УГОЛОВНО-ПРАВОВЫЕ НАУКИ / CRIMINAL-LEGAL SCIENCES

Редактор рубрики *Э. Ю. Латыпова* / Rubric editor *E. Yu. Latypova*

Научная статья **https://doi.org/10.21202/2782-2923.2025.2.312-327**

УДК / UDC 342.7:004.056:004.738.5(410)(430)

А. К. Жарова[1]

[1] *Институт государства и права Российской академии наук, г. Москва, Россия*

Неабсолютное право на тайну цифровых сообщений, или Европейская система достоверной идентификации человека

Жарова Анна Константиновна, доктор юридических наук, доцент, Институт государства и права Российской академии наук
E-mail: anna_jarova@mail.ru
ORCID ID: https://orcid.org/0000-0002-2981-3369
Scopus Author ID: 56964137900
Web of Science Researcher ID: H-4012-2015
eLIBRARY SPIN-код: 2240-1467

Аннотация

Цель: подтверждение либо опровержение гипотезы о том, что введенные в Германии и Англии требования об обязательном использовании провайдерами (операторами связи) технологий массового перехвата сообщений (данных) в совокупности с технологиями анализа больших данных являются новым этапом развития европейской предиктивной полицейской деятельности, проводимой в режиме, близком к реальному времени, и основой для формирования системы достоверной идентификации интернет-пользователя.

Методы: в статье используются всеобщий диалектический метод познания, а также общенаучные (анализ, синтез, индукция, дедукция, моделирование, сравнение) и частнонаучные методы исследования (формально-юридический).

Результаты: автор приходит к выводу о том, что создаваемая в европейских государствах модель идентификации призвана разрешить проблему ложных пользовательских данных. В большинстве стран мира отсутствует требование к интернет-пользователям о регистрации под действительными именем, фамилией и отчеством, если оно предусмотрено национальным обычаем. В результате анализа законодательства указанных стран автор приходит к заключению, что они направлены на создание европейской системы, которая позволит идентифицировать пользователей Интернета с высокой достоверностью, в режиме, максимально приближенном к реальному времени.

Научная новизна: в статье на основании исследования законодательства Англии и Германии, регламентирующего вопросы массового перехвата сообщений, и судебной практики их применения описана формирующаяся европейская система идентификации пользователей в Сети, которая направлена на создание системы узаконенной идентификации человека в Интернете. Доказано, что право на тайну связи в действительности рассматривается как относительное право человека, которое может быть нарушено в целях обеспечения безопасности государства от существующих угроз.

Практическая значимость: исследование поможет ученым, практикам и обучающимся лучше понять тенденции европейского законодательства и риски, которые формируются новой европейской системой идентификации пользователя Сети на основе анализа его цифровых следов.

Ключевые слова:
уголовно-правовые науки, технологии больших данных, массовый перехват сообщений, цифровой профиль, тайна электронных сообщений, нарушение прав человека

Как цитировать статью: Жарова, А. К. (2025). Неабсолютное право на тайну цифровых сообщений, или Европейская система достоверной идентификации человека. *Russian Journal of Economics and Law*, *19*(2), 312–327. https://doi.org/10.21202/2782-2923.2025.2.312-327

Scientific article

A. K. Zharova[1]

[1] *Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia*

Non-absolute right to the secrecy of digital messages, or the European system of reliable identification of a person

Anna K. Zharova, Dr. Sci. (Law), Associate Professor,
Institute of State and Law of the Russian Academy of Sciences
E-mail: anna_jarova@mail.ru
ORCID ID: https://orcid.org/0000-0002-2981-3369
Scopus Author ID: 56964137900
Web of Science Researcher ID: H-4012-2015
eLIBRARY SPIN-code: 2240-1467

Abstract
Objective: to confirm or refute the hypothesis that the requirements, introduced in Germany and Great Britain, for the mandatory use of mass interception of messages (data) by providers (telecommunication operators), combined with big data analysis technologies, constitute a new stage in the development of European predictive policing, conducted in a close to real time regime, and serve as the basis for reliable Internet users' identification systems.
Methods: the article uses the universal dialectical method of cognition, as well as general scientific (analysis, synthesis, induction, deduction, modeling, comparison) and specific scientific research methods (formal legal method).
Results: the author comes to the conclusion that the identification model being created in European countries is designed to solve the problem of false user data. In most countries, there is no requirement for Internet users to register under a valid first name, last name and patronymic, if it is provided for by national custom. Having analyzed the legislation of these countries, the author concludes that they are aimed at creating a European system that will allow identifying Internet users with high reliability, in a mode as close to real time as possible.
Scientific novelty: based on a study of the legislations of Great Britain and Germany regulating the mass interception of messages and judicial practice of their application, the article describes the emerging European system of user identification on the web, which is aimed at creating a system of legalized identification of a person on the Internet. It is proved that the right to communication secrecy is actually considered as a relative human right that can be violated to ensure the state security against existing threats.
Practical significance: the research will help scientists, practitioners and students to better understand the trends in European legislation and the risks posed by the new European system of network user identification based on the analysis of their digital footprints.

Keywords:
criminal-legal sciences, big data technologies, mass interception of messages, digital profile, secrecy of electronic messages, violation of human rights

For citation: Zharova, A. K. (2025). Non-absolute right to the secrecy of digital messages, or the European system of reliable identification of a person. *Russian Journal of Economics and Law*, *19*(2), 312–327. (In Russ.). https://doi.org/10.21202/2782-2923.2025.2.312-327

Введение

С каждым днем объем данных растет экспоненциально. По прогнозам, в 2025 г. он достигнет 175 зеттабайт[1]. Но уже сейчас в нем содержатся данные, напрямую связанные с повседневной жизнью людей. Ученые предупреждают, что в этом году нас ждет кризис хранения данных[2], причем такое стремительное возрастание объема данных обусловлено значительным увеличением числа устройств, подключенных к Интернету. Уходит в прошлое эпоха оцифровки данных, ей на смену приходит время, когда оцифрованная информация, данные сами по себе становятся ценным ресурсом не только бизнеса, науки, но и государства с его основными функциями обеспечения безопасности. Перед государством уже не стоит вопрос, сколько у него больших данных, а возник вопрос, как их можно использовать.

Идея ценности больших данных и развития применения методов их анализа давно не является чем-то новым. Концепция «общества знаний», предложенная ООН, получила поддержку в Уфимской декларации VII саммита БРИКС еще в 2015 г. (п. 33)[3]. В этом документе информационно-коммуникационные технологии (далее – ИКТ) были названы важным инструментом для перехода от информационного общества к обществу знаний.

Однако в настоящее время государства, которые первыми подчеркнули важность обеспечения прав человека на конфиденциальность данных, неприкосновенность частной жизни, вносят изменения в законодательство, обязывая провайдеров и операторов связи иметь в своем арсенале технологии, позволяющие осуществлять массовый перехват сообщений в Интернете.

Эта ситуация позволяет нам сделать предположение, что либо технологии анализа больших данных не представляют такой угрозы для конфиденциальности личных данных, как это утверждали правительства, либо требования об обязательном использовании технологий массового перехвата сообщений в совокупности с технологиями анализа больших данных являются новой ступенькой развития европейской предиктивной полицейской деятельности, проводимой в режиме реального времени.

Чтобы подтвердить либо опровергнуть эту гипотезу, в статье проводится анализ преимуществ использования в сочетании технологий больших данных и массового перехвата сообщений, а также изменений, произошедших в законодательстве Германии и Англии за период с 2022 по 2024 г., направленных на применение технологии массового перехвата сообщений.

Результаты исследования

Можно ли скрыть данные для систем анализа больших данных?

