УДК 342.72/.73
DOI 10.52468/2542-1514.2024.8(4).63-72

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦИФРОВОГО ПРОФИЛИРОВАНИЯ ЧЕЛОВЕКА В ПРАКТИКЕ ЗАРУБЕЖНЫХ СТРАН*

С.С. Кузнецова
Уральский государственный юридический университет имени В.Ф. Яковлева, г. Екатеринбург, Россия

Информация о статье
Дата поступления –
13 июня 2024 г.
Дата принятия в печать –
10 сентября 2024 г.
Дата онлайн-размещения –
20 декабря 2024 г.

Ключевые слова
Цифровые следы, персональные данные, профилирование, автоматизированное принятие решений, неприкосновенность частной жизни, ограничение профилирования, прозрачность

Проведен анализ практики зарубежных стран и сформулированы ключевые параметры использования «цифровых следов» для целей профилирования человека: определен объем цифровых следов, раскрыты подходы к определению понятия профилирования, сформулированы преимущества и риски каждого из них, в том числе в связи с воздействием на реализацию принципа прозрачности, проанализирован объем прав и обязанностей субъектов правоотношений в процессе обработки персональных данных с применением профилирования. Сделан вывод, что наиболее благоприятными условиями является законодательное признание профилирования с участием человека, разграничение порядка раскрытия информации о профилировании в зависимости от его целей, а также ограничение полностью автоматизированного процесса необходимостью получения согласия.

LEGAL REGULATION OF DIGITAL PROFILING OF A PERSON IN THE PRACTICE OF FOREIGN COUNTRIES**

Svetlana S. Kuznetsova
Ural State Law University named after V.F. Yakovlev, Yekaterinburg, Russia

Article info
Received –
2024 June 13
Accepted –
2024 September 10
Available online –
2024 December 20

Keywords
Digital traces, personal data, profiling, automated decision-making, privacy, restriction of profiling, transparency

The subject. The legislation of foreign countries concerning human digital profiling, the advantages and disadvantages of profiling process, that affect the implementation and protection of certain constitutional rights, including the right of privacy, dignity of the human person and right to manage personal data.
The purpose of the article is to systematize the approaches to human digital profiling reflected in the legislation of foreign countries.
Methodology. The author is guided by formal dogmatic, induction and comparative law methods in research.
Main results and conclusions. The author formulates approaches to the concept of human digital profiling that have been developed in the practice of foreign countries. The concept of digital profiling involves the processing of most digital traces, however, the profiling process itself is sometimes limited to solely automated forms of decision-making (most states of the USA), which significantly limits the rights of the personal data subject. Definition of automated forms of decision-making in the personal data protection law of China is positively assessed, because that process is not directly related to personal data, but to areas of human life, which most accurately reflects the essence of the processing digital traces during profiling. Consent to solely automated profiling of a human entailing legal or other significant consequences is required only in the countries of the European Union, while in the USA and China only a subsequent refusal to apply decisions is possible.

* Исследование выполнено при финансовой поддержке РНФ в рамках научного проекта 24-28-01378 «Разработка концепции правового регулирования цифрового профилирования, социального скоринга и использования «цифровых следов».
** The study was carried out with financial support from the Russian Science Foundation within the framework of scientific project 24-28-01378 “Development of a concept for legal regulation of digital profiling, social scoring and the use of “digital traces”.

ISSN 2542-1514 (Print)

It is concluded that obtaining direct consent, considering the volume of information processed about identity for the human profiling and the importance of its consequences for the individual, is a necessary condition for ensuring individual rights. A tendency has been identified to differentiate the procedure for implementing the principle of transparency depending on whether human profiling is carried out by public authorities while making individual decisions, in public interests or by business for commercial purposes. The approach of the EU and China, which provides for the need to disclose the formula of the profiling algorithm when used by public authorities, is a positive practice for implementing the principle of transparency in conjunction with the implementation of the right to know about the activities of a public authority. At the same time, in Sweden and Germany a successful attempt has been made to find a balance between the interests of the individual and the profiling controller when using it for commercial purposes. The American model of legal regulation of personality profiling is assessed negatively, since it removes the possibility of control over the processing of personal data in the human profiling by public authorities and establishes a minimum scope of rights of the data subject when profiling for commercial purposes.

1. Введение

Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы определена в России как одна из целей национального развития[1], что предполагает автоматизацию принятия управленческих решений и совершенствование средств управления цифровыми данными. В эпоху больших данных использование традиционных методов и инструментов обработки и хранения информации невозможно [1, p. 1], это обусловлено особенностями больших данных: генерирование преимущественно машинами, их неструктурированность, наличие в составе информации, которая не имеет ценности [2, с. 14–15]. Одним из эффективных средств обработки больших данных, извлечения информации и ее организации является цифровое профилирование, позволяющее «уменьшить информационную перегрузку, сделать ее управляемой, извлечь из нее смысл и восстановить контроль над последствиями своих действий» [3, p. 30].

