат и выгод учитываются положительные внешние эффекты загрязняющих веществ, что отражено в экологическом законодательстве. Внешние эффекты информации также амбивалентны. Даже в случае утечки данных (и при использовании их не с теми целями, с какими их первоначально собирали) они приносят пользу. Например, *Google Trends* – сервис, использующий поисковые данные *Google* для целей, отличающихся от целей сбора и хранения этой информации, – позволяет делать важные выводы о таких общественных явлениях, как распространенность медицинских и социальных проблем [116]. Аналогичным образом базы данных, собираемые сервисами по генетическому тестированию, могут принести как помощь, так и вред лицам, которые не давали им свои данные. Таким образом, ключевая проблема командно-административного подхода к вопросу информационного загрязнения состоит в том, как заранее определить, какие виды использования данных будут общественно вредны и должны быть ограничены. Может ли закон подняться до выполнения этой сложнейшей задачи?

По мнению ЕС, это возможно. В частности, различные количественные ограничения составляют ключевую часть *GDPR*. Основными принципами являются принципы «минимизации информации» и «ограничение задач». Регламент устанавливает требование «справедливого обращения» с данными исключительно с «конкретными, явными и законными целями»; и даже в таких случаях собранные данные должны быть «адекватными, релевантными и не чрезмерными по отношению к цели или целям, для которых они обрабатываются»[50]. Например, розничные магазины могут собирать персональные данные о покупках, совершаемых их покупателями, чтобы персонализировать предложения и улучшать процесс покупок; также они могут собирать информацию о методах платежа, чтобы ускорить процесс оплаты. Однако, согласно требованию «минимизации информации», им не разрешено собирать информацию о номерах водительских прав покупателей или об их социальных контактах, также они должны удалять данные тех, кто деактивировал свой аккаунт[51]. За исключением случаев использования для персонализированного обслуживания все личные данные должны быть анонимизированы или агрегированы.

Количественные ограничения регулируют не только сбор и хранение, но также обработку и различные способы использования данных. В настоящее время одним из основных видов использования баз данных стала их продажа или сдача в аренду третьим сторонам для различных целей. Такая передача данных может быть запрещена или, по крайней мере, ограничена правовыми методами. Примером такого использования, которое могло быть ограничено, явля-

[49] 42 U.S.C. § 7401; 40 C.F.R. 50.

[50] GDPR, Art. 5.

[51] Пример закона, ограничивающего хранение данных согласно принципу минимизации см. New York's Cybersecurity Requirement for Financial Services Companies, 23 NYCRR 500.13 (2018).

ISSN 2782-2923

ется передача данных компанией *Facebook** компании *Cambridge Analytica*. В законодательстве необходимо установить категории обстоятельств, при которых передача данных запрещена. Можно также ввести стандарты локализации данных – ограничения на передачу баз данных для хранения и использования в других странах[52].

Сложность с принципами «минимизации информации» и «ограничения задач» состоит в том, как определить «справедливые» и «законные» цели и что считать «адекватным, релевантным и не чрезмерным». Достаточно сложной задачей является уже приложение этих принципов к неприкосновенности частной жизни, что и делает *GDPR*; сложность возрастает, когда речь идет о внешних ущербах. В контексте приватности эти ограничения нацелены на восстановление контроля граждан над их персональными данными. В контексте информационного загрязнения эти требования должны быть обоснованы тем, что мы ожидаем наличия совокупных внешних эффектов от работы с базой данных. Это огромная проблема: в результате работы с большими данными обнаруживаются связи, о которых никто ранее не знал и не мог предвидеть. Кто мог предположить, что база данных интернет-запросов позволит предсказывать крупные эпидемии? [117]. Нахождение корреляций данных имеет огромные преимущества, и ограничивать использование баз данных только известными и ожидаемыми целями – значит ставить серьезные барьеры инновационному развитию.

Возможно, решение проблемы в том, чтобы применить количественные ограничения, подобные тем, что предусматривает *GDPR*, только к «чувствительным» данным или целям. Так, законодательство об охране окружающей среды и использовании природных ресурсов устанавливает ограничения в основном относительно обращения с наиболее токсичными веществами и наиболее уязвимыми территориями. Аналогичным образом законодательство об информационном загрязнении может быть направлено на процессы сбора и обработки таких данных, которые при недолжном использовании были бы наиболее токсичными, общественно вредными. Например, большой общественный вред могут нанести такие модели использования информации, которые подрывают основные конституционные принципы или противоречат законам против дискриминации. Повышенный уровень защиты данных может касаться сбора и обработки такой персональной информации, как расовая и этническая принадлежность, религиозные или политические убеждения, а также различная информация о здоровье и сексуальных предпочтениях[53].

Однако такие ограничения на сбор и использование чувствительной информации также являются палкой о двух концах: они защищают определенные группы от потенциальных угроз, но и лишают их потенциальных выгод. Так, большую ценность представляют выводы, основанные на больших данных, о распространении эпидемий среди бедных слоев населения или о влиянии дискриминации на уровень преступности и охраны правопорядка. Причем эта ценность не может быть до конца понята, пока соответствующие выводы не будут сделаны на основе больших данных. Если ограничения на использование данных будут препятствовать созданию нового знания, то может возникнуть непреднамеренный эффект, когда защищаемые группы будут лишены положительных аспектов такого знания. Поскольку данные производят как позитивные, так и негативные внешние эффекты, административно-командные ограничения, направленные против последних, будут неизбежно отсекать и первые.

Еще один возможный путь уменьшить этот тормозящий эффект всеобщих количественных ограничений – это система индивидуальных разрешений, также применяемая в экологическом праве. Так, согласно Закону о чистой воде (*Clean Water Act*)[54], любой выброс определенных загрязняющих веществ в воду должен производиться по специальному разрешению. Аналогично можно установить требование получать разрешение на конкретные действия с информацией, которая несет в себе повышенные риски. Например, если веб-сайт хочет запустить алгоритм, получающий и использующий данные о расовой принадлежности клиентов, то должен будет получить разрешение, обосновав необходимость таких данных и доказав их безопасность для соответствующей группы населения

[52] GDPR, Art. 5.

[53] GDPR, Art. 9.

[54] 33 U.S.C. § 1342.

ISSN 2782-2923

Преимущество режима получения разрешений состоит в большей информированности: ограничения вводятся в зависимости от конкретных целей и обстоятельств сбора данных, а также от конкретных потенциальных ущербов, к которым может привести создание базы данных. Этот режим помогает решать проблемы после их возникновения, как, например, использование базы данных *Facebook** в политических целях. Также этот режим можно настроить для получения информации, необходимой законодателям. Аналогично тому, как предприятие должно предоставить данные о потенциальном влиянии своей деятельности на окружающую среду для определения возможных ущербов и издержек[55], так и потенциальные загрязнители информационной среды должны будут предоставлять информацию о своих целях и практиках, сообщая о вреде, который они могут нанести[56].

Регулирование через получение разрешений является одним из самых трудоемких и дорогих видов административно-командного регулирования; он имеет множество недостатков. Во-первых, это огромная административная нагрузка по проверке каждого информационного сервиса через системы вроде институциональных наблюдательных советов (*IRB*), что отрицательно сказывается на регулируемой деятельности. Во-вторых, лицензирующие органы, которые должны уравновешивать риски и выгоды, имеют тенденцию к чрезмерному регулированию (ущербы от запретительной деятельности менее выражены). В-третьих, если агентство не выказывает перекоса в сторону запретов, то оно может сконцентрироваться на формальных аспектах, например, требовать от компаний получения «информированного согласия» пользователей. Именно этим занимаются *IRB*, и эффективность их регулятивной деятельности никогда не была доказана [119. Гл. 4]. Для защиты от внешних эффектов она особенно бессмысленна.

Кроме использования режима получения разрешений, административно-командное регулирование может сосредоточиться на технологиях, которые компании применяют при работе с данными. Экологическое право контролирует выбросы путем поощрения передовых технологий. Предприятия, загрязняющие воздух, должны применять «наилучшие из доступных технологий контроля», чтобы добиться «наименьших из возможных уровней выбросов»[57]. В области работы с данными можно потребовать от компаний использовать технологии обработки данных и обеспечения безопасности с желаемыми свойствами[58]. Это помогло бы решить две основные проблемы информационного загрязнения – прозрачность и безопасность. Можно установить требование, чтобы алгоритмы, применяемые в персонализированных сервисах, отвечали стандартам прозрачности и позволяли уполномоченным органам наблюдать за процессом. Аналогичным образом проблемы безопасности данных можно решить с помощью требования «наилучших из доступных технологий».

Экологическое право признает неэффективность и тормозящее влияние количественного регулирования и иногда борется с этой проблемой через систему торгов. Ограничивая количественные показатели или требуя разрешений, можно уменьшить выбросы; система торгов выдвигает на первый план деятельность более высокого уровня. В дальнейшем эффективное производство достигается через систему ограничений и торговли квотами, потому что она поощряет предприятия, производящие выбросы, совершенствовать свои методы контроля над загрязнениями [120, 121].