Технологии анализа данных стали активно применяться в 1990-х гг., когда объемы информации начали стремительно расти. Термин «большие данные» был впервые использован в 2008 г. редактором журнала

[1] Эксперт: объем данных в мире к 2025 году вырастет более чем в пять раз. (2019, 12 марта). ТАСС. https://tass.ru/ekonomika/6209822

[2] Глобальный кризис хранения данных. Почему места в хранилищах на всех не хватит. (2023, 16 января). Хабр. https://habr.com/ru/companies/first/articles/710838/

[3] Уфимская декларация VII саммита БРИКС (Принята в г. Уфе 09.07.2015). Официальный сайт Президента Российской Федерации. http://static.kremlin.ru/media/events/files/ru/YukPLgicg4mqAQIy7JRB1HgePZrMP2w5.pdf

Nature К. Линчем в статье, посвященной будущему науки[4]. Благодаря революции в области информационных технологий применение подобных технологий стало более доступным (Филипова, 2025; Краулин, 2023). Однако с этих пор люди осознали, что применение технологий анализа данных несет не только удобство, но и риск утраты конфиденциальности персональных данных (Редкоус, 2021; Begishev, 2022). Те инструменты, которые раньше были эффективными для защиты личных данных (Филипова, 2020), начинают терять свою актуальность в эпоху анализа больших данных (Хисамова, Бегишев, 2019). И связано это с возможностями таких технологий, которые позволяют анализировать любую информацию, включая информацию ограниченного доступа, размещенную в Сети (Смирнов, 2018). Так, если информация размещена на странице социальной сети и ее владелец предоставил к ней доступ только для определенной группы людей (Добкач, 2019), например, для друзей, то для технологии анализа больших данных это не имеет значения, важен сам факт ее присутствия в Интернете.

Сложностью для технологий анализа больших данных являются криптографически защищенные данные. Однако с течением времени (Громова, Петренко, 2023), как только будет решена задача создания квантового компьютера, все зашифрованные данные станут доступными для изучения (Жарова, 2023).

Но даже если некоторые персональные данные не размещены в Сети, технологии анализа больших данных позволяют получить их самостоятельно (Жарова, 2019; Уварова, Хроль, 2023) на основе анализа цифровых теней и цифровых следов, оставленных человеком (Bekkulov, 2023; Жарова, 2022). Например, швейцарские ученые провели эксперимент, который позволил убедиться, что большие языковые модели (*LLM*) могут собрать и раскрыть личную информацию пользователей Сети. В качестве примера ученые взяли 1,5 тысячи случайных профилей с площадки *Reddit* и проанализировали их активность с помощью *LLM*. *LLM* смогли точно определить место рождения и жительства, а также уровень дохода людей по вторичной информации, оставленной пользователями Сети. GPT-4 идентифицировал эти атрибуты с точностью 85 %, а *LlaMA-2-7b* – с точностью 51 % [5].

В таком случае, если современные технологии анализа данных, например, оставленных человеком в Интернете, представляют серьезную опасность конфиденциальности, поскольку могут сформировать цифровой профиль человека либо достаточно точно идентифицировать его по независимым между собой атрибутам, то возникает вопрос о целесообразности предъявления требований к провайдерам и операторам связи о наличии технологий, позволяющих массово перехватывать сообщения в Интернете с целью идентификации человека?

Ответ кроется в функциональных особенностях каждой технологии. Технологии массового перехвата сообщений и анализа больших данных представляют собой два различных подхода к обработке информации, которые могут применяться в сочетании. Между ними существуют значительные различия, которые заключаются в целях, методах сбора и обработки данных, а также в области их применения.

Цель применения массового перехвата сообщений заключается в собирании данных путем осуществления перехвата максимально возможного объема данных в реальном времени или в режиме, близком к нему, из различных источников, таких как интернет-трафик, телефонные разговоры, сообщения, переданные по электронной почте, размещенные в социальных сетях, и т. д. Все эти данные являются большими данными, они собираются без согласия или уведомления пользователей. Анализ полученных данных идет в режиме, близком к реальному времени, и направлен на выявление потенциально подозрительной активности, отслеживание коммуникаций и сбор разведывательной информации.

Целью применения технологии анализа больших данных является анализ уже собранных данных, например, перехваченных с целью выявления закономерностей, связей и скрытых тенденций. Этот анализ может быть как ретроспективным, так и перспективным.

Для анализа разных цифровых данных (системных и идентификационных) разработаны и используются различные методы и технологии работы с ними (Халапсин, Данилюк, 2022). Например, один из методов – это детерминированная идентификация, которая осуществляется с помощью анализа цифровых данных, уникальных для каждого человека и не меняющихся от устройства к устройству. К таким данным относятся имя,

[4] История больших данных (Big Data) – часть 1. (2019, 15 января). КомпьюТерра. https://www.computerra.ru/234239/istoriya-bolshih-dannyh-big-data-chast-1/

[5] Нейросети раскрыли личные данные пользователей соцсетей. (2023, 1 ноября). Lenta.ru. https://lenta.ru/news/2023/11/01/llm/

фамилия, номер телефона, электронная почта и др. Эти данные человек вводит сам в начале использования устройства, в случае применения интернет-технологий такими данными могут быть регистрационные данные.

Еще один метод анализа данных – вероятностное определение – основывается на анализе различных данных о пользователе, которые сопоставляются с помощью специальных вероятностных моделей. Для этого используются различные системные и идентификационные параметры, такие как *IP*-адрес пользователя, страна его проживания, маска сети и подсети, а также информация об интересах и поведении пользователя, например, скорости нажатия на клавиши клавиатуры, его запросах и другие сведения.

Однако любые технологии анализа данных могут быть использованы, только когда эти данные собраны или перехвачены. Причем перехватить данные можно только на определенных этапах приема-передачи данных в Сети. Технологии массового перехвата могут перехватить данные лишь в случае, если передаваемые по Интернету пакеты данных собрались в интернет-узле. Им может быть маршрутизатор, компьютеры, сотовые телефоны, специальные сетевые устройства, серверы, другие устройства. Перехват может быть реализован в режиме реального времени.

Основным протоколом приема и передачи данных по Сети является протокол *TCP/IP*, он передает данные небольшими пакетами, которые в процессе их передачи по Сети невозможно распознать и оценить на предмет их смысла и содержания. Однако этот же протокол *TCP/IP* собирает данные в целое у получателя информации, в узле Сети, и когда данные представляют целое, то их можно перехватить, а далее технологиями анализа данных оценить.

Таким образом, перехватить пакеты данных в процессе их передачи по Сети с технологической точки зрения невозможно, но можно это сделать в интернет-узле.

Исходя из функциональных возможностей сравниваемых информационных технологий – массового перехвата сообщений и анализа больших данных, мы приходим к выводу, что технологии массового перехвата сообщений значительно расширяют функционал систем обработки больших данных. Они позволяют в режиме реального времени собирать данные из различных интернет-источников для получения разведывательной информации и выявления новых угроз, исходящих от всех пользователей, подключенных к Сети (Жарова, 2019; Кубасов и др., 2020). И, вероятно, истинный смысл массового перехвата сообщений заключается в предоставлении правоохранительным органам инструментов для «первичного отбора» потенциально подозрительной информации, которая затем может быть подвергнута более детальному анализу с помощью технологии больших данных.

Неабсолютное право на тайну электронных сообщений

В период с 2022 по 2024 г. в законодательствах Великобритании и Германии произошли изменения, касающиеся требований к провайдерам и операторам связи о наличии у них технологий, обеспечивающих массовый перехват сообщений в Интернете. Хотя в Европе судебная практика по делам о применении технологии массового перехвата начала формироваться намного раньше. Так, Европейский суд по правам человека (далее – ЕСПЧ), рассмотрев дело в закрытых заседаниях 11 июля, 4 и 6 сентября 2019 г. и 17 февраля 2021 г., вынес в последнюю дату решение по делу Максимилиана Шремса, в котором постановил, что американские компании не обеспечивают должную защиту конфиденциальности данных в соответствии с европейскими стандартами. Суд также признал, что законодательство, позволяющее государственным органам получать доступ к содержанию электронных сообщений на общей основе, нарушает фундаментальное право на неприкосновенность частной жизни [6].