Длительное время термин «профиль» ассоциировался исключительно с криминалистическим профилированием как методом установления личности преступника [4, с. 111], выявления его личностных и поведенческих характеристик [5]. Однако развитие цифровых технологий раскрыло потенциал использования цифрового профилирования в целях маркетинга, управления персоналом [6, p. 49], государственного управления [7]. На сегодняшний день профилирование представляет собой «процесс сбора и анализа информации о человеке или организации, в том числе обращающейся в сети “Интернет”» [8, с. 9], а также «обращения с человеком или группой в свете этих характеристик (т. е. процесса применения профиля)» [9, p. 77].

Цифровая трансформация общества обеспечивает повышение эффективности правореализационных процессов [10, с. 10]. Однако автоматизация обработки цифровых следов отличается не только рядом преимуществ [11], но и несет угрозу, особенно в случаях, когда осуществляется в отношении персональных данных. Ключевым вопросом становится поиск баланса интересов субъекта автоматизированной обработки данных и субъекта данных, желающего защитить права на неприкосновенность частной жизни, уважение достоинства личности. Так как профилирование работает с информацией о личности и нацелено на получение новых знаний о ней, в том числе персональных, всегда существует риск утраты субъектом данных контроля над ними [12, с. 92].

Цель настоящего исследования заключается в выявлении и формулировании концепции правового регулирования цифрового профилирования. Для достижения цели проведен анализ норм законодательства и правоприменительной практики в зарубежных странах, определены понятие и цели профилирования, объем информации, подлежащей обработке, гарантии прав лиц, подвергшихся профилированию.

2. Понятие профилирования

В законодательстве профилирование рассматривается в свете обработки персональных данных, поэтому определение понятия раскрывается в специальном законодательстве о защите данных.

[1] Указ Президента РФ от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Российская газета. 2024. 11 мая.

Общий регламент по защите данных (*GDPR*) Европейского Союза (далее также – ЕС) использует широкую концепцию профилирования: «*любая* форма автоматической обработки персональных данных», нацеленная на формирование информации о личности, в частности о здоровье, личных предпочтениях, интересах, экономическом положении, а также создание вероятностных моделей поведения человека [13], например результативность работы, надежность и перемещения. Ввиду того, что оценка информации с позиции наличия в ней персональных данных осуществляется контекстуально [14], то обработка большинства цифровых следов может подпадать под требования Общего регламента. Так как Регламент признаёт любые формы профилирования, то под регулирование попадают как случаи полной автоматизации процесса принятия решения, так и основанные на участии человека [15].

В США на федеральном уровне отсутствует законодательство, регламентирующее процесс профилирования, однако данный термин используется в законодательстве тринадцати штатов. В штатах Вирджиния, Монтана и Нью-Йорк понятие профилирования близко по содержанию воспроизводит концепцию ЕС: «*любая* форма автоматической обработки персональных данных для оценки, анализа или прогнозирования характеристик идентифицированной или идентифицируемой личности в таких сферах, как экономическое положение, состояние здоровья, личные предпочтения, интересы, поведение, надежность, местоположение или передвижение». В штатах Делавэр, Индиана, Коннектикут, Нью-Гемпшир, Теннесси, Техас, Флорида под профилирование подпадают случаи исключительно автоматизированного процесса, в связи с чем обработка информации о личности с участием человека исключает получение дополнительных гарантий, предусмотренных законодательством. В штатах принята широкая концепция персональных данных, что позволяет обеспечить регулирование процесса профилирования в отношении большинства цифровых следов. В штате Калифорния к личной информации относится не только та, что напрямую идентифицирует личность, но и описывающая характеристики субъекта данных (список покупок, поисковые запросы), которая может быть связана с ним, и, прямо или косвенно, позволяет идентифицировать в совокупности с другими данными.

В Законе КНР «О защите персональных данных» понятие профилирования отсутствует, однако в ст. 73 дается определение автоматизированного принятия решения: «деятельность по автоматическому анализу и оценке поведенческих привычек, увлечений или экономического статуса, состояния здоровья или кредитоспособности человека с помощью компьютерных программ и принятию решений». Понятие автоматического принятия решений раскрыто не через персональные данные, а через информацию об отдельных сферах жизни личности, таким образом, анализ любых цифровых следов может рассматриваться как автоматическое принятие решений, если получена та информация о личности, которая отражена в определении. Анализ ст. 73 и 24 указанного закона позволяет сделать вывод, что автоматизированное принятие решения не исключает возможность участия в данном процессе человека, однако данный факт будет иметь правовые последствия с позиции объема прав субъекта данных.

