

ОГРАНИЧЕНИЯ ПРАВА НА ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ПАНДЕМИИ COVID-19

А. А. Вербанович

Белорусский государственный университет, г. Минск;

verbanovichnastya@gmail.com;

науч. рук. – А. В. Талерёнок

Во время борьбы с кризисом в области здравоохранения главной задачей является сохранение человеческих жизней. Несомненно, такие исключительные условия, как пандемия, требуют немедленного реагирования со стороны государств, однако это не означает, что любые меры, предпринимаемые государствами в ходе борьбы с пандемией, оправданы. Кроме того, весьма трудно установить, будут ли принимаемые меры эффективны в ходе защиты общественного интереса, чем и объясняется актуальность исследования. В результате борьбы с COVID-19 усилия по сдерживанию распространения вируса привели к волне беспрецедентных в глобальном масштабе нарушений права на неприкосновенность частной жизни, в особенности, права на защиту персональных данных. Целью работы является рассмотрение правомерных ограничений права на защиту персональных данных в условиях пандемии. Для раскрытия цели в статье были проанализированы особенности обработки персональных данных о здоровье, а также особенности обработки метаданных.

Ключевые слова: право на неприкосновенность частной жизни; защита персональных данных; правомерные ограничения.

Государственные органы, работники здравоохранения в условиях пандемии в большом объеме обрабатывают данные, связанные со здоровьем человека. Такие данные относятся к особой категории [1, ст. 9 (1); 2] и имеют более высокий уровень защиты ввиду того, что их обработка представляет «значительный риск для основных прав и свобод человека» [3]. Данные о здоровье определяются как данные, относящиеся к физическому здоровью лица, а также данные об оказании медицинских услуг [1, ст. 4 (15)]. В контексте пандемии к таким данным относится информация о результатах тестирования на COVID-19, информация о симптомах, а также сведения о нахождении лиц на карантине [4].

Особая защита данных о здоровье выражается в том, что по общему правилу их обработка возможна только с согласия субъекта данных [1, ст. 9(2)(b)]. Однако из общих правил обработки существуют исключения: защита жизненно важных интересов [1, ст. 9 (2) (c)] и интересы общественного здравоохранения (*public health*) [5].

Защита жизненно важных интересов человека подразумевает действия, необходимые для сохранения его жизни или жизни третьих лиц [5]. Следовательно, обработка такой информации в ходе мониторинга эпидемии в целях спасения жизней других людей является оправданной.

Однако данное исключение применимо только в случае, если лицо не способно дать согласие [1, ст. 9 (2)].

Гораздо более гибким является второе исключение. Обработка данных о здоровье без согласия лица возможна в целях защиты общественного интереса в области здравоохранения [6], что подразумевает принятие мер, связанных с угрозой здоровью населения или отдельных лиц [7]. Таким образом, охрана общественного здоровья также может служить правовым основанием для сбора данных, необходимых для борьбы с эпидемией.

Намного сложнее определить правовые основания обработки метаданных в контексте пандемии. Опыт некоторых стран показывает, как массовый сбор данных может сократить распространение вируса [8]. Однако гарантируют ли подобные методы соблюдение прав человека?

Подход, который позволяет соблюдать права человека, основывается на анализе информации, с помощью которой можно установить, например, какое количество человек покидает город, в какое время, что позволяет учреждениям здравоохранения отслеживать скопления людей, прогнозировать географическое распространение заболевания и оценивать эффективность карантинных мер. Этот подход может быть квалифицирован как «макроуровневый», так как ориентирован на все население или на большие группы людей. В таком случае раскрывается анонимная информация, которая может обрабатываться без соблюдения основных принципов защиты данных [9].

«Микроуровневый» подход в гораздо меньшей степени гарантирует соблюдение прав человека. В этом случае государство контролирует каждого человека, отслеживая его перемещение и состояние здоровья. Такие страны, как Китай, Южная Корея, Тайвань, собирают широкий спектр личных данных для обеспечения эффективности мер общественного здравоохранения [4]. Несмотря на то, что сами по себе метаданные не раскрывают личность человека, их анализ может раскрыть весьма конфиденциальную информацию о личности [10, п. 15]. Следовательно, обработка метаданных должна подчиняться тем же правилам, что и обработка любых других персональных данных [12], ввиду чего обработчики данных должны указывать типы получаемых данных, цель обработки, обеспечивать сохранность данных, а также их удаление по достижении цели обработки.