Однако судебные постановления не смогли остановить формирование системы законодательных документов, которые нацелены на то, чтобы массово перехватывать сообщения. Так, 22 декабря 2023 г. в Германии были внесены изменения в Закон об ограничениях секретности письменных, почтовых сообщений и теле-

[6] Постановление ЕСПЧ от 25.05.2021 «Дело «Центр правосудия (Centrum for rattvisa) против Швеции» (жалоба № 35252/08). По делу обжалуются массовый перехват трансграничных сообщений разведывательными службами, сам факт существования правового режима скрытого наблюдения, а также пропорциональность и гарантии законодательства Швеции о перехвате информации в разведывательных целях. По делу было допущено нарушение требований статьи 8 Конвенции о защите прав человека и основных свобод. (2022). Прецеденты Европейского суда по правам человека, 1.

коммуникаций (*Gesetz zur Beschränkung des Brief, Post- und Fernmeldegeheimnisses*[7] (далее – *G 10*)), который аналогичен британскому Закону о регулировании следственных полномочий 2000 г.

В декабре 2022 г. в Великобритании вступил в силу Кодекс практической деятельности по перехвату сообщений 2022 г. (*Interception of communications code of practice 2022*) (далее – Кодекс практики)[8], который дополняет британский Закон о регулировании следственных полномочий 2000 г.[9] Он устанавливает обязанность провайдеров и операторов связи обеспечить на технологическом уровне перехват и анализ сообщений, отправляемых через Интернет. Хотя еще в 2016 г., в соответствии с положениями британского Закона о полномочиях по проведению расследований 2016 г.[10] (далее – Закон «О проведении расследований»), был разрешен перехват сообщений.

Согласно п. 1.1 Кодекса практики, он применяется при реализации положений, предусмотренных Законом «О проведении расследований», содержит рекомендации по процедурам, которые необходимо соблюдать при перехвате сообщений и/или получении вторичных данных в соответствии с этими положениями. В первую очередь он предназначен для государственных органов, перечисленных в разделе 18 Закона «О проведении расследований», а также для операторов почтовой и телекоммуникационной связи и других заинтересованных организаций, чтобы помочь им соблюсти необходимые процедуры перехвата сообщений.

В п. 1.4 Кодекса практики отмечается, что некоторые права, изложенные в Законе о правах человека 1998 г. и в Европейской конвенции о защите прав человека и основных свобод (далее – ЕКПЧ), являются абсолютными, например, запрет на пытки, в то время как другие являются относительными.

Судя по всему, право на тайну связи, телефонных и почтовых сообщений Великобритания отнесла к относительным правам, нарушение которых возможно при определенных условиях. В Кодексе практики об этом так и написано. Перехват сообщений и получение вторичных данных из этих сообщений, скорее всего, повлекут за собой нарушение прав человека в соответствии с ЕКПЧ (п. 4.10 Кодекса практики). Кроме того, Кодексом практики признается, что «среди прав, подлежащих ограничению, есть право человека на уважение его личной и семейной жизни, жилища и переписки, предусмотренное статьей 8 ЕКПЧ» (п. 1.5. Кодекса практики).

Хотя должны отметить, что в законодательстве Великобритании возможность перехвата данных допускается для достижения законной цели, а действия, направленные на это, должны быть ей соразмерны. Закон «О проведении расследований» требует установления одного или нескольких оснований, указанных в ст. 20 Закона «О проведении расследований», для выдачи ордера, причем в любом случае конечной целью выступает обеспечение национальной безопасности. Основаниями для выдачи ордера на массовый перехват данных могут служить:

– интересы национальной безопасности;

– предотвращение или выявление тяжких преступлений, которые определены в ст. 263(1) Закона «О проведении расследований» как деяния, за которые лицо, достигшее 21 года и не имеющее судимостей, может быть справедливо приговорено к тюремному заключению на срок от трех лет и более. К таким преступлениям могут относиться деяния, связанные с насилием, ведущие к существенной финансовой выгоде или совершаемые группой лиц с общей целью;

– защита экономического благополучия Великобритании, если это соответствует интересам национальной безопасности.

Право на выдачу ордера на перехват с целью обеспечения экономического благополучия может быть реализовано только в том случае, если государственный секретарь сочтет обстоятельства, соответствующими интересам национальной безопасности, а решение будет одобрено судебным комиссаром. При этом право на выдачу ордера на перехват в целях защиты экономического благополучия может быть использовано только

---

[7] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10). (2001, 26 June). https://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html

[8] Interception of communications code of practice 2022. (2022). Gov. UK. https://www.gov.uk/government/publications/interception-of-communications-code-of-practice-2022/interception-of-communications-code-of-practice-2022-accessible

[9] Regulation of Investigatory Powers Act 2000 (RIPA). (2023, 25 July). Gov. UK. https://www.gov.uk/government/publications/regulation-of-investigatory-powers-act-2000-ripa/regulation-of-investigatory-powers-act-2000-ripa

[10] The Investigatory Powers Act. (2016, March 1). Gov. UK. https://www.gov.uk/government/collections/investigatory-powers-bill

тогда, когда необходимая информация касается действий или намерений лиц, находящихся за пределами Британских островов;

– приведение в действие положений документа о взаимной помощи Европейского союза или международного ордера на оказание взаимной помощи.

В связи с этим особый интерес представляет решение ЕСПЧ, вынесенное в 2021 г., фиксирующее противоречивую позицию[11]. С одной стороны, в решении ЕСПЧ говорится, что режим массового перехвата или массовой слежки нарушает свободу выражения мнений в соответствии со ст. 10 ЕКПЧ. С другой – Большая палата ЕСПЧ пришла к выводу, что массовый перехват сообщений не является нарушением прав человека[12], учитывая «множество угроз, с которыми государства сталкиваются в современном обществе»[13]. Для исключения нарушения положений ЕКПЧ при осуществлении массового перехвата судьи ЕСПЧ приходят к выводу, что процесс массового перехвата должен сопровождаться комплексными мерами безопасности, подлежать надзору и независимой проверке. Применяемые меры, направленные на массовый перехват, должны отвечать требованиям необходимости и соразмерности. Их проведение должно подчиняться законодательно зафиксированному порядку получения разрешения на его проведение и определения цели и масштабов применяемых мер.

Таким образом, в 2021 г. судьи ЕСПЧ признали возможность проведения массового перехвата в целях противодействия угрозам в современном обществе. Хотя еще в 2008 г. судьи ЕСПЧ подтвердили правомерность действий хостинг-провайдера, который отказался раскрывать информацию о лице, разместившем объявление на сайте. Поскольку, как посчитал хостинг-провайдер, его действия могут быть расценены как нарушение права на уважение частной и семейной тайны на основании ст. 8 ЕКПЧ [14].

Таким образом, мы видим, как за четыре года кардинально меняется мнение судей ЕСПЧ. Хотя Руководящий комитет по правам человека Совета Европы в своем докладе о долгосрочных перспективах развития правовой системы, основанной на ЕКПЧ, отметил, что «длительное неисполнение постановлений ЕСПЧ является вызовом авторитету самого суда и, как следствие, всей правовой системе, основанной на ЕКПЧ»[15].

В таком случае возникает закономерный вопрос: не подрывают ли сами судьи свой авторитет, вынося резко отличающиеся друг от друга решения? Возможным ответом будет то, что в настоящей геополитической ситуации на первое место выходит не столько авторитет судей, сколько формирование европейскими государствами практики массового перехвата информации в Сети на основании аргументов о наличии множества угроз, с которыми государства сталкиваются в современном обществе.