Могут ли ограничения на выбросы данных стать предметом торгов? Вероятно, нет. Система ограничений и торговли квотами оказалась эффективной мерой контроля загрязнений воздуха потому, что была определена конкретная группа загрязняющих объектов – электростанции общего пользования; каждый объект получил детально прописанное разрешение на выброс одного загрязняющего вещества – диоксида

[55] National Environmental Policy Act of 1969, 42 U.S.C. §§ 4321–4347.

[56] Froomkin [18. Pp. 1745–1747] предлагает ввести обязательное «Уведомление о влиянии на безопасность частной жизни» по образцу существующих требований Закона о национальной экологической политике (NEPA), аргументируя, что это «создаст условия для более обоснованного обсуждения». В отличие от анализа, представленного в настоящей статье, Froomkin видит корень проблемы во влиянии на индивидуальную приватность, а не в ущербе для всей экосистемы, который подобен ущербу от загрязнения. См. в целом [118].

[57] 42 U.S.C.S. §§ 4321–4347.

[58] Hirsch [21. P. 37] предлагает обязать компании, собирающие данные, самим разрабатывать рентабельные методы борьбы с утечками и «приводить эти действия в соответствие с требованиями законодательства».

ISSN 2782-2923

серы [122. Pp. 9–40]. Какие объекты и вещества соответствуют этой ситуации в сфере экономики данных? Электроэнергия производится несколькими крупными предприятиями, которые выбрасывают известные загрязняющие вещества, однако цифровые услуги может оказывать практически любая компания. Если вхождение на рынок цифровых услуг является почти бесплатным, как можно контролировать количественные показатели? Кроме того, принципы «минимизации информации» и «ограничения задач», которые лежат в основе ограничений на сбор данных, нелегко конкретизировать и определить в количественных величинах, поэтому сложно выделить четкие ограничительные линии, необходимые для торгов.

Проблема системы ограничений и торговли квотами в области информации не сводится к простому определению стоимости данных, а является более фундаментальной. Количественные требования направлены на ограничение аккумуляции баз данных, которые дают слишком много информации, слишком много власти, позволяют прибегать к манипулированию и повышают риск злоупотреблений. Именно объединение различных уровней информации создает общественный эффект (как положительный, так и отрицательный), что означает потенциальный ущерб от торгов. Например, если принцип минимизации информации не позволяет предприятию розничной торговли собирать данные водительских удостоверений клиентов или накапливать персональную информацию о лицах, не являющихся клиентами, то было бы ошибкой позволить этому предприятию покупать эти данные у третьих сторон. Предположим, закон о количественных ограничениях позволяет компании *A* собирать только информацию *X*, а компании *B* – только информацию *Y*, поскольку такое разделение устраняет некий общественный вред. Однако если компании *A* и *B* имеют право обмениваться этими данными (или сливаться), то в результате одна из компаний может получить всю информацию, обойдя запреты. Если основным источником загрязнений является компиляция данных, система торгов не сможет предотвратить эти загрязнения.

Если вероятность загрязнений возрастает с ростом баз данных, то целесообразно ограничить их рост. В настоящее время основной проблемой вокруг таких мегакомпаний, собирающих большие данные, как *Facebook** и *Google*, представляется их влияние на рынок и потенциальное антиконкурентное поведение. Но если крупные платформы с большей вероятностью вызывают непропорционально значительные внешние ущербы, то ограничение размеров становится обоснованным даже без явной демонстрации их влияния на рынок. Возможно, меры против крупных компаний могли бы стать хорошим первым шагом в рамках административно-командного подхода. Это позволит избежать проблемы, уже проявившейся в связи с *GDPR*, а именно применения к большим и малым компаниям одного и того же набора ограничений, что налагает непропорциональную нагрузку на малый бизнес, для которого фиксированные издержки становятся неподъемными[59].

Итак, поскольку существуют способы тонкой настройки количественных ограничений, в этом разделе мы покажем, что информационные потоки сложно контролировать должным образом через командные методы, запрещающие определенные области использования данных, так как это одновременно будет препятствовать сбору нужной информации [21. Pp. 33–37]. В рамках парадигмы защиты частной жизни, которая в настоящее время лежит в основе регулирования данных, ущерб от ограничительного регулирования во многом сглажен, потому что информационная платформа может продолжать свою деятельность, предоставляя своим пользователям больше «контроля». Ограничения, устанавливаемые законами об информационном загрязнении, не могут быть заменены требованиями пользовательского согласия или контроля, так как ущербу подвергаются не столько сами пользователи, сколько третьи лица. Введение обязательных ограничений при работе с данными может разрушить те важнейшие и до сих пор не раскрытые преимущества, которые дает информация.

4.2. Налог на информацию

Можно ли снизить загрязнение, не увеличивая при этом административную нагрузку и тормозящие эффекты административно-командного регулирования? Теоретически можно: с помощью использования цен,

[59] How Facebook* and Google Could Benefit From the G.D.P.R., Europe's New Privacy Law, New York Times (April 23, 2018). URL: https://www.nytimes.com/2018/04/23/technology/privacy-regulation-facebook*-google.html; https://www.nytimes.com/2018/04/23/technology/privacy-regulation-face-book-google.html

ISSN 2782-2923

а не количества в качестве объекта регулирования. Установление расценок – хорошо известный способ контролировать загрязнения. Внешний ущерб интернализируется через «налог Пигу» либо непосредственно на соответствующую деятельность, либо на конкретный продукт, который производится в рамках деятельности, приводящей к загрязнению.

В промышленном производстве большая доля загрязнений производится углеродом, поэтому налог на углерод – это яркий пример налога Пигу, который является общепризнанным эффективным способом регулирования загрязнений [123. P. 500]. В цифровой экономике топливом выступает информация, которая порождает деятельность и все выгоды от нее, но также и потенциальный вред. Таким образом, внешний ущерб может быть интернализирован через налог на информацию[60].

Самым естественным моментом для налогообложения является момент сбора данных. Рассмотрим сделку купли-продажи между розничным продавцом и покупателем. Когда покупатель покупает товар за наличные в физическом магазине, никакая персональная информация не собирается. Но если тот же человек покупает этот товар за ту же цену в онлайн-магазине, в сделке возникает мощный информационный компонент. Веб-сайт собирает и хранит данные о покупателе, включая его историю поиска, информацию об оплате, а возможно, и множество еще более интересных данных, полученных от его цифрового устройства[61]. Действительно, в случае такого «обмена» данными (и по большей части благодаря ему) сделка в онлайн-магазине будет соответствовать стандартным условиям контракта, разработанным специально для онлайн-торговли, которые не будут применяться к сделке с теми же товарами в физическом магазине. Если к цифровым сделкам можно применить развернутые условия контракта, то к ним можно применить и небольшое положение о налоге.

Как установить размер этого налога? Налог на углерод призван уравновесить социальный ущерб от углерода; аналогично налог на информацию должен уравновесить социальный ущерб от данных. Но на этом подобие заканчивается, поскольку концептуальные и практические различия становятся слишком большими. Социальный ущерб от углерода может быть очень неопределенным и спорным, но на базовом уровне поддается строгим оценкам[62]. Общество может организовать грубое измерение уровня выбросов, статистических корреляций и объемов ущерба. Социальный ущерб от информации измерить сложнее. Пока вред не нанесен, может быть невозможно предсказать, какие именно виды деятельности вызовут ущерб, не говоря уже о его величине.

Кроме того, в отличие от углерода, который создает преимущественно негативные внешние эффекты, информация может нести положительные общественные эффекты. Налог на данные, призванный снизить частные и общественные издержки от использования информации, нужно будет модифицировать с учетом этих положительных внешних эффектов. Отметим, однако, что, хотя информация несет множество непредвиденных выгод, некоторые из них не будут являться внешними эффектами, а значит, не должны уменьшать налог на информацию. У владельцев баз данных возникает мотив присвоить и монетизировать эти положительные внешние эффекты, продавая персонализированный доступ к этим выгодам. С негативными эффектами такого не происходит; у компаний, порождающих их, не возникает мотива их «присвоить». Для уравновешивания этой асимметрии необходимо вмешательство государства. Однако даже в условиях такой односторонней мотивации многие выгоды оказываются слишком размытыми и в целом перевес в сторону положительных внешних эффектов сохраняется. Информация является общественным благом, и если владельцы баз данных не получают всей выгоды от них, они не будут вкладывать в них

[60] Налог на информацию следует отличать от выплат за выбросы в виде спама на электронную почту, которые налагаются не на сбор информации и построение баз данных, а на конкретное использование этих данных. См. [21. Pp. 42–48; 124; 125. P. 304].

[61] Например, сайт Walmart.com [126] собирает *IP*-адреса, данные о местоположении, о типе оборудования и программного обеспечения, которые пользователь задействовал при совершении сделки, историю поиска в браузере. Через установку куки-файлов и маяков сайт Walmart.com может продолжать собирать информацию о поисках в будущем, даже если при этом не задействована электронная почта и пользователь не реагировал на рекламу.

[62] В настоящее время модели, применяемые для оценки общественных издержек, не учитывают всех важных физических, экологических и экономических влияний из-за недостатка точных данных. См. [127]; см. также [128].