В законодательстве всех рассмотренных стран профилирование предполагает обработку большинства цифровых следов, которые связаны с личностью или описывают ее, идентифицируют или позволяют идентифицировать (страны ЕС, США), обеспечивают возможность получить информацию об отдельных сферах жизни человека (КНР). Большинство стран допускает участие человека в процессе профилирования, что обеспечивает субъекту данных возможность получить дополнительные гарантии реализации права на управление персональными данными, однако в отдельных штатах США концепция предусматривает исключительно автоматизированные варианты принятия решений. Представляется, что понятие автоматизированного принятия решений, предложенное в Китае, наиболее точно отражает сущность профилирования, так как обработке подвергаются любые цифровые следы [16, p. 254; 17, с. 46], а не только персональные данные. Такой подход может обеспечить более высокий уровень гарантированности прав личности, так как субъект данных будет знать о наличии факта профилирования. В Китае при использовании алгоритмов автоматизированного принятия решений в целях прямого маркетинга предусматривается обязанность оператора предложить варианты обработки, не основанные на характеристиках личности, или отказаться от маркетинга.

3. Гарантии прав человека при цифровом профилировании

В соответствии со ст. 22 Общего регламента ЕС субъект данных вправе не быть подвергнутым профилированию с исключительно автоматизированным принятием решения, если оно влечет пра-

ISSN 2542-1514 (Print)

вовые последствия или «похожим образом влияет на него». Не исключается возможность обращения к соответствующим алгоритмам в одном из следующих случаев:

– они не влекут правовые или аналогичные последствия для субъекта данных;

– получено прямое согласие;

– необходимо для заключения договора с субъектом данных или его исполнения;

– разрешен нормативными правовыми актами ЕС или государства – члена ЕС (например, в ст. 37 Федерального закона ФРГ «О защите информации» обработка возможна в связи с исполнением договора страхования[2]).

Автоматизированный процесс обработки персональных данных предполагает соблюдение всех принципов Общего регламента, в том числе прозрачности. Его реализация налагает обязанность предоставить доступным языком информацию в соответствии со ст. 13 и 14, в том числе о наличии «процесса автоматизированного принятия решения, включая профилирование, и, как минимум, о соответствующей логике, а также о значимости и предполагаемых последствиях обработки для субъекта данных». Отдельно гарантируется предоставление информации о наличии права отказаться от профилирования в целях маркетинга. Как отмечает А.Н. Мочалов, «формулировка *GDPR* не обладает необходимой конкретикой и не позволяет однозначно сказать, каким образом контролер персональных данных должен исполнить соответствующую обязанность» [18, с. 81]. В странах Европейского Союза сложно формируется практика по определению порядка применения данной нормы в части раскрытия информации о логике алгоритмов. В Австрии суд признал, что принцип прозрачности влечет за собой предоставление информации, которая позволяет лицу понимать автоматизированное решение, включая раскрытие входных данных, параметры и переменные, используемые в процессе профилирования, математическую формулу, используемую для расчета рейтинга, объяснение каждой категории профиля, а также того, почему лицо было привязано к определенному профилю. Однако неисполнение решения суда, обоснованное тем, что запрашиваемая информация составляет коммерческую тайну, стало поводом для обращения в Европейский Суд[3]. В ряде стран формируется тенденция разного толкования содержания принципа прозрачности в зависимости от того, используются алгоритмы автоматизированных решений при осуществлении публичной власти или в коммерческой деятельности. В Швеции при рассмотрении вопроса о деятельности банка суд пришел к выводу, что алгоритмические формулы не рассматриваются в качестве значимой информации [19, p. 21], при этом в деле Треллеборг, где алгоритмы применялись в целях принятия решения о выдаче социальной помощи, указано, что «алгоритм представляет собой административный документ», и без его открытости истцы не могут обеспечить защиту своих прав, т. е. в отношениях с публичной властью прозрачность алгоритмов вытекает из права знать [20]. Аналогично в Гаагском районном суде было признано незаконным использование алгоритмов автоматизированного принятия решения *SyRI* в сфере социального обеспечения в связи с нарушением принципов прозрачности и подконтрольности. Необходимость защиты коммерческой тайны получила отражение в ст. 63 Преамбулы Общего регламента, где подчеркивается, что право знать об алгоритме автоматизированного профилирования и последствиях такой обработки не может подрывать коммерческую тайну. Вывод о балансе интересов при автоматизированном принятии решения в коммерческих целях сформулирован федеральным судом Германии в отношении формулы, положенной в основу скоринга[4].

При профилировании также гарантируется:

– получение ясной информации о праве отказа от профилирования в целях прямого маркетинга и возражать против профилирования, осуществляемого в целях достижения публичного интереса, или законных целей контролера;

– запрет на исключительно автоматизированное принятие решений с применением специальных категорий персональных данных;

– право требовать вмешательства со стороны контролера в процесс полностью автоматизированного принятия решений, выражать свою позицию, а также оспаривать решение в случае, если профилирование осуществляется на основании согласия или в целях заключения / исполнения договора.