Однако перехват, осуществляемый массово, позволяет нам заключить, что европейские государства исходят из того, что вся информация, передаваемая в Интернете, по умолчанию является запрещенной для распространения или ограниченного доступа. Иначе в связи с чем тогда ведется речь о массовом перехвате? Кроме того, массовый перехват данных предполагает сбор информации обо всех пользователях, что противоречит основным принципам информационного общества.

Мы считаем, что с позиций российского законодательства такая практика является нарушением права на тайну связи. Так, в соответствии со ст. 15 «Тайна связи» Федерального закона «О почтовой связи» «тайна переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи, гарантируется государством. Осмотр и вскрытие почтовых отправлений, осмотр их вложений, а также иные ограничения тайны связи допускаются только на основании судебного решения. Все операторы почтовой связи обязаны обеспечивать соблюдение тайны связи. Информация об адресных данных пользователей услуг почтовой связи, о почтовых отправлениях, почтовых переводах денежных средств, телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые от-

[11] Big Brother Watch and Others v. the United Kingdom, Application Nos. 58170/13, 62322/14 and 24960/15 (ECtHR May 25, 2021).

[12] Там же.

[13] Там же.

[14] Информация о постановлении ЕСПЧ от 2 декабря 2008 г. по делу «K.U. (K.U.) против Финляндии» (жалоба № 2872/02). По делу обжалуется уклонение от принуждения сервис-провайдера раскрыть данные о личности разыскиваемого за размещение непристойного объявления о несовершеннолетнем на интернет-сайте знакомств. По делу допущено нарушение требований ст. 8 Конвенции о защите прав человека и основных свобод. (2009). Бюллетень Европейского Суда по правам человека, 4.

[15] Human Rights Intergovernmental Cooperation. Council of Europe portal. https://www.coe.int/web/human-rights-intergovernmental-cooperation/

правления, переводимые денежные средства, телеграфные и иные сообщения являются тайной связи и могут выдаваться только отправителям (адресатам) или их представителям» [16].

Причем процесс приема-передачи по Сети данных от одного пользователя к другому оставляет множество вторичных данных, которые так или иначе могут быть квалифицированы как персональные данные на основании ч. 1. ст. 3 ФЗ «О персональных данных»: так, персональные данные – «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»[17].

И для того, чтобы получить наиболее полную информацию об интернет-пользователе, законодательства Великобритании и Германии определяют порядок массового перехвата, т. е. перехвата всех возможных цифровых данных – первичных и вторичных (цифровых теней и цифровых следов). На это обращают внимание в совместном мнении судьи Лемменс, Вехабович и Бошняк по делу «Big Brother Watch и другие против Соединенного Королевства»[18]. В своем мнении они указывают на то, что в Интернете содержится гораздо больше коммуникационных данных, чем самого контента. Это связано с тем, что каждый фрагмент контента окружен множеством фрагментов коммуникационных данных[19]. Кроме того, получение связанных коммуникационных данных значительно расширяет возможности получения полной информации о человеке[20].

Далее они цитируют судью Верховного суда США Уильяма О. Дугласа, который в 1996 г., выражая несогласие по делу Осборн против Соединенных Штатов, описал угрозу массовой слежки: «Может наступить время, когда никто не сможет быть уверен, записываются ли его слова для последующего использования. Каждый будет опасаться, что его самые сокровенные мысли больше не принадлежат ему, а принадлежат правительству. Самые личные и конфиденциальные разговоры всегда будут открыты для нетерпеливых и любопытных ушей. Когда это время настанет, уединение и свобода перестанут существовать»[21].

Иными словами, судьи говорят именно об опасностях правам человека, которые могут идти от тотального перехвата и анализа всех цифровых данных человека, оставленных им в Интернете. Причем технологии анализа больших данных не ограничиваются открытыми данными, технологии способны проанализировать данные, связанные с зашифрованным контентом. Несмотря на то, что системы анализа данных не могут получить прямой доступ к содержанию и расшифровать какую-либо личную информацию об отправителе или получателе, они могут проанализировать коммуникационные данные, связанные с зашифрованным контентом. Такой контент содержит обширный массив личной информации, включая личность, его друзей, географические координаты отправителя и получателя, а также не только IP устройства передачи сообщения, но и его полные технические характеристики (Смирнов и др., 2021).

В Российской Федерации еще в 2003 г. Конституционный Суд Российской Федерации постановил, что «право каждого на тайну телефонных переговоров по своему конституционно-правовому смыслу предполагает комплекс действий по защите информации, получаемой по каналам телефонной связи, независимо от времени поступления, степени полноты и содержания сведений, фиксируемых на отдельных этапах ее осуществления. В силу этого информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям органам, осуществляющим оперативно-разыскную деятельность, необходимо получение судебного решения»[22]. В этом постановлении Конституционный Суд Российской Федерации подтверждает, что право на тайну сообщения распространяется на любые сведения, связанные с приемом и передачей, включая так называемые второстепенные данные.

---

[16] О почтовой связи. № 176-ФЗ от 17.06.1999. (1999). СЗ РФ, 29. Ст. 3697.

[17] О персональных данных. № 152-ФЗ от 27.07.2006. (2006). СЗ РФ, 31 (1 ч.). Ст. 3451.

[18] Big Brother Watch and Others v. the United Kingdom, Application Nos. 58170/13, 62322/14 and 24960/15 (ECtHR May 25, 2021).

[19] Там же.

[20] Там же.

[21] Osborn v. United States, 385 U.S. 323 (1966).

[22] Определение Конституционного Суда РФ от 02.10.2003 № 345-О «Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 года «О связи». (2004). Вестник Конституционного Суда РФ, 1.

Порядок массового перехвата сообщений

Закон G 10 разрешает автоматическое прослушивание внутренних и международных сообщений, а в § 2 G 10 определены обязанности поставщиков почтовых и телекоммуникационных услуг. Часть (1) § 2 гласит: «Любой, кто предоставляет почтовые услуги или участвует в оказании таких услуг в коммерческих целях, должен предоставить уполномоченному органу информацию об обстоятельствах почтовых отправлений и передать любые отправления, которые ему поручено собирать, пересылать или доставлять, в соответствии с ордером»[23].

Часть (1a) § 2 G 10 определяет, что «любой, кто предоставляет телекоммуникационные услуги или участвует в оказании таких услуг в коммерческих целях, имеет разрешение уполномоченного органа: предоставлять информацию о более подробных обстоятельствах телекоммуникаций, осуществляемых после вступления в силу ордера, разглашать содержимое, доверенное ему для передачи по телекоммуникационному каналу, разрешить мониторинг и запись телекоммуникаций, в том числе путем предоставления доступа к своим объектам в обычное рабочее время, а также разрешить использование технических средств для выполнения действия, предусмотренного § 11 (1a) G 10, путем оказания помощи уполномоченному органу в перенаправлении телекоммуникаций»[24]. Параграф 11 (1a) G 10 гласит: «Мониторинг и запись текущих телекоммуникационных сообщений, переданных после даты ордера, также могут осуществляться способом вмешательства в информационно-техническую систему, используемую заинтересованным лицом, когда это необходимо для обеспечения возможности мониторинга и записи, особенно в незашифрованном виде. Содержимое и обстоятельства связи, хранящиеся в информационно-технической системе заинтересованного лица с момента распоряжения, могут контролироваться и записываться, даже если они могли контролироваться и записываться в зашифрованном виде во время текущего процесса передачи в общедоступной телекоммуникационной сети»[25].