ISSN 2782-2923

достаточно средств. В целом итоговая общественная ценность выбросов данных не равна нулю, учитывая, что административные издержки не слишком высоки, некоторая форма информационного налога или субсидии оправдана.

Детальная разработка модели налога на информацию выходит за рамки настоящего исследования. Возможно, практические сложности не позволят даже грубо определить общественные издержки, связанные с информацией, для вычисления размера адекватного финансового возмещения сбора и производства цифровой информации. И это не говоря уже о политических интересах, осложняющих и без того запутанную концептуальную проблему. Тем не менее было бы целесообразно установить для начала хотя бы небольшой налог на крупные базы данных. Даже чисто номинальный налог заставит компании задуматься о необходимости сбора конкретных данных.

В целом компании могут оценивать потенциальные выгоды от владения данными более точно, чем государство, однако последнее, вероятно, более чувствительно и внимательно к потенциальным ущербам. При существующем безналоговом режиме у компаний нет причин соотносить объемы их работы с данными с величиной ожидаемой выгоды, как и нет причин воздерживаться от «максимизации данных», т. е. от сбора всей доступной информации. Напротив, при командно-административном режиме возникает противоположная проблема: государству придется оценивать не только ущерб, но и потенциальную выгоду от информации, не имея необходимых средств для этого. Режим «небольшого налога» даст возможность учесть знания компаний о получаемых выгодах. При этом государство, имея некую грубую оценку конкретных рисков, связанных со сбором данных, может соответственно изменить этот налог.

Налог на информацию может отражать как количество, так и качество собираемых данных. Очевидно, что чем больше данных и о большем количестве людей собирает компания, тем выше будет налог. Кривая маргинального налога не обязательно должна быть линейной; она должна отражать маргинальные риски добавочных данных. Например, налоговая ставка может повышаться с ростом количества собираемых данных, отражая повышенные общественные риски (включая вопросы конкуренции), связанные с крупными базами данных. Логично, что размер налога на компанию *Amazon* и на местный книжный магазинчик может отличаться в расчете на одну единицу информации.

Налог на информацию может также отражать различную степень чувствительности данных. Налог на информацию о расовой принадлежности или медицинской истории пользователя может быть выше, чем налог на данные о его местоположении. Внутри же отдельной категории величина налога может зависеть от релевантности информации. Так, за сбор информации о медицинской истории больница заплатит меньше, чем спортзал, а спортзал – меньше, чем социальная сеть. Сбор биометрических данных может быть бесплатным, если работодатель использует его для предоставления доступа в здание, но облагаться налогом, если эта информация коммерциализируется. Данные о ДНК являются высокочувствительными, и компании, создающие банки генетических данных, могут порождать значительные внешние эффекты, как позитивные, так и негативные. Если сбор данных облагается налогом, то необходимо разрешить таким компаниям получать оплату за некоторые положительные внешние эффекты, создаваемые их базами данных.

Кто будет платить этот налог? Естественно предположить, что это будут компании, осуществляющие сбор данных. Однако по размышлению можно заключить, что его могут платить непосредственно лица, предоставляющие информацию. Налог налагается на транзакцию, и в терминах реальной экономики неважно, какая из сторон его уплачивает, поскольку он в любом случае будет включен в общую стоимость. Если налог на углероды выплачивает заправочная станция, то она назначит более высокую цену на бензин и перенесет по крайней мере часть налога на потребителей.

Учитывая это, мы видим убедительные причины обложить таким налогом тех, кто предоставляет информацию (потребителей), а не тех, кто ее получает. Первые предоставляют информацию не только о себе, но и о своих социальных контактах. Так, пользователи *Gmail* раскрывают не только свои электронные адреса, но и тех, с кем они ведут переписку[63]. Клиенты сайта

[63] В деле Daniel Matera v. Google Inc., No. 5:15-cv-04062 2016 WL 454130 (N.D. Cal. Sept. 4, 2015) лица, не пользовавшиеся сервисом Gmail, подали групповой иск против *Gmail* и его пользователя за раскрытие их электронных адресов без их согласия.

ISSN 2782-2923

Ancestry.com раскрывают генетическую информацию о своих родственниках. Пользователи *Facebook** создают порталы доступа к данным своих друзей: пользователь, имеющий тысячу друзей, дает доступ к большему объему данных, чем тот, кто имеет сто друзей, а значит, должен заплатить больше.

Предоставление данных сходно с использованием общего пастбища. Базы данных дают информацию не только о самом владельце данных и его ближайшем окружении. Поэтому стоимость участия в такой деятельности должна отражать ее влияние на социум. В типичном бытовом сценарии, включающем охрану природных ресурсов (например, рыболовство), мы беспокоимся об их чрезмерном использовании. Такая реакция на проблему охраны общего достояния аналогична налогообложению лиц, которые предоставляют данные, затрагивающие других.

Часто говорят, что информация – это новые деньги. Люди пользуются ценными цифровыми услугами, расплачиваясь личными данными вместо денег. Совсем недавно устройства навигации для автомобилей стоили от 200 долларов. Затем появились бесплатные приложения, за которые мы «платим» данными геолокации, которые представляют большую ценность для рекламодателей. Реальные деньги – это валюта, обладающая высокой личной ценой (уплаченные деньги нельзя использовать снова), но не имеющая внешних эффектов. Напротив, данные обладают низкой личной ценностью (персональную информацию можно предоставлять снова и снова), но потенциально высокой общественной ценностью. Даже те пользователи, которые неохотно предоставляют свои персональные данные в качестве оплаты за услуги и заботятся о защите своей частной жизни, будут использовать эту валюту независимо от ее общественного влияния. Налог на информацию, собираемый с пользователей, будет способствовать исправлению этого перекоса в выборе средств оплаты.

Такой режим налогообложения пользователей, в отличие от компаний, собирающих информацию, имеет также символический аспект. Он отражает нормативный сдвиг – проблема информационного загрязнения состоит *не* в защите частной жизни граждан, а в защите общественной экосистемы. В рамках парадигмы информационного загрязнения не лица, предоставляющие информацию, нуждаются в защите, а от них нужно защищать экосистему. Они слишком часто и легко предоставляют слишком много информации, и их следует ограничивать. Проблема не в том, что они сильно беспокоятся о защите своей частной жизни и не получают этой защиты, но скорее в том, что они слишком мало беспокоятся о раскрытии данных, способствующих информационному загрязнению, и тем самым производят это загрязнение. Действительно, факт использования данных в качестве оплаты часто не осознается. Ребенок, скачивающий приложение для игры *Angry Birds* за 99 центов, не понимает, что позже через это приложение будут скачиваться его персональные данные. Налог на информацию, несомненно, исправит это упущение и выявит скрытый смысл этого выбора для пользователей.

Налог на информацию может полностью перевернуть представление о «скидках на информацию», которые в настоящее время предлагаются пользователям и владельцам данных. Интернет-компании иногда предоставляют своим клиентам выбор – платить деньгами или данными. «Базовые» опции требуют меньше денег и большего объема персональных данных, премиум-аккаунты более дорогостоящие, но предполагают меньший объем или полное отсутствие собираемых данных[64]. Например, компании *AT&T* и *Comcast* предлагают тарифы широкополосного доступа по более высокой цене (примерно в два раза), но без сбора данных и без рекламы, основанной на этих данных [62]. Эти тарифы не пользуются спросом – подавляющее большинство пользователей предпочитают платить информацией взамен на скидку. Делая такой выбор, они игнорируют негативный общественный эффект информационного загрязнения и должны облагаться налогом на информацию. Тем самым схемы оплаты данными потеряют свою привлекательность.

Как уже говорилось, налог на информацию – это всего лишь идея, а не готовое для внедрения предложение. Практические трудности его введения очень велики, но, возможно, самый значительный повод для беспокойства – это вероятность того, что внешние выгоды информации намного превосходят наносимый ею

[64] Скидки за информацию – это частный случай более общей модели «оплаты за информацию», согласно которой компании должны будут платить пользователям за их персональные данные. См., например, [25].

ISSN 2782-2923

вред. Если это так, то объектами регулирования должны стать конкретные виды вредоносного использования данных, а не сами данные как общая категория.

4.3. Работа с утечками данных

Командно-административное регулирование и налог на информацию представляют собой два основных метода регулирования сбоев рынка на этапе создания базы данных. Они схожи с двумя центральными методами экологического права – количественной и ценовой регуляцией. Однако экологическое право имеет в своем арсенале еще одно мощное средство – законодательство об обращении с отходами. Помимо средств для контроля выбросов до их возникновения *ex ante*, имеются также сложные схемы управления ущербами *ex post*, особенно в случае непредвиденных выбросов.

Если в индустриальную эпоху выбросы токсичных отходов были крупной проблемой, то сейчас утечки данных быстро становятся главной социальной проблемой цифровой эры[65]. Согласно одному отчету, киберпреступность затрагивает полмиллиарда человек в год, потери во всем мире составляют 110 млрд долларов[66]. Утечки данных часто вызваны намеренным преступным взломом[67], и их можно предотвратить хотя бы частично с помощью более мощной защиты. Действительно, недавние законодательные акты обязывают компании придерживаться более высоких стандартов профилактики таких правонарушений [134. P. 1057; 135. P. 1]. Кроме того, даже если взлом произошел, величина ущерба может быть снижена за счет организационных мер, таких как сбор меньшего количества данных, своевременное удаление данных, активация мер снижения ущерба после взлома.