Страны – участницы ЕС могут предусмотреть дополнительные гарантии прав субъекта данных в случае обращения к полностью автоматизированным системам принятия решения. Дж. Мальджери

[2] Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097).
[3] Dun & Bradstreet Austria, Case C-203/22.
[4] BGH, Urteil vom 28.01.2014 – VI ZR 156/13, BGHZ 200, 38 Rn. 24ff.

ISSN 2658-4050 (Online)

отмечает, что такие гарантии получили отражение в небольшом количестве стран и носят «процедурный» характер (Ирландия), раскрывают требования к порядку рассмотрения обращений и возражений при использовании алгоритмов автоматического принятия решений, или «проактивный», устраняющий пробелы в регулировании *GDPR* [21] (право на разъяснение алгоритмических решений на основании Кодекса отношений между общественностью и администрацией Франции).

В США порядок обработки информации о личности федеральными органами исполнительной власти регламентируется законами «О частной жизни» и «Об электронном правительстве». Оба закона обладают рядом недостатков, препятствующих эффективной защите прав в процессе профилирования. Закон «О частной жизни» обеспечивает защиту лишь данных, которые «отражают характеристики и качества индивида», «поэтому *IP*-адрес, например, не подлежит защите как запись, так как идентифицирует устройство, а не пользователя» [22, с. 110]. Информация подпадает под защиту при условии, что она является частью системы записей и извлекается через идентификатор лица. Применение современных технологий позволяет обрабатывать информацию и профилировать без извлечения информации через идентификатор. Несоответствие закона современным реалиям подтверждается в докладе Счетной палаты США: среди 25 опрошенных агентств большинство признало, что при сборе и обработке информации не использовали личный идентификатор[5], таким образом, субъект информации лишался защиты права на неприкосновенность частной жизни.

Закон «Об электронном правительстве» расширил круг информации, рассматриваемой в качестве конфиденциальной: под «идентифицируемой формой» понимается «*позволяющая прямым или косвенным путем* идентифицировать личность лица, к которому относится информация», таким образом, под действие попадают географические метки и иные дескрипторы. Однако закон не устанавливает пределы обработки цифровой информации: если Закон «О частной жизни» обязывает собирать наибольший пласт необходимой информации непосредственно от самого субъекта, то Закон «Об электронном правительстве» позволяет собирать информацию о физических лицах из различных источников, в том числе путем закупки коммерческих баз данных и объединения их с государственными базами. В случае, если агентства систематически дополняют свои базы данных базами, содержащими информацию в идентифицируемой форме, полученными из коммерческих или общедоступных источников, то они обязаны провести оценку воздействия на конфиденциальность, а также разместить информацию о целях и объеме обработки цифровых данных на своем сайте (с широким перечнем исключений, когда такое раскрытие не требуется). Таким образом, сфера цифровых неидентифицируемых следов остается пробельной в правовом регулировании, что позволяет собирать информацию без контроля со стороны субъекта данных. При соединении ее с базами данных самих органов исполнительной власти цифровые неидентифицируемые следы могут обеспечить идентификацию лица, позволить создать новые личные данные. Аналитики отмечают факты сотрудничества органов исполнительной власти с агрегаторами коммерческих баз данных для сканирования веб-сайтов и закупки приложения для геолокации смартфонов [23].

В законодательстве штатов США на оператора обработки данных при профилировании возлагаются дополнительные обязанности:

1. Проводить оценку защиты данных, обрабатываемых в целях профилирования, в случае, если имеют место риски незаконных действий.

2. Обеспечить наличие функции отказа от полностью автоматизированного профилирования, если оно ведет «к юридическим или иным значимым последствиям», под которыми понимаются решения о предоставлении или отказе в предоставлении финансовых или кредитных услуг, жилья, страхования, медицинских услуг, доступа к основным товарам и услугам, получения образования, трудоустройства или уголовное преследование.

В отличие от стран ЕС, штаты США не требуют получения согласия и не предусматривают возможность возражать против профилирования. Ни один из штатов США не гарантирует право субъекта данных получить информацию об использовании алгоритмов профилирования и принципах их работы, о том, какие новые данные могут быть созданы. Право «знать» предполагает раскрытие достоверной информации о том, какие данные и из каких источников подлежат сбору, цели обработки, срок хранения и категории информации, передаваемой третьим лицам

[5] Wilshusen G.C. Federal Law Should Be Updated to Address. Changing Technology Landscape. United States Government Accountability Office, July 31, 2012. P. 7. URL: https://www.gao.gov/assets/gao-12-961t.pdf.

ISSN 2542-1514 (Print)

с указанием целей, содержание прав субъекта данных и порядка их реализации, в том числе права на отказ от обработки персональных данных в целях профилирования. Таким образом, принцип прозрачности не реализуется [18, с. 84–85], а субъекты данных не могут контролировать вновь созданную информацию о них. Законодательство штатов о защите персональных данных не распространяется на деятельность органов государственной власти и органов местного самоуправления, процесс профилирования личности, осуществляемый последними, находится вне контроля со стороны субъекта данных.