Однако в ходе борьбы с COVID-19 эти правила не соблюдаются. Приложения, анализирующие симптомы пользователей, а также их местонахождение, в контексте COVID-19 действительно могут оказаться полезными. Посредством геолокации указывается, находился ли человек в тесном контакте с человеком с положительным результатом на

COVID-19. При обработке информации с помощью приложений правовой основой обработки является согласие субъекта данных [1, ст. 6 (1)(a)]. Однако их использование не всегда является добровольным. Граждане в некоторых странах должны установить приложение на свой смартфон и пройти обязательную процедуру персонализации с помощью их имени, номера телефона и национального идентификационного номера [8]. В таком случае согласие выражается субъектом несвободно, так как использование приложения является обязательным, и у пользователя нет возможности не указывать данные, позволяющие его идентифицировать.

Наиболее очевидным является нарушение принципов четкого определения цели и минимизации данных. Любая обработка персональных данных должна осуществляться для конкретной, четко определенной цели [1, ст. 5 (1)(b)]. Обработка персональных данных для неопределенных или неограниченных целей, а также для возможного, но не определенного последующего использования соответственно, нарушает права человека. Однако при сборе данных, если субъект об этом уведомлен, в основном указывается лишь достаточно размытая цель «приостановление распространения инфекции», в то время как о конкретных способах и методах обработки субъект не уведомляется [8].

Согласно принципу минимизации персональных данных информация должна обрабатываться в минимальном объеме, необходимом для достижения цели [1, ст. 5(1); 2, ст. 5(4)]. Необходимо устанавливать, как постоянный мониторинг местонахождения граждан, информация о продолжительности телефонных разговоров, а также о банковских транзакциях будет полезна в ходе борьбы с COVID-19. То есть необходимо установление существенной связи между систематической обработкой данных и заявленной целью предотвращения распространения эпидемии.

Одним из самых негативных последствий борьбы с пандемией может стать неограниченное хранение такой информации. Данные не должны храниться дольше, чем требуется для достижения цели, для которой они были собраны [1, ст. 5(1)(e)]. Однако приложения не предоставляют гарантии того, что данные будут удалены. Кроме того, трудно в принципе определить момент, в который такая цель, как «приостановление распространения инфекции», будет достигнута.

Таким образом, при использовании правомерных ограничений права на неприкосновенность частной жизни в качестве оснований обработки данных необходимо устанавливать баланс между общественными интересами в борьбе с эпидемией и уважением прав и свобод личности. Исключительные меры должны быть сбалансированы соответствующими

механизмами защиты. Следует учитывать, что правила защиты данных вовсе не являются препятствием для борьбы с вирусом. Наоборот, такие правила включают правомерные исключения, предназначенные для обработки необходимой информации, а также позволяющие при этом и избежать последствий несанкционированного использования персональных данных и соблюдать права человека.

Библиографические ссылки

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [Electronic resource]. – 2016. – Mode of access: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>. – Date of access: 03.05.2020
2. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Committee of Ministers, 17 May 2018 [Electronic resource]. – 2018. – Mode of access: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf. – Date of access: 03.05.2020
3. Recital 51 GDPR [Electronic resource]. – 2016. – Mode of access: <https://www.privacy-regulation.eu/en/recital-51-GDPR.htm>. – Date of access: 03.05.2020
4. Louis-Philippe Gratton, 'Contact tracing, Data Tracking, Coronavirus, and Law', 2.04.2020 [Electronic resource]. – 2020. – Mode of access: <https://www.linkedin.com/pulse/data-tracking-spread-coronavirus-law-louis-philippe-gratton/>. – Date of access: 03.05.2020
5. Recital 46 GDPR [Electronic resource]. – 2016. – Mode of access: <https://www.privacy-regulation.eu/en/recital-46-GDPR.htm>. – Date of access: 03.05.2020
6. Recital 54 GDPR [Electronic resource]. – 2016. – Mode of access: <https://www.privacy-regulation.eu/en/recital-54-GDPR.htm>. – Date of access: 03.05.2020
7. Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights Annex, UN Doc E/CN.4/1984/4 [Electronic resource]. – 2016. – Mode of access: <https://www.uio.no/studier/emner/jus/humanrights/HUMR5503/h09/undervisningsmateriale/SiracusaPrinciples.pdf>. – Date of access: 03.05.2020
8. Privacy International, 'Covid-19 response: overview of data and technology' [Electronic resource]. – 2020. – Mode of access: <https://privacyinternational.org/news?page=1>. – Date of access: 03.05.2020
9. Recital 26 GDPR [Electronic resource]. – 2016. – Mode of access: <https://www.privacy-regulation.eu/en/recital-26-GDPR.htm>. – Date of access: 03.05.2020
10. UNHRC 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', 17 April 2013, UN Doc A/HRC/23/40 [Electronic resource]. – 2013. – Mode of access: https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf. – Date of access: 01.05.2020