В экологическом праве ставится амбициозная задача на случай уже произошедшего выброса – очистка места утечки токсичных веществ[68], которая не имеет аналога в цифровой сфере. В целом последствия выбросов данных невозможно отменить. Цифровая материя существует не в отдельном, определенном, замкнутом пространстве. Ее можно бесконечно воспроизводить простым нажатием кнопки или одной строчкой алгоритмического кода. Выпустив информацию, ее нельзя собрать. Вместо этого законодательство должно сосредоточиться на других мерах по снижению ущерба, а также на мерах ответственности *ex post* для предотвращения таких ситуаций.

4.3.1. Снижение ущерба

Недавний резкий рост количества нарушений безопасности данных привел к соответствующему увеличению числа законодательных актов, налагающих ответственность на владельцев взломанных баз данных. Одна из таких обязанностей – «максимально срочное» раскрытие информации об утечке, уведомление государственных органов и пострадавших сторон; предполагается, что эта «открытость» будет способствовать скорейшей подаче частных исков жертвами для возмещения их ущерба[69]. Развитие таких схем уведомления о произошедших утечках составляет основное содержание различных предложений по борьбе с утечками данных[70].

Такие уведомления нельзя считать совершенно бесполезными [138]. Отдельные граждане могут предпринять меры для снижения своего частного ущерба от кражи их данных. Они могут активировать услугу отслеживания кредитов (оповещение о попытке мошенников оформить кредит на основе украденных данных), замораживания кредитов (блокировка открытия новых аккаунтов), блокировать и заменять украденные кредитные карты или номеров социального страхования, регулярно проверять отчеты по своим кредитам, вовремя оформлять налоговые вычеты и т. д. И все же

---

[65] Оценки ущербов от нарушения безопасности данных сильно разнятся. В докладе генерального прокурора Нью-Йорка [129] говорится, что «в 2012 г. в США прямые и косвенные потери от кражи идентичности составили 24,7 млрд долларов, что превосходит потери от всех остальных видов имущественных преступлений, вместе взятых». См. также [130. P. 7; 131; 132].

[66] См. выше сноску 17.

[67] По данным Центра исследований кражи идентичности (*Identity Theft Research Center*) [133], взлом с преступными целями составляет почти 60 % всех правонарушений в сфере информации, оставляя далеко позади все остальные виды таких правонарушений.

[68] Comprehensive Environmental Response, Compensation, and Liability Act of 1980, 42 U.S.C. §§ 9601–9616.

[69] См., например, Cal. Civ.Code § 1798.29(a), 1798.82(a); Consumer Privacy Protection Act of 2017, H.R. 4081 115th Cong. § 211

[70] Hirsch [21. P. 58] предложил принять новую федеральную программу *Data Release Inventory* (*DRI*), согласно которой компании должны будут ежегодно отчитываться об объемах данных, обнародованных как намеренно, так и ненамеренно. См. также [136, 137] (предлагаются правила оповещения об утечках данных для государственных органов).

ISSN 2782-2923

реакция потребителей на письменные уведомления о нарушениях безопасности остается в лучшем случае медлительной[71]. Это объясняется не ленью или каким-то неверным когнитивным суждением. Такое безразличие рационально, поскольку потребители в основном защищены системой частного или общественного страхования от финансовых потерь в результате нарушения безопасности данных [140; 141. P. 982][72]. Кроме того, это безразличие неизбежно в ситуации, когда такие уведомления выглядят как стандартный, очень длинный документ, как очередное раскрытие информации, которое все привыкли игнорировать [73].

Снижение ущерба от произошедших утечек данных может быть организовано без активного участия потребителей, но все же обычно требует их согласия. После нарушения безопасности данных пострадавшая компания может включить своих клиентов в программы защиты. Например, после массивной утечки данных компания *Equifax* предложила бесплатный мониторинг кредитов через программу *TrustedID*, включение в которую было очень простым. Согласно законопроекту о защите частной жизни потребителей (*Consumer Privacy Protection Act*), компании, допустившие утечку данных, должны будут «в течение пяти лет предоставлять услуги по предотвращению кражи идентичности и возмещению ущерба» бесплатно для любого, кто обратится за такими услугами (однако самостоятельная запись на такие услуги без обращения к компании по-прежнему запрещена)[73].

Меры возмещения могут снизить потенциальный частный ущерб лиц, чьи данные оказались доступными, но общественный вред будет по-прежнему значительным. Так, кражи идентичности и другие нарушения продолжают происходить. Кроме того, сами эти меры возмещения требуют затрат – люди теряют деньги и время как до, так и особенно после нарушения безопасности своих данных. Хотя реальный ущерб может понести лишь небольшая доля потребителей, абсолютно все страдают от усиления чувства финансового риска или от необходимости принимать затратные меры предосторожности. Действительно, жертва в среднем тратит около семи часов на ликвидацию проблем, вызванных кражей идентичности, а некоторые значительно больше. В целом 15 % людей переживали кражу идентичности хотя бы раз в жизни, а ощущение риска связано с сильным эмоциональным беспокойством [143. P. 1013].

Наличие большого количества социальных программ, нацеленных на уменьшение и предотвращение частного ущерба от утечек данных, является одним из механизмов, которые превращают информационное загрязнение из частной проблемы в общественную. Например, издержки от мошенничества с кредитной картой несет выпустивший ее банк, а не владелец карты. Однако эти издержки банк возмещает, повышая оплату своих услуг для других потребителей. В любом случае платят все клиенты: чем выше страховые суммы, встроенные в стоимость обслуживания кредитных карт, тем значительнее утечки данных. Это внешние эффекты страхования, которые мы рассматривали в разд. 2. Инструменты *ex post* регулирования эффективны для перераспределения убытков, но снижение убытков требует иных инструментов. Одним из них может стать система ответственности, другим – частное регулирование.

4.3.2. Ответственность за ущерб

Экологическое право налагает серьезную ответственность *ex post* на компании, допустившие утечку вредных веществ. Ответственность компании *Exxon* за разлив нефти из танкера «Эксон Валдез» измерялась суммой более 1 млрд долларов (не считая стоимости возмещения ущерба на сумму 507 млн долларов)[74], а разлив нефти на платформе *Deepwater Horizon* в 2010 г. стоил компании *BP* более 40 млрд долларов. Могут ли утечки информации повлечь настолько же серьезные меры?

В разд. 3 было показано, почему деликтное право не способно обеспечить ответственность компаний

[71] The Ponemon Institute [139] показал, что «самой частой реакцией на уведомление было игнорирование и отсутствие каких-либо мер».

[72] Благодаря страхованию последствия для жертв в основном сглажены. Согласно оценкам, около 25 % жертв правонарушений в сфере информации подверглись краже идентичности в результате этих правонарушений, а 14 % жертв кражи идентичности понесли личные финансовые потери в размере 1 доллар и более, при этом у половины из них потери составили менее 100 долларов. См. [142, 143].

[73] Consumer Privacy Protection Act of 2017, H.R. 4081 U5th Cong. § 211.

[74] Exxon v. Baker, 554 U.S. 471 (2008).

ISSN 2782-2923

за утечку информации. Проблемы неопределенности причинно-следственных связей, общественного ущерба, оценки затрудняют для потенциальных жертв рассмотрение дела в суде и получение компенсации за вред, нанесенный утечками данных. Однако система публичного правоприменения не ограничена подобными стандартами в области свидетельских показаний и возмещения ущерба. Меры ответственности могут отражать *ожидаемый* общественный ущерб, при этом жертвы не обязаны доказывать и оценивать свой фактический ущерб, а также не стоит проблема распределения суммы возмещения между жертвами.

Чтобы служить оптимальной превентивной мерой, мера ответственности должна отражать общий ожидаемый объем издержек, возникший из-за утечки данных. Будь то штраф по уголовному делу, выплаты по гражданскому иску или предусмотренный законом штраф по групповому иску, сумма должна равняться наиболее адекватной оценке *риска* для общества, вызванного утечкой данных. Это решит проблему отсроченного ущерба от утечек данных, если будут созданы инструменты комплексной оценки ущерба.

Один из таких инструментов комплексной оценки общественного вреда – проведение опросов. Например, по оценке Департамента юстиции, ущерб жертвы кражи идентичности составляет в среднем около 1 500 долларов [87]. Оценки вероятности кражи идентичности у лиц, пострадавших от кражи номеров социального страхования, могут различаться на 14–30 % [129]. Имея такие оценки, можно установить фиксированные выплаты каждому пострадавшему. Тогда общая сумма штрафа составит величину ожидаемого ущерба на одного пострадавшего, умноженную на количество пострадавших. Таким образом, штрафы за утечки данных могут быть установлены заранее, различаясь по сумме за кражу информации с кредитной карты, номеров социального страхования или другой чувствительной информации, аналогично тому, как установлены штрафы за различные виды потенциально опасной деятельности в зависимости от тяжести этой опасности.