Федеральное министерство внутренних дел, строительства и внутренних дел Германии, в соответствии с законодательным декретом, наделено полномочиями согласовывать с Федеральным канцлером, Федеральным министерством экономики и энергетики, Федеральным министерством транспорта и цифровой инфраструктуры, Федеральным министерством юстиции и защиты прав потребителей и Федеральным министерством обороны, а также с согласия Федерального совета более детальные технические и организационные меры для выполнения обязательств по содействию массового перехвата сообщений. G 10 подробно определяет полномочия государственных органов и требования к провайдерам и операторам связи о содействии в массовом перехвате сообщений.

В Великобритании в соответствии с п. 4.11 Кодекса практики запросы на массовый перехват или целевое изучение данных могут подаваться только главой разведывательной службы или от его имени в интересах национальной безопасности. В соответствии с законодательством Великобритании перехват сообщений считается законным, если он осуществляется на основании ордера. Хотя возможен перехват сообщений и без ордера, например, такие случаи определены в гл. 12 Кодекса практики. Разделы 15(2)(b) и 136(2)(b) Закона «О проведении расследований» определяют, что ордер на перехват сообщений может разрешать сбор вторичных данных. Эти данные могут быть единственной целью ордера или дополнять основную задачу перехвата сообщений, указанную в документе. Также возможно получение ордера только на сбор вторичных данных, но и в этом случае законодательство допускает возможность перехвата содержимого сообщений, если эти данные необходимы для извлечения вторичных сведений из сообщений, упомянутых в ордере.

Кроме того, вторичные данные законодательством Великобритании разделяются на системные и идентификационные данные (разделы 16 и 137 Кодекса практики и раздел 263 Закона «О проведении расследований»). По нашему мнению, такое разделение проведено специально. Оно помогает технологии анализа данных наиболее точно определить личность пользователя Сети.

---

[23] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10). https://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html

[24] Там же.

[25] Там же.

К системным (в соответствии с разделом 263(4) Закона «О проведении расследований») относятся данные, которые содержатся в перехватываемых сообщениях, являются их частью и прикреплены к ним или логически связаны с ними.

Иными словами, под системными данными законодательство Великобритании понимает любые данные, которые связаны с функционированием систем или сервисов. Примерами таких данных могут быть: сообщения, отправляемые между элементами сетевой инфраструктуры, предназначенными для управления потоком данных; данные о конфигурации маршрутизатора или брандмауэра; информация об операционной системе, ее версии; история работы пользователя; альтернативные идентификаторы учетных записей, такие как адреса электронной почты или идентификаторы устройств пользователей; период времени, в течение которого маршрутизатор был активен в Сети.

Если системные данные входят в состав перехваченного сообщения, являются его частью, прикреплены к нему или логически связаны с ним, то они могут рассматриваться в качестве вторичных данных, в соответствии с разделами 16 и 137 Закона «О проведении расследований».

К идентификационным (в соответствии с разделами 263(2) и (3) Закона «О проведении расследований») относятся данные, которые содержатся в сообщении, являются его частью, прикреплены к нему или логически связаны с ним, могут быть логически отделены от остальной части сообщения и после отделения не раскрывают ничего из того, что можно было бы обоснованно считать смыслом (если таковой имеется) сообщения. Это данные, которые могут быть использованы для идентификации или содействия в идентификации пользователя Сети. Например, данные о любом лице, устройстве, системе или услуге; любом событии; местоположении человека, события или вещи. Как сказано в Кодексе практики, во многих случаях эти данные также могут быть системными. Однако бывают ситуации, когда они не обеспечивают или иным образом не способствуют функционированию сервиса или системы и, следовательно, не являются системными данными.

Исследователи утверждают, что разделение данных на системные и идентификационные служит обеспечению конфиденциальности, прозрачности и соразмерности в процессе сбора, обработки и хранения данных (Anyanwu et al., 2024; Sargiotis, 2024; Erdos, 2022; Nadji, 2024).

Однако, по нашему мнению, разделение цифровых данных на системные и идентификационные сделано преднамеренно. Поскольку анализ системных данных позволяет создать цифровой профиль человека, а анализ идентификационных данных позволяет связать этот цифровой профиль с пользователем. Фактически подтвердить, например, что именно этот конкретный пользователь выходил в Сеть в такой-то промежуток времени, именно он (с его устройства) осуществлял какие-то действия в Сети. Причем чем больше разных данных, связанных с человеком, будет проанализировано, тем точнее будет идентификация человека.

Европейский суд юстиции в нескольких делах рассматривал вопрос о том, является ли массовый сбор метаданных сообщений юридически эквивалентным слежке за их содержанием (Buono & Taylor, 2017; Mulligan, 2016)[26], и в результате постановил, что массовый сбор телефонных и интернет-данных со стороны спецслужб является незаконным. Суд ограничил полномочия агентств безопасности во Франции и других странах ЕС, допустив возможность проведения массового перехвата только в тех случаях, «если правительство столкнулось с серьезной угрозой национальной безопасности»[27]. Но и в такой ситуации полный доступ к пользовательским данным должен быть ограничен «строго необходимым» периодом и проходить под надзором суда или независимой профильной структуры[28].

Подобное дело рассматривал Суд ЕС, но по отношению к предприятиям США. В своем постановлении он отметил, что принцип безопасной гавани[29], который используется в США, применим только к предприятиям США, которые его придерживаются. Принцип безопасной гавани не распространяется на правительство США. Суд ЕС также отметил, что в США требования национальной безопасности, охраны общественных интере-

[26] Европейский суд признал незаконным массовый сбор данных спецслужбами. (2020, 6 октября). Securitylab.ru. https://www.securitylab.ru/news/512785.php

[27] Там же.

[28] Там же.

[29] Принцип безопасной гавани – это система законодательства США, в рамках которой существует защита от ответственности, возникающей в результате утечки данных, но для этого предприятия должны внедрять и поддерживать программы кибербезопасности, которые соответствуют признанным в отрасли стандартам передовой практики США.

сов и правопорядка преобладают над принципом безопасной гавани, поэтому предприятия США обязаны игнорировать без каких-либо сомнений как этот принцип, так и ограничение правил защиты, установленных данным принципом. Следовательно, наличие принципа безопасной гавани не препятствует властям США вмешиваться в основные права лиц, поскольку в США не существует норм, которые ограничивали бы такое вмешательство или обеспечивали бы эффективную правовую защиту от вмешательства[30].

Таким образом, подводя итог, должны отметить: для того чтобы перехваченные данные служили доказательством, необходимо не только иметь технологические инструменты перехвата данных и их анализа, но и должны быть сформированы правовые и организационные основы установления порядка применения таких технологий перехвата данных, требования к технологиям обработки и анализа данных. Именно это и является целью последних изменений в законодательстве Великобритании и Германии.

Правоприменительная практика

Отметим, что отправной точкой происходящих в настоящее время правовых изменений в области введения требований о применении технологий массового перехвата данных является разработанная Советом Европы и открытая для подписания в 2001 г. Европейская конвенция «О преступлениях в сфере компьютерной информации» (далее – Конвенция). За истекший период времени опубликовано большое число научных исследований как на территории Российской Федерации, так и за рубежом, обсуждающих возможные нарушения прав человека в Сети, связанные с реализацией положений Конвенции. Но большая часть исследователей связывает возникшее внимание к проблеме нарушения конфиденциальности данных о человеке в Сети с разоблачением, проведенным в июне 2013 г. Э. Сноуденом, правительств США и Великобритании в проведении массовой слежки и перехвате данных в Интернете. Хотя эти разоблачения произошли в 2013 г., т. е. спустя 12 лет после того, как Совет Европы открыл Конвенцию для подписания.

Э. Сноуден передал газетам «Вашингтон пост» и «Гардиан» информацию о слежке правительственных организаций США и Великобритании за пользователями в Интернете и собирании данных обо всех звонках пользователей. По данным, опубликованным в СМИ, в рамках сверхсекретной программы под кодовым названием ПРИЗМ (*PRISM*) спецслужбы собирают аудио- и видеофайлы, фотографии, электронную переписку, документы и данные о подключениях пользователей к тем или иным сайтам[31].