В Китае не запрещается обращение к полностью автоматизированным способам принятия решений с применением персональных данных, получения согласия не требуется, однако, если профилирование оказывает существенное влияние на права и интересы лица, это лицо будет вправе потребовать объяснений и отклонить принятое решение. В соответствии со ст. 24 Закона «О защите персональных данных» автоматизированная обработка персональных данных должна обеспечивать прозрачность принятия решений, справедливость и беспристрастность. В законе не раскрыто содержание принципа прозрачности применительно к автоматизированной обработке, в связи с чем должны применяться общие положения ст. 17 о необходимости раскрытия информации о целях и методе, способе и сроках хранения данных, порядке осуществления физическим лицом прав. Указание на метод обработки позволяет сделать вывод, что должна быть предоставлена информация о факте использования автоматизированных форм принятия решения, о персональных данных, которые будут обработаны, и, как отмечают Х. Ву и Х. Лин, «основная информация об используемом алгоритме» [24, p. 1187]. Содержание права на объяснение исследователями раскрывается по-разному, в зависимости от того, кто является субъектом обработки данных – органы государственной власти или коммерческие организации. В первом случае право знать предполагает право на объяснение причин принятия того или иного решения, что требует раскрытия самого алгоритма. В случае профилирования в коммерческих целях человек вправе запросить только «объяснение основных обстоятельств использованного алгоритма» ввиду того, что сам алгоритм может охраняться коммерческой тайной [24, p. 1190]. В Положении об управлении алгоритмическими рекомендациями в информационных службах Интернета[6] подчеркивается рекомендательный характер оптимизации прозрачности и объяснимости правил поиска, сортировки, выбора, чтобы избежать негативного воздействия и предотвратить разногласия. В соответствии с п. 14 данного положения на поставщика алгоритмических рекомендаций также возлагается обязанность информировать заметным образом о факте использования алгоритмов, предполагаемых целях, основных механизмах работы, что позволяет «устранить риски необоснованных отказов… предоставить необходимую информацию, такую как область применения алгоритма, пользователь услуги, уровень риска алгоритма и другие, на том основании, что четкие законодательные установления в этом отношении отсутствуют» [25, с. 350].

4. Заключение

Подходы к регулированию профилирования личности значительно отличаются в практике зарубежных стран, при этом можно выделить несколько тенденций:

• Формирование широкой концепции профилирования, которая позволяют ввести в правовое поле обработку большинства цифровых следов.

• Разграничение подходов к реализации принципа прозрачности в зависимости от целей профилирования. В ЕС и Китае использование автоматизированных алгоритмов принятия решений налагает на органы публичной власти обязанность по раскрытию формулы, обеспечению подконтрольности процесса обработки данных, в то время как алгоритм, используемый в коммерческих целях, может быть защищен тайной. Данный подход представляется оправданным, так как прозрачность принятия индивидуальных решений со стороны органов власти имеет особо важное значение для личности. Не менее важно обеспечение справедливого и прозрачного профилирования со стороны частного сектора с соблюдением баланса интересов сторон, что предполагает раскрытие полной и достоверной информации о факте профилирования, обрабатываемой информации, целях, и возможных последствиях, в том числе о вероятности формирования новой информации о личности, что требует точных и взвешенных формулировок. Наличие в Китае обязательных и рекомендуемых для раскрытия элементов информации о профилировании представляется достаточно

[6] *Provisions on the Management of Algorithmic Recommendations in Internet Information Services* (2021).

интересным подходом, однако предложенные формулировки отличаются отсутствием необходимого уровня формальной определенности, в связи с чем могут толковаться на практике по-разному. Наиболее неблагоприятным является правовое регулирование профилирования в США, так как специальные требования к обеспечению прозрачности профилирования в деятельности органов государственной власти отсутствуют, что позволяет последним собирать и формировать неограниченный объем информации о личности. Законодательство штатов, регламентирующее профилирование в коммерческих целях, также склонно нарушать баланс в пользу бизнеса: в большинстве штатов раскрытие факта о профилировании, его целях и обрабатываемой информации необходимо только при использовании исключительно автоматизированной модели принятия решений, таким образом, даже незначительное участие человека в данном процессе лишает лицо права на получение информации о факте профилирования, а также освобождает оператора данных от обязанности оценивать риски использования алгоритмов.

• Формирование различных подходов к необходимости получения согласия на использование полностью автоматизированных алгоритмов принятия решений в целях профилирования: в США и Китае возможен отказ от профилирования (возражение против применения решения) в случае, если возникают правовые или иные значимые для лица последствия, в то время как в Европейском Союзе по общему правилу необходимо получение согласия лица в случае, если имеют место соответствующие последствия. Представляется, что подход стран Европы более взвешенно обеспечивает баланс интересов сторон правоотношения, что обусловлено и иными основаниями для профилирования (например, в общественных интересах), которые в национальном законодательства США и Китая отсутствуют.