Ответственность *ex post* можно очертить таким образом, чтобы сформировать нужную мотивацию. Величина штрафа может отражать финансовую чувствительность информации, количество украденных записей, степень халатности при их хранении, предпринятые меры для снижения ущерба и т. д. В настоящее время законодательные акты устанавливают различные стандарты защиты информации, и мера ответственности может быть снижена (и даже совсем отменена), если вина лежит не на пострадавшей компании. Стандарты могут также относиться к технической стороне защиты баз данных. Однако важнейшая их часть касается обоснования получения информации. Более высокие штрафы предусмотрены за утечку данных, которые собирались без достаточного обоснования.

В конечном итоге общая сумма ответственности всех компаний, допустивших утечку, должна равняться общей сумме ущерба всех жертв. Существуют надежные оценки такого ущерба – например, в одном из исследований ущерб от случая мошенничества с персональными данными в 2018 г. в США оценивается в 16,8 млрд долларов [144]; при этом единственная проблема, связанная с этим эпизодом, – как разделить сумму возмещения между компаниями, допустившими его. Доля вины каждой компании может рассчитываться по различным критериям в зависимости от количества или качества раскрытой информации или от наличия недостатков в системе безопасности. Деликтное право решает сходные проблемы распределения ответственности применительно к делам с совместными делинквентами или при параллельных правонарушениях, но законодательство об информационном загрязнении не может переложить такие решения на частные деликтные иски. Проблему неопределенности причинно-следственных связей, которая не позволяет установить меру ответственности в рамках деликтного права, можно решить при помощи модели ответственности, предписанной законом.

4.3.3. Обязательное страхование

Ответственность *ex post* может способствовать предотвращению правонарушений, но только в том случае, если компании в состоянии выплатить возмещение и обладают информацией, необходимой для выбора адекватных по стоимости мер предосторожности. В сфере кибербезопасности обе проблемы – платежеспособность и наличие информации – могут подорвать эффективность этого инструмента; угроза такого развития событий существовала и в области экологического права [145]. Поэтому необходимо страхование ответственности, способное решить обе указанные проблемы.

Общепризнано, что обязательная покупка страховки против возможного ущерба от деятельности

ISSN 2782-2923

заставляет субъектов этой деятельности, потенциально защищенных от наказания, учитывать внешние эффекты, которые они иначе игнорировали бы, например, стоимость ответственности, которую они иначе не могли бы выплатить. Страховка выполняет функцию налога Пигу: дифференцированные страховые премии, выплачиваемые компаниями, отражают различные внешние издержки, которые они порождают [54. P. 207]. Система обязательного страхования задействует эквивалент налога на информацию, который мы обсуждали выше; это делается не напрямую через государственную систему *ex ante*, а косвенно, когда страховщики оценивают риск наступления ответственности.

Менее известен профилактический эффект страхования ответственности. Считается, что страхование несет в себе риск злоупотреблений – что сторона, застрахованная против определенной угрозы, не имеет стимула снижать эту угрозу. Однако риск злоупотреблений возникает только в случае, если страховщики не могут отслеживать профилактические усилия, предпринимаемые застрахованными лицами, и соответственно менять стоимость своих услуг [146; 147. Pp. 168–169]. Если цены устанавливаются на основе точных статистических оценок ожидаемого ущерба с учетом реальных профилактических усилий, предпринимаемых застрахованными лицами, то у компаний появляется стимул снижать риски. Кроме того, страховщики могут на основе своих технических знаний рекомендовать своим клиентам наиболее эффективные и экономически обоснованные профилактические меры – этой информации не хватает многим сторонам коммерческих отношений.

Компании, занимающиеся страхованием ответственности в сфере кибербезопасности, проводят «проверки кибербезопасности», чтобы помочь своим клиентам «повысить уровень защиты данных» [148]. Используя точные методы, разработанные в страховой индустрии, они составляют рейтинги компании с точки зрения обеспечения безопасности, которые затем влияют на размер страховых премий и на получение рекомендаций по устранению проблем. Иногда страховщики тестируют систему защиты своих клиентов, пытаясь удаленно взломать ее. Они требуют от застрахованных компаний проходить аудиты и перенимать опыт третьих сторон. А также они достаточно быстро приступают к ликвидации последствий взломов систем безопасности, чтобы снизить объем ущерба и предусмотренных законом возмещений [148].

Страхование в сфере кибербезопасности представляет собой новую форму страхования коммерческой ответственности. Как и его гораздо более зрелый «родственник» – страхование ответственности в сфере охраны окружающей среды, – это специализированный инструмент, позволяющий возмещать ущерб третьих сторон, вызванный коммерческой деятельностью, который в ином случае был бы исключен из стандартного покрытия страхования коммерческой ответственности. Экологическое право содержит сложную систему управления рисками, согласно которой на объектах должны применяться меры профилактики, контроля и ликвидации последствий выбросов[75]. Но даже при наличии такой разработанной регулятивной основы система страхования ответственности в сфере охраны окружающей среды часто требует от компаний придерживаться более строгих частных экологических стандартов, чем те, что предусмотрены *EPA* [149. P. 477; 150; 54. Pp. 225–226]. Учитывая зачаточную стадию существования законодательства в сфере кибербезопасности, частная разработка стандартов снижения рисков могла бы стать значительным преимуществом, основанным на режиме строгой ответственности за утечку данных в сочетании с обязательным страхованием ответственности.

5. ЗАКЛЮЧЕНИЕ

Закон о цифровых данных должен касаться не только защиты частной жизни. Обмен данными между отправителем и получателем слишком часто затрагивает интересы третьих сторон; данные могут содержать информацию о других лицах; или, что еще важнее, базу данных можно использовать таким образом, что будут затронуты общественные интересы, помимо защиты частной жизни отдельных пользователей. Эта проблема носит название «загрязнение информационной среды», а законодательство в этой сфере – это комплекс правовых инструментов, призванный бороться с данным загрязнением.

Такое законодательство может позаимствовать ряд правовых решений, создававшихся для защиты частной

[75] Environmental Protection Agency; Oil Pollution Prevention Spill Prevention Countermeasure, 40 C.F.R. § 112 (2010).

ISSN 2782-2923

жизни, но чаще требуются другие инструменты. Например, два столпа законодательства о защите частной жизни – «пользовательский контроль» и «информированное согласие» – не применимы в законодательстве о загрязнении информационной среды. Эти инструменты используются в рамках смелого предположения, что они помогают людям защитить себя. Даже если бы это было правдой, нет оснований считать, что люди перестанут генерировать информацию, которая может нанести вред другим. Снизить уровень информационного загрязнения могли бы различные механизмы вмешательства, включая некоторые законы, уже принятые в рамках недавних реформ законодательства о защите частной жизни. Однако любое вмешательство имеет отрицательные последствия, уменьшая положительный эффект от распространения информации.

Таким образом, налог на информацию является, вероятно, самой инновационной технологией, способной снизить уровень информационного загрязнения. В этом законодательство о загрязнении информационной среды, очевидно, расходится с законодательством о защите частной информации. Если нарушения приватности необходимо остановить, то на информационное загрязнение нужно просто установить плату. Разработка рационального налога на информацию представляет собой крайне сложную проблему, и разд. 4 данной статьи содержит ряд первоначальных посылок для ее решения. Мы видим две относительно простые стратегии в этом направлении. Во-первых, необходимо прекратить вредоносную передачу данных за деньги. Люди постоянно получают оплату за свои персональные данные, в первую очередь в виде услуг, которые им предоставляют центры сбора данных; настойчиво высказываются предложения заставить компании платить гражданам за собираемую информацию [24, 25]. Это то же самое, что платить людям за загрязнение окружающей среды. Во-вторых, небольшой номинальный налог на данные помог бы прекратить бессмысленное накопление ненужной информации, которое тормозит важные инновации. Даже небольшой налог заставил бы сборщиков данных применить критическое мышление и снизить уровень информационного загрязнения.

Срочная необходимость в законодательстве о загрязнении информационной среды назрела потому, что в настоящее время законодательство о защите частной информации доказало свою полную неэффективность. Действительно, новые решения в законах о защите частной информации могут в будущем привести к успеху там, где прежние инструменты (в первую очередь раскрытие информации) были неэффективными. Возможно, люди станут больше заботиться о защите своей цифровой частной жизни. Однако обеспечение приватности не решает социальных проблем, связанных с информацией. Информационное загрязнение остается проблемой, даже если частная жизнь защищена.

Научная ценность представленной статьи не в том, что она решает проблему информационного загрязнения. Хотя мы и боремся против доминирования проблем приватности в сфере информационного законодательства, однако мы не призываем уделять меньше внимания защите цифровой частной жизни. Главным образом, мы стремились показать, что проблема информационного загрязнения существует. Если, как мы утверждаем, информационное загрязнение вызвано влиянием баз данных, то законодатели должны тщательно разграничить внешние эффекты данных и вред, наносимый приватности данных, и найти способы снизить социальные издержки от этих явлений.