Так, согласно статье *The Guardian*[32], *GCHQ* (*Government Communications Headquarters*) имела возможность следить примерно за четвертью мировых кабелей, по которым передавался интернет-трафик, большая часть которого шла из США. Спецслужбы Великобритании регулярно перехватывали данные, идущие по оптоволокну в рамках принятых программ слежки «Управление Интернетом» и «Глобальная эксплуатация телекоммуникаций». Для анализа этих потоков данных было задействовано 300 аналитиков из *GCHQ* и 250 аналитиков из АНБ. После перехвата данных британское правительство использовало «селекторы» и «критерии поиска» для фильтрации контента и собираемых метаданных, поисковых запросов *Google*, покупок на *Amazon*, данных о местоположении и *IP*-адресов и других данных. Все перехваченные данные были собраны в огромную базу данных под кодовым названием «Полиция Кармы».

После опубликования информации последовали решения ЕСПЧ, в которых суд постановил, что использование Великобританией массовой слежки, о которой рассказал Э. Сноуден, нарушает фундаментальное право на неприкосновенность частной жизни. Однако, несмотря на это, в целях обеспечения национальной безопасности такие действия могут быть осуществлены специальными службами государств.

---

[30] Постановление ЕСПЧ от 25.05.2021 «Дело «Центр правосудия (Centrum for rattvisa) против Швеции» (жалоба № 35252/08). По делу обжалуются массовый перехват трансграничных сообщений разведывательными службами, сам факт существования правового режима скрытого наблюдения, а также пропорциональность и гарантии законодательства Швеции о перехвате информации в разведывательных целях. По делу было допущено нарушение требований статьи 8 Конвенции о защите прав человека и основных свобод. (2022). Прецеденты Европейского суда по правам человека, 1.

[31] Разоблачения Эдварда Сноудена. (2013, 24 октября). ТАСС. https://tass.ru/spravochnaya-informaciya/695264

[32] GCHQ taps fibre-optic cables for secret access to world's communications. (2013, June 21). https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

В июле 2013 г. в Трибунале по следственным полномочиям Великобритании (*IPT*)[33] было проведено разбирательство по поводу несанкционированного «массового перехвата», который называли также массовой слежкой. Жалоба была подана правозащитной организацией *Privacy International* вместе с девятью другими неправительственными организациями со всего мира, включая Американский союз защиты гражданских свобод[34].

Но уже в декабре 2014 г. *IPT* пришел к выводу, что и массовый перехват данных в Великобритании и США в целом является законным. В ответ десять правозащитных организаций подали иск в ЕСПЧ, оспаривая решение. Результатом этого дела было решение ЕСПЧ, в котором он постановил, что массовая слежка сама по себе не нарушает права человека, поскольку входит в «пределы усмотрения государства в выборе наиболее эффективных способов достижения законной цели – защиты национальной безопасности»[35]. Однако нарушением прав человека, по мнению ЕСПЧ, является отсутствие должного контроля за прослушиванием оптоволоконных кабелей и анализом собранных данных со стороны *GCHQ*. ЕСПЧ также отметил, что перехват метаданных и их анализ позволит получать более полную информацию о личной жизни человека, нежели сам контент.

Однако мы хотели бы обратить внимание на один интересный момент. В своих обсуждениях возможных нарушений прав, связанных с массовым перехватом данных, *IPT* и ЕСПЧ анализируют соответствие национального законодательства статьям ЕКПЧ. При этом они не ссылаются на Европейскую конвенцию о преступности в сфере компьютерной информации (Конвенция), хотя именно в Конвенции содержатся статьи, определяющие порядок массового перехвата, сбора и анализа данных.

Мы убеждены, что национальное законодательство европейских стран в области применения технологий массового перехвата данных основывается на положениях Конвенции, которая определяет дальнейшие правовые принципы. Этот вывод вытекает не только из анализа правонарушений, который мы провели, но и из положений Конвенции. Так, в ст. 20 Конвенции установлены правовые основания «сбора в режиме реального времени данных о потоках информации». В соответствии с п. «d» ст. 1 Конвенции под данными о потоках понимаются «любые компьютерные данные, относящиеся к передаче информации посредством компьютерной системы, которые генерируются компьютерной системой, являющейся составной частью соответствующей коммуникационной цепочки, и указывают на источник, назначение, маршрут, время, дату, размер, продолжительность или тип соответствующего сетевого сервиса»[36].

Пункт «b» ч. 1 ст. 20 Конвенции определяет право каждого государства принимать законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий в части «обязывания поставщиков услуг в пределах имеющихся у них технических возможностей: i) собирать или записывать с применением технических средств на территории этой Стороны; ii) сотрудничать с компетентными органами и помогать им собирать или записывать в реальном режиме времени данные о потоках информации, связанные с конкретными сообщениями на территории этой Стороны, передаваемыми по компьютерной системе»[37].

Требования, аналогичные тем, что зафиксированы в п. «b» ч. 1 ст. 20 Конвенции, зафиксированы и в п. «b» ч. 1 ст. 21 Конвенции, но касаются отношений, возникающих при «перехвате данных о содержании».

В ч. 2 ст. 20 Конвенции определено, что в случае, если одна из Сторон не может собирать или записывать поток данных с применением технических средств на своей территории в связи со спецификой своего внутригосударственного права, то Сторона может принять законодательные и другие обеспечительные меры, которые необходимы для сбора и регистрации данных в режиме реального времени о потоках информации,

---

[33] *IPT* – это суд, который рассматривает и выносит решения по жалобам, в которых утверждается, что государственные органы или правоохранительные учреждения незаконно использовали скрытые методы и нарушали право человека на неприкосновенность частной жизни. Также этот суд рассматривает иски против служб безопасности и разведки за действия, которые нарушают более широкий спектр прав человека.

[34] Privacy International v. Secretary of State for the Foreign and Commonwealth Office et al. (UK Mass Surveillance / UK-US Intelligence Sharing). https://privacyinternational.org/legal-case-files/1619/privacy-international-v-secretary-state-foreign-and-commonwealth-office-et-al

[35] Там же.

[36] Конвенция о преступности в сфере компьютерной информации (ETS N 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001). СПС «КонсультантПлюс».

[37] Там же.

относящихся к соответствующим сообщениям, на своей территории с использованием доступных технических средств.

Кроме того, в Конвенции определяются требования к принятию Сторонами всех необходимых мер на законодательном и ином уровне в целях сохранения в тайне поставщиком услуг как самого факта осуществления любых действий, так и информации об этих действиях. Данные требования зафиксированы в ст. 20 и 21 Конвенции.

Полномочия и процедуры, направленные на реализацию положений, закрепленных в ст. 20 и 21 Конвенции, принимаются каждой Стороной самостоятельно в рамках законодательных и иных мер, необходимых для установления полномочий и процедур, предусмотренных процессуальным законодательством Стороны в целях проведения конкретных уголовных расследований или судебного разбирательства (ч. 1 ст. 14 Конвенции).

Для операторов сотовой связи в ст. 18 Конвенции предусмотрены аналогичные требования о собирании сведений об абонентах. Так, ч. 3 ст. 18 под «сведениями об абонентах» понимается любая имеющаяся «у поставщика услуг информация о его абонентах в форме компьютерных данных или любой другой форме, кроме данных о потоках или содержании информации, с помощью которой можно установить: a) вид используемой коммуникационной услуги, принятые с этой целью меры технического обеспечения и период оказания услуги; b) личность пользователя, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание; c) любые другие сведения о месте установки коммуникационного оборудования, имеющиеся в соглашении или договоре на обслуживание»[38].