СПИСОК ЛИТЕРАТУРЫ

1. Ramadan R. A. Big Data Tools – An Overview / R. A. Ramadan // International Journal of Computer & Software Engineering. – 2017. – Vol. 2. – Art. 125. – DOI: 10.15344/2456-4451/2017/125.

2. Тесленко И. Б. Data = Большие данные : учеб. пособие / И. Б. Тесленко, А. М. Губернаторов, О. Б. Дигилина, В. Е. Крылов. – Владимир : Изд-во ВлГУ, 2021. – 123 с.

3. Profiling the European citizen: Cross-disciplinary perspectives / eds. M. Hildebrandt, S. Gutwirth. – Dordrecht : Springer, 2008. – 373 p. – DOI: 10.1007/978-1-4020-6914-7.

4. Бахтеев Д. В. Понятие и свойства криминалистического профилирования личности и поведения неизвестного преступника / Д. В. Бахтеев, И. В. Леднев // Юридическая наука и правоохранительная практика. – 2020. – № 3 (53). – С. 110–118.

5. Petherick W. Reframing criminal profiling: a guide for integrated practice / W. Petherick, N. Brooks // Psychiatry, Psychology and Law. – 2021. – Vol. 28, iss. 5. – P. 694–710. – DOI: 10.1080/13218719.2020.1837030.

6. Ilina T. Approaching to Digital Profiling in the Financial Market / T. Ilina // Journal of Corporate Finance Research. – 2020. – Vol. 14, iss. 4. – P. 47–60.

7. Виноградова Е. В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации / Е. В. Виноградова, Т. А. Полякова, А. В. Минбалеев // Правоприменение. – 2021. – Т. 5, № 4. – С. 5–19. – DOI: 10.52468/2542-1514.2021.5(4).5-19.

8. Жарова А. К. Парадигма цифрового профилирования деятельности человека: риски, угрозы, преступления : моногр. / А. К. Жарова, В. М. Елин, А. В. Минбалеев. – М. : РУСАЙНС, 2022. – 239 с.

9. Mendoza I. The Right Not to be Subject to Automated Decisions Based on Profiling / I. Mendoza, L. A. Bygrave // EU Internet Law / eds. T. E. Synodinou, P. Jougleux, C. Markou, T. Prastitou. – Cham : Springer, 2017. – P. 77–98. – DOI: 10.1007/978-3-319-64955-9_4.

10. Алимов Д. А. Трансформация идеи субъективных прав и свобод в условиях цифровой реальности / Д. А. Алимов // Права человека в условиях цифровой трансформации общества и государства : сб. ст. – Ростов н/Д. ; Таганрог : Изд-во Юж. федер. ун-та, 2021. – С. 9–11.

11. Меньшиков Я. С. Преимущества автоматического сбора данных в сети Интернет над ручным сбором данных / Я. С. Меньшиков // Universum: технические науки. – 2022. – № 10 (103). – URL: https://7universum.com/ru/tech/archive/item/14383.

12. Мочалов А. Н. Цифровой профиль: основные риски для конституционных прав человека в условиях неопределенности / А. Н. Мочалов // Lex russica. – 2021. – Т. 74, № 9. – С. 88–101. – DOI: 10.17803/1729-5920.2021.178.9.088-101.

13. Purificato E. User Modelling and User Profiling: a Comprehensive Survey : Preprint / E. Purificato. L. Boratto, E. W. De Luca. – February 21, 2024. – 71 p. – URL: https://arxiv.org/pdf/2402.09660.

14. Corte L. D. Scoping personal data: Towards a nuanced interpretation of the material scope of EU data protection law / L. D. Corte // European Journal of Law and Technology. – 2019. – Vol. 10, iss. 1. – URL: https://ejlt.org/index.php/ejlt/article/view/672.

15. Ferraris V. Defining Profiling : Working paper / V. Ferraris, F. Bosco, G. Cafiero, E. D'Angelo, Y. Suloyeva. – December 11, 2013. – 40 p. – DOI: 10.2139/ssrn.2366564.

16. Adnan M. Using Digital Traces for User Profiling: The Uncertainty of Identity Toolset / M. Adnan, L. Rosi, S. Veluru, M. Mouseli, P. A. Longley, M. Rajarajan // SIN '14 : The 7th International Conference on Security of Information and Networks. – New York : ACM, 2014. – P. 254–260. – DOI: 10.1145/2659651.2659741.

17. Петров А. А. Российская матрица цифрового профиля россиянина / А. А. Петров // Национальная ассоциация ученых. – 2020. – № 52. – С. 39–52. – DOI: 10.31618/nas.2413–5291.2020.1.52.144.