Список литературы / References

1. Economist. (2017, May 6). Data Is Giving Rise To A New Economy. *Economist*. https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy

2. DeVries, Will Thomas. (2003). Protecting Privacy in the Digital Age. *Berkeley Tech. L. J.*, 18*, 283–311.

3. Isenberg, Howard. (1995). The Second Industrial Revolution: The Impact of the Information Explosion. *Ind. Eng., 27*, 14.

4. Granville, Kevin (2018, March 19). Facebook** and Cambridge Analytica: What You Need to Know as Fallout Widens. *The New York Times*. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

5. Schwartz, Paul M., Karl-Nikolaus Peifer. (2017). Transatlantic Data Privacy Law. *Geo. L. J., 106,* 115–179.

6. Westin, Alan. (1967). *Privacy and Freedom*. New York, NY, Atheneum Press.

7. Reiman, Jeffrey H. (1982). Privacy, Intimacy, and Personhood. In F.D. Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (pp. 300–316). Cambridge, UK: Cambridge University Press.

8. Schwartz, Paul M. (1999). Privacy and Democracy in Cyberspace. *Vand. L. Rev., 52,* 1609–1702.

ISSN 2782-2923

9. Cohen, Julie E. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Stan. L. Rev., 52,* 1373–1437.

10. Nehf, James P. (2003). Recognizing the Societal Value in Information Privacy. *Wash. L. Rev., 78,* 1–92.

11. Ashenmacher, George. (2016). Indignity: Redefining the Harm Caused by Data Breaches. *Wake Forest L. Rev., 51,* 1–56.

12. Solove, Daniel J. (2002). Conceptualizing Privacy. *Cal. L. Rev., 90,* 1087–1155.

13. Sunstein, Cass R. (2017). *#Republic: Divided Democracy in the Age of Social Media*. Princeton, NJ, Princeton University Press.

14. Sunstein, Cass R. (2018, January 22). Is Social Media Good or Bad for Democracy. *Facebook** Newsroom*. https://newsroom.fb.com/news/2018/01/sunstein-democracy/

15. Wittes, Benjamin, Jodie C. Liu. (2015, May). *The Privacy Paradox: The Privacy Benefits of Privacy Threats*. Center for Technology Innovation at Brookings. https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf

16. Hermstrüwer, Yoan. (2017). Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data. *J. Intell. Prop. Info. Tech. & Elec. Com. L., 8,* 9–26.

17. Athey, Susan et al. (2018). *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2916489

18. Froomkin, A. Michael. (2015). Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements. *U. Ill. L. Rev.*, 1713–1790.

19. Acquisti, Alessando, Brandimarte, Laura, Loewenstein, George. (2015). Privacy and Human Behavior in the Age of Information. *Science, 347*, 509–514.

20. Dewees, Donald N. (1992). The Role of Tort Law in Controlling Environmental Pollution. *Can. Public Pol'y, 18,* 425–442.

21. Hirsch, Dennis D. (2006). Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law. *Ga. L. Rev., 41,* 1–63.

22. Hirsch, Dennis D. (2014). The Glass House Effect: Big Data, the New Oil, and the Power of Analogy. *Me. L. Rev., 66,* 373–395.

23. Hirsch, Dennis D., Jonathan H. King. (2016). Big Data Sustainability: An Environmental Management Systems Analogy. *Wash. & Lee L. Rev., 72,* 406–419.

24. Kaiser, Brittany. (2018, April 9). Facebook** Should Pay Its 2bn Users for Their Personal Data. *Financial Times*. https://www.ft.com/content/7a99cb46-3b0f-11e8-bcc8-cebcb81f1f90

25. Posner, Eric, Glen Weyl. (2018). *Radical Markets*. Princeton, NJ, Princeton University Press.

26. Abraham, Kenneth S. (2008). *The Liability Century: Insurance and Tort Law from the Progressive Era to 9/11*. Cambridge, MA, Harvard University Press.

27. Thomsen, Simon. (2015, July 21). Extramarital Affair Website Ashley Madison Has Been Hacked and Attackers Are Threatening to Leak Data Online. *Business Insider*. https://www.businessinsider.com/cheating-affair-websiteashley-madison-hacked-user-data-leaked-2015-7

28. Keats Citron, Danielle. (2019). Sexual Privacy. *Yale L. J.***, 128,* 1870–1961.

29. Silverman, Jacob. (2016, June 14). Just How 'Smart' Do You Want Your Blender to Be? *The New York Times*. https://www.nytimes.com/2016/06/19/magazine/just-how-smart-do-you-want-your-blender-to-be.html

30. Steinberg, Joseph. (2014, January 27) These Devices May Be Spying On You (Even In Your Own Home). *Forbes*. https://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-yourown-home/#7eb0e320b859.

31. Morey, Timothy et al. (2015, May). Customer Data: Designing for Transparency and Trust. *Harvard Business Review*, 1–11. https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

32. Pollack, Wendy, Mike Sullivan. (2018, April 20). The Information Subscribers Most Likely to Pay for Google Among Tech Services. *The Information*. https://www.theinformation.com/articles/the-information-subscribers-most-likely-to-pay-for-google-among-tech-services

33. Dell Technologies. (2014). EMC Privacy Index. *Dell*. https://www.emc.com/campaign/privacy-index/global.htm.

34. IBM. (2018, April 16). New Survey Finds Deep Consumer Anxiety over Data Privacy and Security. *IBM News Room*. https://newsroom.ibm.com/2018-04-15-New-Survey-Finds-Deep-Consumer-Anxiety-over-Data-Privacyand-Security

35. Acquisti, Alessandro, Leslie K. John, George Loewenstein. (2013). What Is Privacy Worth? *J. Legal Stud., 42,* 249–273.

36. Strahilevitz, Lior J., Matthew B. Kugler. (2016). Is Privacy Policy Language Irrelevant to Consumers? *J. Legal Stud., 45,* 69–95.

37. Matthews, Alex, Catherine Tucker. (2017). *Government Surveillance and Internet Search Behavior*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564

38. Perez-Pena, Richard, Matthew Rosenberg. (2018, January 29). Strava Fitness App Can Reveal Military Sites, Analysts Say. *The New York Times*. https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html

39. Brown, Daniel. (2018, January 29). Here are Some of the Biggest Reveals from a Fitnesstracker Data Map That May Have Compromised Top-secret US Military Bases around the World. *Business Insider*. https://www.businessinsider.com.au/strava-heatmap-most-revealing-images-2018-1

40. Cohen, Bret et al. (2017). Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy. *Antitrust, 32,* 107–114.

ISSN 2782-2923

41. Yanqing, Hong. (2017, June 20). The Cross-Border Data Flows Security Assessment: An important part of protecting China's basic strategic resources. Yale Law School*** Paul Tsai China Center. *Working Paper*.

42. Miller, Amalia R., Catherine Tucker. (2017). Frontiers of Health Policy: Digital Data and Personalized Medicine. *Innovation Policy and the Economy, 17,* 49–75.

43. Lambrecht, Anja, Catherine Tucker. (2018). *Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads*. https://www.ssrn.com/abstract=2852260

44. Datta, Amit et al. (2015). Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination. *PoPETs,* 92–112.

45. Sweeney, Latanya. (2013). Discrimination in Online Ad Delivery. *ACMQueue, 11,* 1–10.

46. Datta, Amit et al. (2018). Discrimination in Online Advertising a Multidisciplinary Inquiry. *Proc. Mach. Learn. Res., 81,* 1–15.

47. Benkler, Yochai, Robert Faris, Hal Roberts. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford, Oxford University Press.

48. May, Ashley. (2018, April 27). Took an Ancestry DNA Test? You Might Be a 'Genetic Informant' Unleashing Secrets about Your Relatives. *USA Today*. https://www.usatoday.com/story/tech/nation-now/2018/04/27/ancestry-genealogy-dna-test-privacy-golden-state-killer/557263002/

49. Lamotte, Sandee. (2017, December 27). After 60 Years of Friendship, They Learned They're Biological Brothers. *CNN*. https://www-m.cnn.com/2017/12/27/health/friends-brothers-dna-discovery-hawaii-trnd/index.html?r=https%3A%2F%2Fwww.google.com%2F

50. Crossland, Kiley. (2018, January 5). The Hidden Risks of At-home DNA Testing. *World*. https://world.wng.org/content/the_hidden_risks_of_at_home_dna_testing

51. Constine, Josh. (2015, April 28). Facebook** Is Shutting Down Its API for Giving Your Friends' Data to Apps. *TechCrunch*. https://techcrunch.com/2015/04/28/facebook-api-shut-down/

52. Lewis, Paul. (2018, March 20). 'Utterly Horrifying': ex-Facebook** Insider Says Covert Data Harvesting Was Routine. *The Guardian*. https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analyticasandy-parakilas

53. Ben-Shahar, Omri, Anu Bradford. (2012). Efficient Enforcement in International Law. *Chi. J. Int'l L., 12,* 376–431.

54. Ben-Shahar, Omri, Kyle Logue. (2012). Outsourcing Regulation: How Insurance Reduces Moral Hazard. *Mich. L. Rev., 111,* 197–248.

