УДК 004.93

ПРОБЛЕМА ДЕАНОНИМИЗАЦИИ ЛИЧНОСТИ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Лошин Никита Дмитриевич,
Рогожкина Елизавета Евгеньевна
Уральский федеральный университет имени
первого Президента России Б. Н. Ельцина, Екатеринбург, Россия
nicosx@mail.ru
elizaveta.rogozzhkina@yandex.ru

Аннотация. В статье рассматриваются причины и методы деанонимизации личных данных граждан, объясняются позиции сторонников и противников данного явления. Мы попытаемся ответить на вопрос: благо или зло борьба с анонимностью, а также рассмотрим, как она протекает в наши дни и с какими трудностями приходится сталкиваться. Помимо этого, присутствуют размышления о человеческом поведении в деанонимизированном пространстве.
Ключевые слова: деанонимизация личности; свобода; безопасность; система распознавания лиц; паноптикум; информационные технологии; информационное общество

THE ISSUE OF DE-ANONYMIZATION OF THE PERSONALITY IN TODAY'S "MEDIA" SOCIETY

Nikita D. Loshin, Elizveta I. Rogozhkina
Ural Federal University named after
the first President of Russia B. N. Yeltsin, Ekaterinburg, Russia
nicosx@mail.ru
elizaveta.rogozzhkina@yandex.ru

Abstract. In the article we observe the causes and methods of civil citizens data's De-anonymization from the allies and opponents of the theory. We try to debunk the theory and find out whether its impact is negative or positive, the process of De-anonymization and which difficulties you can face. Despite of that, we also apply the idea of people's behavior in such society under De-anonymization.
Keywords: deanonymization of a person; liberty; safety; face recognition system; panopticon; information technology; information society

В текущее время мы можем наблюдать следующую мировую тенденцию – проникновение цифровых технологий в разные сферы жизни общества. Человек ежедневно пользуется множеством цифровых сервисов, подозревает он об этом или нет. Например, приложения в телефоне, звонки, оплата покупок банковской картой, поиск информации в интер-

© Лошин Н. Д.,
Рогожкина Е. Е., 2023

нете, общение в мессенджерах, публикация на личной странице в социальных сетях, фитнес-браслеты и многое другое. Совершая определенные действия, человек оставляет за собой цифровой след. Различные компании, сервисы и приборы могут считывать этот цифровой след и преобразовывать его в данные. Далее эти данные могут передаваться в обезличенном виде другим лицам, в том числе и государству.

Изначально интернет считался островом свободы, где можно было делать многое и чувствовать себя в безопасности. Люди могли делать здесь то, что не могли позволить себе в реальной жизни, а самое главное, могли делать это анонимно или же под фейковым аккаунтом, создавая себе любую желаемую личность. Интернет был обителью свободы и по той причине, что государству была тогда еще не интересна неотъемлемая часть нашей современной жизни. С развитием интернета и цифровых технологий и их всеохватывающим проникновением государство уже не могло игнорировать цифровую реальность. Оно решило контролировать и регулировать цифровые сервисы тоже. Чтобы государству было легче управлять своими гражданами, оно должно больше о них знать, а если учесть, что люди значимую часть своей жизни проводят в цифровом пространстве, то упускать его из виду было бы большой ошибкой.

В данной статье мы попытаемся рассмотреть, как государство работает с цифровыми данными для деанонимизации личности и данных своих граждан. Попытаемся понять, в чем вред и польза данного процесса.

Начать следует с понятия «анонимность» – сокрытие персональных и, в принципе, любых данных о личности. Деанонимизация – это обратный процесс анонимности, когда персональная информация о человеке становится доступна всем или определенным лицам. К персональным данным можно отнести все что угодно: ФИО, дату рождения, место проживания, номер мобильного телефона, страницы в социальных сетях, IP-адрес и т. п. Деанонимизация делится на виды, такие как:

Добровольная – информация пользователем предоставляется о себе самостоятельно, например YouTube-блоггер Руслан Соколовский после достижения популярности перестал вести свою деятельность анонимно и сделал деанон.

Случайная – возникает вследствие невнимательности самого пользователя либо излишней внимательности тех, кто за ним следит (при публикации скриншотов, фотографий или постановок – непреднамеренно на публикацию попадает излишняя информация: случайно раскрывается местоположение или настоящее имя и т. д.).

Злонамеренная – обнародование данных пользователя для травли, преследования или наказания. В данной ситуации, как правило, у пользователя, чьи данные раскрылись, может быть тревожность, чувство стыда или даже страх.