18. Мочалов А. Н. Прозрачность алгоритмов как правовой принцип автоматизированной обработки данных о человеке / А. Н. Мочалов // Юридические исследования. – 2023. – № 12. – С. 77–88. – DOI: 10.25136/2409-7136.2023.12.69452.

19. Barros Vale S. Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities / S. Barros Vale, G. Zanfir-Fortuna. – Future of Privacy Forum, 2022. – 60 p. – URL: https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf.

20. Foss-Solbrekk K. Searchlights across the black box: Trade secrecy versus access to information / K. Foss-Solbrekk // Computer Law & Security Review. – 2023. – Vol. 50. – Art. 105811. – DOI: 10.1016/j.clsr.2023.105811.

21. Malgieri G. Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations / G. Malgieri // Computer Law & Security Review. – 2019. – Vol. 35, iss. 5. – Art. 105327. – DOI: 10.1016/j.clsr.2019.05.002.

22. Право на доступ в Интернет, анонимность и идентификация пользователей (конституционно-правовые проблемы) / под. ред. М. С. Саликова. – Екатеринбург : Изд-во УМЦ УПИ, 2020. – 167 с.

23. Lee N. T. Police surveillance and facial recognition: Why data privacy is imperative for communities of color / N. T. Lee, C. Chin-Rothman // Brookings. – April 12, 2022. – URL: https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

24. Lin H. A Right to an Explanation of Algorithmic Decision-Making in China / H. Lin, H. Wu // Hong Kong Law Journal. – 2022. – Vol. 52, iss. 3. – P. 1163–1192.

25. Харитонова Ю. С. Правовые средства обеспечения принципа прозрачности искусственного интеллекта / Ю. С. Харитонова // Journal of Digital Technologies and Law. – 2023. – Т. 1, № 2. – С. 337–358. – DOI: 10.21202/jdtl.2023.14.

REFERENCES

1. Ramadan R.A. Big Data Tools – An Overview. *International Journal of Computer & Software Engineering*, 2017, vol. 2, art. 125. DOI: 10.15344/2456-4451/2017/125.

2. Teslenko I.B., Gubernatorov A.M., Digilina O.B., Krylov V.E. *Big Data*, Teaching aid. Vladimir, Vladimir State University named after Alexander and Nikolay Stoletovs publ., 2021. 123 p. (In Russ.).

3. Hildebrandt M., Gutwirth S. (eds.). *Profiling the European citizen: Cross-disciplinary perspectives*. Dordrecht, Springer Publ., 2008. 373 p. DOI: 10.1007/978-1-4020-6914-7.

4. Bakhteev D.V., Lednev I.V. The concept and characteristics of forensic profiling of the personality and behavior of an unknown offender. *Yuridicheskaya nauka i pravookhranitel’naya praktika = Legal Science and Law Enforcement Practice*, 2020, no. 3 (53), pp. 110–118. (In Russ.).

5. Petherick W., Brooks N. Reframing criminal profiling: a guide for integrated practice. *Psychiatry, Psychology and Law*, 2021, vol. 28, iss. 5, pp. 694–710. DOI: 10.1080/13218719.2020.1837030.

6. Ilina T. Approaching to Digital Profiling in the Financial Market. *Journal of Corporate Finance Research*, 2020, vol. 14, iss. 4, pp. 47–60.

7. Vinogradova E.V., Polyakova T.A., Minbaleev A.V. Digital profile: the concept, regulatory mechanisms and enforcement problems. *Pravoprimenenie = Law Enforcement Review*, 2021, vol. 5, iss. 4, pp. 5–19. DOI: 10.52468/2542-1514.2021.5(4).5-19.

8. Zharova A.K., Elin V.M., Minbaleev A.V. *The paradigm of digital profiling of human activity: risks, threats, crimes*, Monograph. Moscow, RUSAINS, 2022. 239 p. (In Russ.).

9. Mendoza I., Bygrave L.A. The Right Not to be Subject to Automated Decisions Based on Profiling, in: Synodinou T.E., Jougleux P., Markou C., Prastitou T. (eds.). *EU Internet Law*, Cham, Springer Publ., 2017, pp. 77–98. DOI: 10.1007/978-3-319-64955-9_4.

10. Alimov D.A. Transformation of the idea of subjective rights and freedoms in the conditions of digital reality, in: *Prava cheloveka v usloviyakh tsifrovoi transformatsii obshchestva i gosudarstva*, collected articles, Rostov-on-Don, Taganrog, Southern Federal University Publ., 2021, pp. 9–11. (In Russ.).

11. Menshikov Ya. Advantages of Automatic Data Collection in the Internet over Manual Data Collection. *Universum: tekhnicheskie nauki*, 2022, no. 10 (103), available at: https://7universum.com/ru/tech/archive/item/14383. (In Russ.).