55. Insurance Information Institute. (1999). *HO3, Section I.E.6*. Insurance Information Institute. https://www.iii.org/sites/default/files/docs/pdf/HO3_sample.pdf

56. Liberty Mutual Insurance. (2019). Identity Fraud Expense Coverage. *Liberty Mutual Insurance*. https://www.libertymutual.com/identity-theft-insurance

57. McAfee. (2017). Grand Theft Data – Data Exfiltration Study: Actors, Tactics, and Detection. *McAfee Report*. https://www.mcafee.com/us/resources/reports/rp-data-exfiltration.pdf

58. Center for Strategic and International Studies***. (2014, June 5). *Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime II. Intel Security*.

59. Norton Security. (2012, September 5). 2012 Norton Cybercrime Report. *Symantec*. https://www.symantec.com/about/newsroom/press-releases/2012/symantec_0905_02

60. Kramer, Ann. (2019, July 24). Ransomware, Data Breaches Expose Gaps in Cyber Insurance Market. *Bloomberg Law*.

61. Bar-Gill, Oren, Omri Ben-Shahar, Florencia Marotta-Wurgler. (2017). Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts. *U. Chi. L. Rev., 84,* 7–35.

62. Bode, Karl. (2016, March 17). AT&T Charges Steep Premium for Privacy, Calls it a 'Discount'. *DSL Reports*. https://www.dslreports.com/shownews/ATT-Charges-Steep-Premium-for-Privacy-Calls-it-a-Discount-136511

63. Google. (2019). Google Privacy Checkup. *Google*. https://myaccount.google.com/privacycheckup

64. Nesheim, Malden C. et al. eds. (2015). *A Framework for Assessing Effects of the Food System*. Washington, DC: National Academic Press. https://www.ncbi.nlm.nih.gov/books/NBK305182/

65. Kohn, Jeff, Kelsey Kruger. (2016, November 17). Understand Pollution, Environmental Impacts from Food in 6 Charts. *GreenBiz*. https://www.greenbiz.com/article/understand-pollution-environmental-impactsfood-6-charts

66. Marotta-Wurgler, Florencia. (2016). Self-Regulation and Competition in Privacy Policies. *J. Legal Stud., 45,* S13–S39.

67. Froomkin, A. Michael. (2000). The Death of Privacy? *Stan. L. Rev., 52,* 1461–1543.

68. PrivacyGrade.org. (2014). *Search Results for "facebook"**. *Carnegie Mellon University*. http://privacygrade.org/apps/search?utf8=%E2%9C%93&q=facebook

69. Johnson, Dominic, Simon Levin. (2009). The Tragedy of Cognition: Psychological Biases and Environmental Inaction. *Curr. Sci., 97,* 1593–1603.

70. Adjerid, Idris et al. (2016). A Query-Theory Perspective of Privacy Decision Making. *J. Legal Stud., 45,* S97–S121.

ISSN 2782-2923

71. Jensen, Carlos, Colin Potts. (2004). Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. In *Proceedings of the 2004 Conference on Human Factors in Computing Systems* (pp. 471–478). Vienna, Austria, ACM Press.

72. Pan, Yue, George M. Zinkhan. (2006). Exploring the Impact of Online Privacy Disclosures on Consumer Trust. *J. Retailing, 82,* 331–338.

73. Ben-Shahar, Omri, Carl Schneider. (2014). *More than You Wanted to Know: The Failure of Mandated Disclosure*. Princeton, NJ, Princeton University Press.

74. McDonald, Alecia M., Lorrie Faith Cranor. (2008). The Cost of Reading Privacy Policies. *I/S: J.L. & Pol'y for Info. Soc'y, 4,* 540–565.

75. Radin, Margaret Jane. (2013). *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law*. Princeton, NJ: Princeton University Press.

76. Willis, Lauren E. (2013). When Nudges Fail: Slippery Defaults. *U. of Chi. L. Rev., 80,* 1155–1229.

77. Ben-Shahar, Omri, Lior J. Strahilevitz. (2016). Contracting over Privacy. *J. Legal Stud., 45,* S1–S11.

78. Rosenberg, David. (1984). The Causal Connection in Mass Exposure Cases: A "Public Law" Vision of the Tort System. *Harv. L. Rev., 97,* 849–949.

79. Dewees, Donald N. et al. (1996). *Exploring the Domain of Accident Law: Taking the Facts Seriously*. Oxford, UK, Oxford University Press.

80. Esty, Daniel C. (2004). Environmental Protection in the Information Age. *NYU L. Rev., 79,* 115–211.

81. Koo, Jimmy H. (2017, December 12). Equifax Negligent in Data Breach, Community Banks Allege. *Class Action Litigation Report, Bloomberg BNA*. https://news.bloomberglaw.com/class-action/equifax-negligent-in-databreach-community-banks-allege

82. Keats Citron, Danielle. (2007). Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age. *S. Cal L. Rev., 80,* 241–297.

83. Viscusi, Kip. (2000). Foreword. In Richard L. Stroup and Roger E. Meineres, eds., *Cutting Green Tape: Toxic Pollutants, Environmental Regulation, and the Law*, ix. Piscataway & New Brunswick, NJ, Transaction Publishers.

84. Schroeder, Christopher H. (2002). Lost in the Translation: What Environmental Regulation Does That Tort Cannot Duplicate. *Washburn L. J., 41,* 583–606.

85. Lin, Albert C. (2005). Beyond Tort: Compensating Victims of Environmental Toxic Injury. *S. Cal. L. Rev., 78,* 1439–1528.

86. Shavell, Steven. (1987). *Economic Analysis of Accident Law*. Cambridge, MA, Harvard University Press.

87. Harrell, Erika, Lynn Langton. (2017). *Victims of Identity Theft 2014*. U.S Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/vit14.pdf

88. Brennan, Troyen A. (1988). Causal Chains and Statistical Links: The Role of Scientific Uncertainty in Hazardous-Substance Litigation. *Cornell L. Rev., 73 ,* 469–533.

89. Solove, Daniel J., Danielle Keats Citron. (2018). Risk and Anxiety: A Theory of Data Breach Harms. *Tex. L. Rev., 96,* 737–786.

90. Silverman, David L. (2017). Developments in Data Security Breach Liability. *Bus. L., 73,* 215.

91. Gelpe, Marcia R., A. Dan Tarlock. (1974). The Uses of Scientific Information in Environmental Decisionmaking. *S. Cal. L. Rev., 48,* 371–427.

92. American Law Institute. (1991). *Enterprise Responsibility for Personal Injury* (pp. 319–321). Philadelphia, PA, American Law Institute.

93. Ben-Shahar, Omri, Ariel Porat. (2018). The Restoration Remedy in Private Law. *Colum. L. Rev., 118,* 1901–1952.

94. Solove, Daniel J., Paul Schwartz. (2017). *Information Privacy Law* (6th ed.). Philadelphia, PA, Wolters & Kluwer.

95. American Law Institute. (2010). *Principles of the Law of Aggregate Litigation*. Philadelphia, PA, American Law Institute.

96. Barnett, Kerry. (1987). Equitable Trusts: An Effective Remedy in Consumer Class Actions. *Yale L. J.***, 96,* 1591–1614.

97. Abraham, Kenneth S. (2002). The Relation Between Civil Liability and Environmental Regulation: An Analytical Overview. *Washburn L. J., 41*, 379–398.

98. Butler, Henry N., Jonathan R. Macey. (1996). Externalities and the Matching Principle: The Case for Reallocating Environmental Regulatory Authority. *Yale L.*** & Pol'y Rev., 14,* 23–66.

99. Lin, Albert C. (2012). Public Trust and Public Nuisance: Common Law Peas in a Pod. *U.C.D. L. Rev., 45,* 1075.

100. Sharkey, Catherine. (2003). Punitive Damages as Societal Damages. *YaleL. J.*** , 113 ,* 347–453.

101. Swanson, Elizabeth J., Elaine L. Hughes. (1990). *The Price of Pollution: Environmental Litigation in Canada*. Edmonton, Environmental Law Center.

102. Bradshaw, Karen. (2016). Settling for Natural Resource Damages. *Harv. Env. L. Rev., 40,* 211–253.

103. American Law Institute. (2019). *Principles of the Law, Data Privacy: §§ 3–4*. American Law Institute.

104. Ben-Shahar, Omri, Adam Chilton. (2016). Simplification of Privacy Disclosures: An Experimental Test. *J. Legal Stud., 45,* 42–67.

105. Barnhill, Allison Rosser. (1989). The Unraveling of California's Proposition 65. *Wake Forest L. Rev., 24,* 367–408.

ISSN 2782-2923

106. Barsa, Michael. (1997). California's Proposition 65 and the Limits of Information Economics. *Stan. L. Rev., 49,* 1223–1247.

107. Bui, Linda T. (2005). Public Disclosure of Private Information as a Tool for Regulating Environmental Emissions: Firm-Level Responses by Petroleum Refineries to the Toxics Release Inventory. *Center for Economic Studies, U.S. Census Bureau, Working Papers,* 05–13.

108. Bae, Hyunhoe et al. (2010). Information Disclosure Policy: Do State Data Processing Efforts Help More than the Information Disclosure Itself? *J. Pol'y Anal. Mgmt., 29,* 163–182.