Проблема деанонимизации имеет две полярные позиции – сторонников и противников. Позиция сторонников, воспринимающих деанонимизацию как положительное явление, сводится к основному аргументу – к безопасности, так как анонимность позволяет людям говорить и делать, что хочется, в независимости от того, как их действия повлияют на других людей. Это может быть как намеренно, так и случайно. Деанонимизация позволяет защитить других людей от негативного влияния с помощью контроля над знанием личности субъекта, оказывающего это влияние. Получается так: если человек будет знать, что ему не удастся быть анонимным, ему придется контролировать свои действия, чтобы они не противоречили правилам и нормам морали. Из-за такого контроля у людей может складываться чувство безопасности и справедливости. Безопасность заключается в избегании негативного влияния, а справедливость – в понимании, что субъекта негативного влияния можно будет легко вычислить и наказать по закону. Так, при активной реализации политики деанонимизации могут появиться безопасные пространства. Противники деанонимизации апеллируют к проблеме непонимания того, как это может сказаться на их свободе. У людей есть понимание личного пространства, в которое они не хотели бы никого пускать, тем более государство, поскольку они не знают, как их данные могут использоваться. Существует страх перед тем, что благими намерениями будет оправдываться механизм проникновения в частную жизнь человека, которую бы он хотел держать в тайне. Также деанонимизация может стать регрессионным механизмом борьбы с противниками политической риторики государства.

Представитель Госдумы Илья Костунов говорит, что «угрозы, связанные с контентом и коммуникациями, идут из-за смеси анонимности и неанонимности в интернете… Это благотворная среда, которая влечет иллюзию вседозволенности. Когда нет наказания, травля продолжается, и никто не задумывается, что у человека может быть сломана жизнь» [2]. Решение проблемы он видит в деанонимизации пользователей через верификацию при регистрации, чтобы избежать фейков и ботов: «Читать можно анонимно, а вот писать – только после идентификации. Если у нас будет эта система, мы сократим до минимума травлю, фейки, анонимность» [2].

Глава комитета Госдумы по информационной политике А. Хинштейн, призвал Роскомнадзор к активной работе по деанонимизации в интернете для противодействия киберпреступности. Он считает: «Если вопросы деанонимизации в сети в ближайшее время нам сообща не удастся решить, удельная доля IT-преступлений будет только возрастать, угрожая национальной безопасности страны» [3].

На данную инициативу отреагировал известный юрист, глава комиссии по правовому обеспечению цифровой экономики московского отделения Ассоциации юристов России А. Журавлев, сказав следующее:

«К вопросам деанонимизации в интернете необходимо подходить осторожно и взвешенно, соблюдая баланс между личной жизнью граждан и защитой их возможных угроз. Роскомнадзор по действующему законодательству наделен полномочиями по мониторингу соблюдения закона и может, например, блокировать сим-карты, проверять подлинность их владельцев. Также ведомство является регулятором в интернете» [5].

Он указал на то, что проблема безнаказанного противоправного поведения в интернете «порождает необходимость предпринимать определенные действия по защите граждан от оскорблений в сети, кибербуллинга, фишинга, хакерских атак» [5]. Но Журавлев осознает всю опасность деанонимизации. На весах, на которых на противоположных сторонах лежат личная жизнь граждан и защита их от угроз, может нарушиться равновесие из-за злоупотребления надзорных органов власти, потому, по нашему мнению, перед тем как давать органами какие-либо полномочия, нужно заранее придумать механизм их сдерживания.

Относительно недавно в сети стали появляться в открытом доступе базы данных с генетической информацией людей (от полных последовательностей всего генома – сиквенса, до ограниченной информации по коротким тандемным повторам Y-хромосомы). Например, пользователи делятся информацией о своих галотипах на генеалогических сайтах для выяснения родственных связей и поиска дальних родственников, естественно, все эти данные не анонимны. Также в свободном доступе находится анонимная медицинская генетическая информация, например из научного проекта «1000 геномов человека» (проект по полной расшифровке геномов тысячи разных людей), где анонимность доноров ДНК поддерживается по этическим причинам. Чем же это интересно? Генеалогические данные, несомненно, помогают деанонимизировать личность пользователей. Бывали случаи, когда матери, искусственно оплодотворенные анонимными донорами, использовали генеалогическую базу и узнавали фамилии биологических отцов. Предположить далее не составляет труда: допустим, им в руки попалась информация о месте рождения или проживания через очень дальних родственников, засветившихся в базе, и они могут полностью идентифицировать биологического отца. Достижение, конечно, сомнительное, по крайней мере, для тех, кто подвергся подобному преступлению против личности.