12. Mochalov A.N. Digital Profile: Main Risks for Constitutional Human Rights in the face of Legal Uncertainty. *Lex Russica*, 2021, vol. 74, iss. 9, pp. 88–101. DOI: 10.17803/1729-5920.2021.178.9.088-101. (In Russ.).

13. Purificato E., Boratto L., De Luca E.W. *User Modelling and User Profiling: A Comprehensive Survey*, Preprint. February 21, 2024. 71 p. Available at: https://arxiv.org/pdf/2402.09660.

14. Corte L.D. Scoping personal data: Towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, 2019, vol. 10, iss. 1, available at: https://ejlt.org/index.php/ejlt/article/view/672.

15. Ferraris V., Bosco F., Cafiero G., D'Angelo E., Suloyeva Y. *Defining Profiling*, Working paper. December 11, 2013. 40 p. DOI: 10.2139/ssrn.2366564.

16. Adnan M., Rosi L., Veluru S., Mouseli M., Longley P.A., Rajarajan M. Using Digital Traces for User Profiling: The Uncertainty of Identity Toolset, in: *SIN '14*, The 7th International Conference on Security of Information and Networks, New York, ACM Publ., 2014, pp. 254–260. DOI: 10.1145/2659651.2659741.

17. Petrov A.A. Russian Matrix of the Digital Profile of the Russian. *Natsional'naya assotsiatsiya uchenykh*, 2020, no. 52, pp. 39–52. DOI: 10.31618/nas.2413-5291.2020.1.52.144. (In Russ.).

18. Mochalov A.N. Transparency of Algorithms as a Legal Principle of Automated Processing of Human Data. *Yuridicheskie issledovaniya*, 2023, no. 12, pp. 77–88. DOI: 10.25136/2409-7136.2023.12.69452. (In Russ.).

19. Barros Vale S., Zanfir-Fortuna G. *Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities*. Future of Privacy Forum Publ., 2022. 60 p. Available at: https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf.

20. Foss-Solbrekk K. Searchlights across the black box: Trade secrecy versus access to information. *Computer Law & Security Review*, 2023, vol. 50, art. 105811. DOI: 10.1016/j.clsr.2023.105811.

21. Malgieri G. Automated decision-making in the EU Member States: The right to explanation and other «suitable safeguards» in the national legislations. *Computer Law & Security Review*, 2019, vol. 35, iss. 5, art. 105327. DOI: 10.1016/j.clsr.2019.05.002.

22. Salikov M.S. (ed.). *The right to access the Internet, anonymity and identification of users (constitutional legal problems)*. Yekaterinburg, Ural Polytechnic Institute Publ., 2020. 167 p. (In Russ.).

23. Lee N.T., Chin-Rothman C. Police surveillance and facial recognition: Why data privacy is imperative for communities of color. *Brookings*, April 12, 2022, available at: https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

24. Lin H., Wu H. A Right to an Explanation of Algorithmic Decision-Making in China. *Hong Kong Law Journal*, 2022, vol. 52, iss. 3, pp. 1163–1192.

25. Kharitonova Yu.S. Legal Means of Providing the Principle of Transparency of the Artificial Intelligence. *Journal of Digital Technologies and Law*, 2023, vol. 1, iss. 2, pp. 337–358. DOI: 10.21202/jdtl.2023.14.

ISSN 2542-1514 (Print)

ИНФОРМАЦИЯ ОБ АВТОРЕ

Кузнецова Светлана Сергеевна – кандидат юридических наук, доцент, доцент кафедры конституционного права
Уральский государственный юридический университет имени В.Ф. Яковлева
620137, Россия, г. Екатеринбург, ул. Комсомольская, 21
E-mail: kss001@usla.ru
ORCID: 0000-0003-2426-8055
SPIN-код РИНЦ: 3387-9420; AuthorID: 804404

INFORMATION ABOUT AUTHOR

Svetlana S. Kuznetsova – PhD in Law, Associate Professor; Associate Professor, Department of Constitutional Law
Ural State Law University named after V.F. Yakovlev
21, Komsomol'skaya ul., Yekaterinburg, 620137, Russia
E-mail: kss001@usla.ru
ORCID: 0000-0003-2426-8055
RSCI SPIN-code: 3387-9420; AuthorID: 804404

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Кузнецова С.С. Правовое регулирование цифрового профилирования человека в практике зарубежных стран / С.С. Кузнецова // Правоприменение. – 2024. – Т. 8, № 4. – С. 63–72. – DOI: 10.52468/2542-1514.2024.8(4).63-72.

BIBLIOGRAPHIC DESCRIPTION

Kuznetsova S.S. Legal regulation of digital profiling of a person in the practice of foreign countries. *Pravoprimenenie = Law Enforcement Review*, 2024, vol. 8, no. 4, pp. 63–72. DOI: 10.52468/2542-1514.2024.8(4).63-72. (In Russ.).