Таким образом, государства – члены Совета Европы и другие государства, подписавшие Конвенцию, приняли на себя юридические обязательства по внедрению ее положений в национальное законодательство.

Проведенное исследование позволяет сделать вывод, что в Великобритании и Германии был проведен анализ действующего законодательства для определения того, какие положения Конвенции уже реализованы, а какие требуют дополнительных мер.

В законодательство этих европейских государств внесены изменения, касающиеся мер, необходимых для установления полномочий и процедур сбора компьютерных данных в режиме реального времени и представления их в виде электронных доказательств, определен порядок получения ордеров, соблюдения правил цепочки хранения, определены понятия незаконного доступа, перехвата, повреждения данных. Также разработаны подробные инструкции и руководства для правоохранительных органов, как, например, Кодекс практики. Эти инструкции содержат разделы, в которых раскрываются аспекты перехвата данных, их собирания и анализа, получение ордеров на перехват сообщений, сотрудничество с иностранными правоохранительными органами.

Заключение

Изменения в законодательстве, касающиеся массового перехвата данных, рассмотренные нами на примере Великобритании и Германии, направлены на создание системы узаконенной идентификации человека в Интернете. Право на тайну связи Кодекс практики отнес к относительным правам человека, которое может быть нарушено в целях обеспечения безопасности государства от существующих угроз.

Мнения ЕСПЧ по этому вопросу нельзя оценить однозначно, поскольку решения ЕСПЧ в 2008 и 2021 гг. кардинально отличаются. Однако даже в решении ЕСПЧ от 2021 г. нельзя получить однозначный ответ. С одной стороны, очевидно, что если стоит выбор между обеспечением безопасности государства, общества и нарушением права на тайну связи одного человека – подозреваемого в правонарушении, то предпочтение должно быть отдано общественному благу. С другой стороны, согласно европейскому законодательству, речь идет о массовом перехвате сообщений, что подразумевает возможность доступа ко всем данным в Интернете, в котором присутствуют данные не только подозреваемого в правонарушении.

Кроме того, в формирующейся европейской модели массового перехвата сообщений существует еще один аспект, который требует внимания. Поскольку технологии массового перехвата должны иметь в своем

[38] Конвенция о преступности в сфере компьютерной информации (ETS N 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001). СПС «КонсультантПлюс».

арсенале провайдеры и операторы связи, то неизбежен риск нарушения тайны связи третьим лицом, например, сотрудником провайдера или оператора связи при выполнении им своих служебных полномочий. Для минимизации возможного риска должен быть обеспечен контроль за применением технологий массового перехвата. А лицо, которое предполагает, что данные о нем были получены при использовании технологии массового перехвата, должно иметь возможность получить информацию о собранных данных.

Таким образом, за последние несколько лет в европейском законодательстве начала формироваться определенная законодательством модель точной идентификации человека в Интернете. И, несмотря на то, что нами рассмотрены примеры изменения в законодательстве только двух европейских стран, мы можем утверждать, что аналогичные процессы происходят и в других государствах. В свою очередь, это позволяет сделать вывод, что конечной целью таких изменений является создание единой системы идентификации пользователей, которая обеспечивает доступ фактически в режиме реального времени к полной и исчерпывающей информации о действиях человека в Интернете.

Список литературы

Громова, Е. А., Петренко, С. А. (2023). Квантовое право: начало. *Journal of Digital Technologies and Law*, *1*(1), 62–88. EDN: FKAWRT. DOI: https://doi.org/10.21202/jdtl.2023.3

Добкач, Л. Я., Тарапанова, Е. А. (2019). Законодательный механизм ограничения распространения информации в сети Интернет. *Вестник УрФО. Безопасность в информационной сфере*, *2*(32), 30–38. EDN: LIXJZT. DOI: https://doi.org/10.14529/secur190205

Жарова, А. К. (2019). Правовое обеспечение информационной безопасности при использовании интернета вещей. *Информационное право*, *4*, 31–34. EDN: PWHKBY

Жарова, А. К. (2023). Обзор нормативных требований, обеспечивающих национальную безопасность США в сфере квантовых технологий. *Информационное общество*, 3, 69–77. EDN: CCHNJY

Жарова, А. К., Елин, В. М., Минбалеев, А. В. (2022). *Парадигма цифрового профилирования деятельности человека: риски, угрозы, преступления*. Москва: ООО «Русайнс». EDN: DNKVPR

Краулин, К. К. (2023). Правовое развитие способов идентификации в сети Интернет на примере правил идентификации клиентов провайдера хостинга. В сб. *Шестые Бачиловские чтения: сборник статей участников Международной научно-практической конференции, Москва, 2–3 февраля 2023 г.* (с. 243–250). Москва: Институт государства и права РАН. EDN: CECJPN

Кубасов, И. А., Лекарь, Л. А., Кондрущенков, О. М. (2020). Перспективные направления применения методов анализа больших данных в информационно-аналитическом обеспечении оперативно-разыскной деятельности. В сб. И. Г. Чистобородов, А. Л. Ситковский, В. О. Лапин (ред.), *Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: сборник статей Международной научно-практической конференции, Москва, 23 октября 2020 г.* (с. 436–442). Москва: Академия управления Министерства внутренних дел Российской Федерации. EDN: OSZJWB

Редкоус, В. М. (2021). Современные направления правого обеспечения государственной безопасности в Российской Федерации. В сб. *Пенитенциарная система и общество: опыт взаимодействия: сборник материалов VIII Международной научно-практической конференции, Пермь, 6–8 апреля 2021 г.* (Т. 1, с. 67–69). Пермь: Пермский институт Федеральной службы исполнения наказаний. EDN: CUTPJC

Смирнов, Д. В., Грушо, А. А., Забежайло, М. И., Тимонина, Е. Е. (2021). Система сбора и анализа информации из различных источников в условиях Big Data. *International Journal of Open Information Technologies*, *9*(4), 64–71. EDN: VNVDNQ

Смирнов, Е. В. (2018). Описание проблемы обработки и использования результатов анализа больших данных (Big Data). *Информационно-экономические аспекты стандартизации и технического регулирования*, *6*(46), 9. EDN: HDTWPN

Уварова, А. Г., Хроль, Е. В. (2024). Задачи прогнозной аналитики при обработке больших данных. В сб. *Виртуозы науки: сборник тезисов Международной научно-практической конференции студентов и молодых ученых за 2023 г., Краснодар, 6–15 ноября 2023 г.* (с. 542–543). Краснодар: Кубанский государственный аграрный университет им. И. Т. Трубилина. EDN: TBAJVY

Филипова, И. А. (2020). Алгоритмизация: воздействие на сферу труда и ее регулирование. *Российская юстиция*, *11*, 12–14. EDN: KLXDJU

Филипова, И. А. (2025). *Правовое регулирование искусственного интеллекта* (3-е изд., обновл. и доп.). Нижний Новгород: Нижегородский государственный университет имени Н. И. Лобачевского.

Халапсин, А. Б., Данилюк, С. А. (2022). Информационная система интеллектуального анализа больших массивов данных о правонарушениях в Республике Беларусь. *Вестник Белорусского государственного университета транспорта: наука и транспорт*, *2*(45), 35–39. EDN: APGIHK

Хисамова, З. И., Бегишев, И. Р. (2019). Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты. *Всероссийский криминологический журнал*, *13*(4), 564–574. EDN: QOFRXQ. DOI: https://doi.org/10.17150/2500-4255.2019.13(4).564-574

Anyanwu, A., Olorunsogo, T., Abrahams, T. O. et al. (2024). Data confidentiality and integrity: a review of accounting and cybersecurity controls in superannuation organizations. *Computer Science & IT Research Journal*, *5*(1), 237–253. EDN: PBRTQT. DOI: https://doi.org/10.51594/csitrj.v5i1.735

Begishev, I. R. (2022). Criminal-Legal Protection of Robotics: Notion and Content. *International Journal of Law in Changing World*, *1*(2), 73–83. EDN: OCYQJG. DOI: https://doi.org/10.54934/ijlcw.v1i2.33

Bekkulov, N. R. (2023). Internet user classification and identification without using personal data. The World of Science without Borders: proceedings of the 10th All-Russian scientific and practical conference (with international participation) for young researchers, Tambov, 21 апреля 2023 года (с. 266–270). Тамбов: Издательский центр ФГБОУ ВО «Тамбовский государственный технический университет». EDN: OPWSFQ.