109. Federal Trade Commission. (2012, March). Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers. *Federal Trade Commission*. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

110. National Telecommunications and Information Administration. (2013). *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices*. https://www.ntia.doc.gov/les/ntia/publications/july_25_code_draft.pdf

111. White House. (2012, February). *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. White House. https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf

112. Robinson, Matt. (2018, April 25). Yahoo to Pay First SEC Penalty over Its Response to Massive Hack. *Bloomberg BNA*. https://news.bloomberglaw.com/tech-and-telecom-law/yahoo-to-pay- first-sec-penalty-over-its-response-to-massive-hack

113. John D. Graham, Jonathan Baert Weiner eds. (1997). *Risk versus Risk: Tradeoffs in Protecting Health and the Environment*. Cambridge, MA, Harvard University Press.

114. Schwartz, Paul M. (2013). The EU-US Privacy Collision. *Harv. L. Rev., 126,* 1966.

115. Revesz, Richard L., Michael A. Livermore. (2011). *Rataking Rationality: How Cost-Benefit Analysis Can Better Protect the Environment and Our Health*. Oxford, UK: Oxford University Press.

116. Jun, S-P, H.S Yoo, S. Choi. (2018). Ten Years of Research Change Using Google Trends: From the Perspective of Big Data Utilizations and Applications. *Technol. Forecast. Soc. Change, 130,* 69–87.

117. Ginsberg, Jeremy et al. (2009). Detecting Influenza Epidemics Using Search Engine Query Data. *Nature, 457,* 1012–1014.

118. Calo, Ryan. (2013). Consumer Subject Review Boards: A Thought Experiment. *Stan. L. Rev., 66,* 97–102.

119. Schneider, Carl E. (1998). *The Practice of Autonomy: Patients, Doctors, and Medical Decisions*. Oxford, UK, Oxford University Press.

120. Congressional Budget Office. (2001, June). Evaluation of Cap-and-Trade Programs for Reducing U.S. Carbon Emissions. *Congressional Budget Office*. https://www.cbo.gov/publication/13107.

121. Stavins, Robert N. (2003). Experience with Market-Based Environmental Policy Instruments. In Karl-Göran Mäler and Jeffrey Vincent, eds., *Handbook of Environmental Economics* (pp. 355–435). Amsterdam, Netherlands, Elsevier Science.

122. Burtraw, Dallas, Sarah Jo Szambelan. (2009). *U.S. Emissions Trading Markets for SO2 and NOx. Resources for the Future, Discussion Paper*, 09–40.

123. Metcalf, Gilbert E., David Weisbach. (2009). The Design of a Carbon Tax. *Harv. Envtl. L. Rev., 33,* 499–556.

124. Mossoff, Adam. (2004). Spam–Oy, What a Nuisance! *Berkeley Tech. L. J.*, 19,* 625–666.

125. Zhang, Lily. (2005). The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem. *Berkeley Tech. L. J.*, 20,* 301–332.

126. Walmart. (2017, November). Walmart Privacy Policy. *Walmart.com*. https://corporate.walmart.com/privacy-security/walmart-privacy-policy

127. Environmental Protection Agency. (2017). The Social Cost of Carbon: Estimating the Benefits of Reducing Greenhouse Gas Emissions. *Environmental Protection Agency*. https://19january2017snapshot.epa.gov/climatechange/social-cost-carbon_.html.

128. Johnston, Jason Scott. (2016). The Social Cost of Carbon. *Regulation, 39,* 36–44.

129. Office of the New York State Attorney General. (2014, July 7). *Information Exposed: Historical Examination of Data Breaches in New York State*. New York State Attorney General. https://www.ag.ny.gov/pdfs/data_breach_report071414.pdf.

130. Department of Justice. (2015, September). *Victims of Identity Theft, 2014, NCJ 248991*. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/vit14.pdf

131. Ponemon Institute. (2017, June). *Cost of Data Breach Study: Global Overview*. Ponemon Institute. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

132. Juniper Research. (2017, March). Cybercrime Will Cost Businesses over $2 Trillion by 2019. *Juniper Research: Press Releases*. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

133. Identity Theft Research Center. (2017). 2017 Annual Data Breach Year-End Review. *Identity Theft Research Center*. https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf

134. Agelidis, Yasmine. (2016). Protecting the Good, the Bad, and the Ugly: Exposure Data Breaches and Suggestions for Coping with Them. *Berkeley Tech. L. J.*, 31,* 1057–1078.

135. Cheng, Long, Fang Liu, Danfeng (Daphne) Yao. (2017). Enterprise data breach: causes, challenges, prevention, and future

ISSN 2782-2923

directions. *WIREs: Data Mining and Knowledge Discovery, 7,* 1–14.

136. Schwartz, Paul M., Edward J. Janger. (2006). Notification of Data Security Breaches. *Mich. L. Rev., 105,* 913–984.

137. Froomkin, A. Michael. (2009). Government Data Breaches. *Berkeley Tech. L. J.*, 24,* 1019–1059.

138. Romanovsky, Sasha et al. (2011). Do Data Breach Disclosure Laws Reduce Identity Theft? *J. Pol'y Anal. & Management, 30,* 256–286.

139. Ponemon Institute. (2014, April). *The Aftermath of a Data Breach: Consumer Settlement*. Ponemon Institute. https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf.

140. Kiernan, John. (2015, January 20). Fraud Liability Study: Which Cards Protect You Best? *Wallethub*. https://wallethub.com/edu/fraud-liabilitystudy/25726/

141. Pierce, Justin C. (2016). Shifting Data Breach Liability: A Congressional Approach. *Wm. & Mary L Rev., 57,* 975–1017.

142. LexisNexis. (2013, September). LexisNexis True Cost of Fraud Study: Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud. *LexisNexis*. https://www.lexisnexis.com/risk/downloads/assets/ true-cost-fraud-2013.pdf)

143. Harrell, Erika, Lynn Langton. (2013). *Victims of Identity Theft 2012*. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/vit12.pdf

144. Pascual, Al et al. (2018, February 6). Identity Fraud: Fraud Enters a New Era of Complexity. *Javelin Strategy*. https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity

145. Abraham, Kenneth S. (1986). *Distributing Risk: Insurance, Legal Theory, and Public Policy*. New Haven, YaleUniversity Press***.

146. Shavell, Steven. (1979). On Moral Hazard and Insurance. *Q. J. Econ., 93,* 541–562.

147. Shavell, Steven. (2000). On the Social Function and Regulation of Liability Insurance. *Geneva Papers on Risk & Ins., 25,* 166–179.

148. Talesh, Shauhin A. (2017). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Business. *Law and Social Inquiry, 43,* 417–440.

149. Kunzman, Steven A. (1985). The Insurer as Surrogate Regulator of the Hazardous Waste Industry: Solution or Perversion? *Forum, 20,* 469–488.

150. Richardson, Benjamin J. (2002). Mandating Environmental Liability Insurance. *Duke Envtl. L. & Pol'y F., 12,* 293–330.

151. Experian. (2017). Delivering Value in the Digital Age: Exploring UK Attitudes Towards Data. *Experian*. https://engage.experian.co.uk/delivering-value-in-the-digital-age/

152. Federal Trade Commission. (2013). Lost or Stolen Credit, ATM, and Debit Cards. *Federal Trade Commission, Consumer Information*. https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards#Limit

153. Rogers, Anna. (2015, October 21). Breast Implants: The Ticking Time Bomb in Millions of Women's Bodies. *Collective Evolution*. https://www.collective-evolution.com/2015/10/21/breast-implants-the-ticking-time-bombin-millions-of-womens-bodies/

154. Turow, Joseph. (2008). The Federal Trade Commission and Consumer Privacy in the Coming Decade. *J. L. &Pol'y for Info. Soc., 3,* 723–749.

155. Weiss, N. Eric, Rena S. Miller. (2014). *The Target and Other Financial Breaches: Frequently Asked Questions. Cong. Research Serv., R43496*. https://fas.org/sgp/crs/misc/R43496.pdf

156. Wikipedia. (2019). Environmental Certification. *Wikipedia*. https://en.wikipedia.org/wiki/Environmental_certification

157. Zetter, Kim. (2009, March 9). Do Breach Notification Laws Work? *Wired*. https://www.wired.com/2009/03/experts-debate/

158. Ben-Shahar O. Data Pollution, *Journal of Legal Analysis*, 2019, Vol. 11, pp. 104–159.

---

* Принадлежит Калифорнийскому университету, Беркли (с 03.03.2026 включен в перечень нежелательных организаций РФ) / Affiliated with the University of California, Berkeley (designated as an undesirable organization in the Russian Federation effective March 3, 2026).

** Сеть принадлежит компании *Meta*, признана экстремисткой организацией в РФ / The network is owned by Meta, a company recognized as an extremist organization in the Russian Federation.

*** Признана нежелательной организацией в РФ с 01.07.2024 / Recognized as an undesirable organization in the Russian Federation as of 01.07.2024.

Дата поступления / Received 29.10.2021
Дата принятия в печать / Accepted 10.11.2021