Государство принимает попытки защитить личность пользователя в интернете различными способами. Оно следит за тем, чтобы персональные данные не утекали в сеть путем введение административной и уголовной ответственности для лиц, допустивших утечку. Государство регулирует то, в каком виде данные людей могут передаваться третьим лицам. Также не стоит забывать, что государство само является хранителем персональных данных своих граждан и любые утечки с его стороны мо-

гут негативно сказываться на репутации власти и приводить к недовольствам ею граждан, которые могут перерасти во что-то большое. Таким образом, государство оказывается в зоне риска, как и другие компании, работающие с персональными данными.

Президент всемирного экономического форума в Давосе в своей книге цитирует слова профессора Гарварда Майкла Сэндэла: «мы, похоже, все в большей степени готовы обменять конфиденциальность на удобства, когда дело касается многих устройств, которые мы обычно используем» [4, с. 82]. Добровольная деанонимизация ради повышения собственной эффективности в цифровом мире – это вынужденная мера. Например, люди пользуются навигаторами, передавая свою текущую геолокацию сервису. И если выбрать в приложении опцию отслеживать геолокацию всегда, а не только во время использования приложения, то считайте, вы одобряете полноценную и постоянную слежку за вами. Опасность заключается в том, что мы не знаем, как именно цифровые сервисы будут использовать информацию о нас. Также есть вероятность утечки информации в открытый доступ или в доступ к преступникам. Помимо этого, Шваб пишет: «…люди, знающие, что за ними наблюдают, начинают в своем поведении проявлять больший конформизм и соблюдать требования» [4, с. 82]. У людей может появиться страх, что представители спецслужб читают их личную переписку и выискивают информацию, которая может нанести вред государству и обществу. Тут, правда, имеется проблема того, что человек не может знать, когда за ним наблюдают и делают ли это вообще. Мишель Фуко, описывая идею паноптикума Иеремии Бентама, утверждал следующее: «Власть должна быть видимой и недоступной для проверки» [1, с. 195]. Под видимой он имел в виду, что человек должен знать, откуда за ним наблюдают, а под недоступной – не знать момент, когда за ним наблюдают.

Одним из эффективных инструментов наблюдения и борьбы с анонимностью стало введение камер с системой распознавания лиц. Они могут, считывая очертания лица, а затем сравнивая его с картинками в базе данных, рассчитывать, насколько процентов они схожи, и выдавать в качестве ответа наиболее подходящую личность. С помощью таких технологий можно ловить опасных преступников. Правда, у такой технологии есть и обратная сторона: с ее помощью активно ловят митингующих в разных странах. Раньше было важно не попасться в руки представителей власти на митинге, сейчас же ситуация усложнилась и тем, что нужно не попасться и после. Система распознавания лиц способна не только определить личность митингующих, но и показать, где камеры засекли его в последний раз. Сейчас эти системы улучшаются, чтобы можно было узнавать человека в маске или очках, а также по силуэту или походке. Люди, попадающие под око камер, также не остаются в стороне, создавая

специальный макияж или одежду, которая мешает камерам распознавать личность.

Людям, которым важна анонимность, приходится находить и создавать все время новые способы борьбы с деанонимизацией, используя сервисы, которые предлагают возможность быть анонимным, чтобы чувствовать себя в безопасности. Государство пытается бороться с такими сервисами, пытаясь их запретить, различными способами оправдывая это вопросами безопасности.

Деанонимизацию можно приравнять к насилию в том смысле, что государство хочет сделать это своей монополией. Оно всячески борется с теми, кто допускает деанонимизацию личностей и данных граждан, но при этом само государство позволяет себе заниматься этим. Разрешение граждан на использование их данных в определенных целях государству не нужно. Стоит ли обвинять власть в том, что она занимается деанонимизацией граждан? Все зависит от того, соблюдает ли оно баланс между гражданской свободой и государственной безопасностью. Если будет перевес в пользу безопасности, то люди будут чувствовать постоянную слежку и контроль, а если перевес в сторону свободы, то незащищенность от преступности.

Список литературы

1. Фуко М. Надзирать и наказывать. М.: Ад Маргинем, 2018. 384 с.
2. Фыркнуть не удастся. Эксперты объяснили необходимость деанонимизации и введения ответственности соцсетей за контент // ФедералПресс. Публикация от 01.06.2020. URL: https://fedpress.ru/article/2508904 (дата обращения: 30.03.2023).
3. Хинштейн призвал Роскомнадзор к активной работе по деанонимизации в интернете // ТАСС. Публикация от 26.05.2021. URL: https://tass.ru/obschestvo/11476327 (дата обращения: 27.03.2023).
4. Шваб К. Четвертая промышленная революция. М.: Эксмо, 2016. 138 с.
5. Эксперт: К идее деанонимизации в интернете надо подходить, исходя из принципа «не навреди» // Деловая газета «Взгляд». Публикация от 26.05.2021. URL: https://vz.ru/news/2021/5/26/1101257.html (дата обращения: 29.03.2023).