Buono, I., & Taylor, A. (2017). Mass surveillance in the CJEU: forging a European consensus. *Camb Law J*, *76*, 250–253.

Erdos, Dr. D. (2022). Identification in personal data: Authenticating the meaning and reach of another broad concept in EU data protection law. *Computer Law & Security Report*, *46*, 105721. EDN: CMORYQ. DOI: https://doi.org/10.1016/j.clsr.2022.105721

Mulligan, A. (2016). Constitutional aspects of international data transfer and mass surveillance. *Ir Jurist*, *55*, 199–208.

Nadji, B. (2024). Data Security, Integrity, and Protection. In McClellan, S. (Eds.), *Data, Security, and Trust in Smart Cities*. *Signals and Communication Technology*. Springer, Cham. https://doi.org/10.1007/978-3-031-61117-9_4

Sargiotis, D. (2024). Data Security and Privacy: Protecting Sensitive Information. In *Data Governance*. Springer, Cham. https://doi.org/10.1007/978-3-031-67268-2_6

References

Anyanwu, A., Olorunsogo, T., Abrahams, T. O. et al. (2024). Data confidentiality and integrity: a review of accounting and cybersecurity controls in superannuation organizations. *Computer Science & IT Research Journal*, *5*(1), 237–253. https://doi.org/10.51594/csitrj.v5i1.735

Begishev, I. R. (2022). Criminal-Legal Protection of Robotics: Notion and Content. *International Journal of Law in Changing World*, *1*(2), 73–83. https://doi.org/10.54934/ijlcw.v1i2.33

Bekkulov, N. R. (2023). Internet user classification and identification without using personal data. The World of Science without Borders: proceedings of the 10th All-Russian scientific and practical conference (with international participation) for young researchers, Tambov, 21 April 2023 (pp. 266–270). Tambov: Publishing Center of Tambov State Technical University.

Buono, I., & Taylor, A. (2017). Mass surveillance in the CJEU: forging a European consensus. *Camb Law J*, *76*, 250–253.

Crowlin, K. K. (2023). Legal development of methods of identification on the internet by the example of identification rules hosting provider clients. *Sixth Bachilov readings: A collection of articles by participants of the International Scientific and Practical Conference*, Moscow, February 2–3, 2023 (pp. 243–250). Moscow: Institute of State and Law of the Russian Academy of Sciences. (In Russ.).

Dobkach, L. Ya., & Tarapanova, E. A. (2019). Legislative mechanism for limiting the dissemination of information in the Internet. *Bulletin of the Ural Federal District. Information security*, *2*(32), 30–38. (In Russ.). https://doi.org/10.14529/secur190205

Erdos, Dr. D. (2022). Identification in personal data: Authenticating the meaning and reach of another broad concept in EU data protection law. *Computer Law & Security Report*, *46*, 105721. https://doi.org/10.1016/j.clsr.2022.105721

Filipova, I. A. (2020). Algorithmization: impact on the labour market and its regulation. *Rossiyskaya yustitciya*, *11*, 12–14. (In Russ.).

Filipova, I. A. (2025). *Legal regulation of artificial intelligence* (3rd ed., updated and compl.). Nizhny Novgorod: Nizhny Novgorod State University named after N.I. Lobachevsky. (In Russ.).

Gromova, E. A., & Petrenko, S. A. (2023). Quantum law: the beginning. *Journal of Digital Technologies and Law*, *1*(1), 62–88. (In Russ.). https://doi.org/10.21202/jdtl.2023.3

Khalapsin, A. B., & Daniliuk, S. A. (2022). Information system for intelligent analysis of large data on offenses in the Republic of Belarus. *Bulletin of the Belarusian State University of Transport: Science and Transport*, *2*(45), 35–39. (In Russ.).

Khisamova, Z. I., & Begishev, I. R. (2019). Criminal liability and artificial intelligence: theoretical and applied aspects. *Russian Journal of Criminology*, *13*(4), 564–574. (In Russ.). https://doi.org/10.17150/2500-4255.2019.13(4).564-574

Kubasov, I. A., Lekar, L. A., & Kondrushchenkov, O. M. (2020). Promising directions to apply big data analysis in information-analytical support of operational-investigative activities. In I. G. Chistoborodov, A. L. Sitkovsky, V. O. Lapin (Eds.), *Strategic development of the Russian law enforcement system: status, trends, prospects: collection of articles of the International scientific-practical conference, Moscow, October 23, 2020* (pp. 436–442). Moscow: *Academy of Management of the Ministry of Internal Affairs of the Russian Federation*. (In Russ.).

Mulligan, A. (2016). Constitutional aspects of international data transfer and mass surveillance. *Ir Jurist*, *55*, 199–208.

Nadji, B. (2024). Data Security, Integrity, and Protection. In McClellan, S. (Eds.), *Data, Security, and Trust in Smart Cities*. *Signals and Communication Technology*. Springer, Cham. https://doi.org/10.1007/978-3-031-61117-9_4

Redkous, V. M. (2021). Modern directions of the legal support of state security in the Russian Federation. In *Penitentiary system and society: experience of interaction: Proceedings of the 8th International scientific-practical conference, Perm, April 6-8, 2021* (Vol. 1, pp. 67–69). Perm: *Perm Institute of the Federal Penitentiary Service* (pp. 67–69). (In Russ.).

Sargiotis, D. (2024). Data Security and Privacy: Protecting Sensitive Information. In *Data Governance*. Springer, Cham. https://doi.org/10.1007/978-3-031-67268-2_6

Smirnov, D. V., Grusho, A. A., Zabezhailo, M. I., & Timonina, E. E. (2021). System for collecting and analyzing information from various sources in Big Data conditions. *International Journal of Open Information Technologies*, *9*(4), 64–71. (In Russ.).

Smirnov, E. V. (2018). Description of the problem of processing and using the results of the analysis of Big Data. *Information and Economic Aspects of Standardization and Technical Regulation*, *6*(46), 9. (In Russ.).

Uvarova, A. G., & Khrol, E. V. (2024). Tasks of predictive analytics in big data processing. In *Virtuosos of science: collection of abstracts of 2023 International scientific-practical conference for students and young researchers, Krasnodar, November 6–15, 2023* (pp. 542–543). Krasnodar: I.T. Trubilin Kuban State Agrarian University. (In Russ.).

Zharova, A. K. (2019). Legal support of information security in the use of the internet of things. *Information Law*, *4*, 31–34. (In Russ.).

Zharova, A. K. (2023). Review of regulatory requirements that ensure US national security in the field of quantum technologies. *Information Society*, *3*, 69–77. (In Russ.).

Zharova, A. K., Elin, V. M., & Minbaleev, A. V. (2022). *Paradigm of digital profiling of human activity: risks, threats, crimes*. Moscow*:* Rusains. (In Russ.).

Вклад автора

Автор подтверждает, что полностью отвечает за все аспекты представленной работы.

Author's contribution

The author confirms sole responsibility for all aspects of the work.

Конфликт интересов / Conflict of Interest

Автором не заявлен / No conflict of interest is declared by the author

История статьи / Article history

Дата поступления / Received 04.02.2025
Дата одобрения после рецензирования / Date of approval after reviewing 26.03.2025
Дата принятия в печать / Accepted 12.05.2025