УДК 004.056:341(4)(075.8)

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЕВРОПЕЙСКОМ СОЮЗЕ: СУЩНОСТНО-СОДЕРЖАТЕЛЬНЫЕ АСПЕКТЫ

Н.В. Валюшко-Орса

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

В статье рассмотрены сущностно-содержательные аспекты правового регулирования защиты персональных данных в Европейском союзе. Отмечается, что положительный опыт Европейского союза по правовому регулированию защиты персональных данных оказал определенное влияние на развитие законодательства в этой сфере в Республике Беларусь.

***Ключевые слова*:** персональные данные, защита персональных данных, согласие субъекта данных, Европейский союз.

LEGAL REGULATION OF PERSONAL DATA PROTECTION IN THE EUROPEAN UNION: ESSENTIAL AND CONTENT ASPECTS

N.V. Valyushko-Orsa

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The article considers the essential and substantive aspects of the legal regulation of the protection of personal data in the European Union. It is noted that the positive experience of the European Union on the legal regulation of the protection of personal data had a certain impact on the development of legislation in this area in the Republic of Belarus.

Keywords: personal data, protection of personal data, consent of the data subject, European Union.

На современном этапе, ввиду активного развития информационно-коммуникационных технологий, весьма актуальным является вопрос, касающийся защиты персональных данных индивидуума. В частности, в связи наличием глобальной компьютерной сети Интернет, имеется возможность свободного доступа практически к любой информации. Кроме того, существование различных автоматизированных баз данных помогает более оперативно разрабатывать и принимать решения на разных уровнях, в том числе, в процессе осуществления государственного управления. Однако,

при даче лицом согласия на обработку своих персональных данных в глобальной компьютерной сети Интернет различными субъектами (например, органами государственной власти, предприятиями, учреждениями и иными организациями), возникает риск завладения названными данными сторонними лицами, что, в свою очередь, может повлечь за собой нарушение конституционного права на неприкосновенность частной жизни.

Следует отметить, что право на неприкосновенность частной жизни, в том числе, включает в себя право на защиту персональных данных.

В частности, согласно ст. 12 Всеобщей декларации прав человека от 10 декабря 1948 года «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств» [1, с. 2]. Подобного рода норма закреплена в ст. 8 Конвенции о защите прав человека и основных свобод от 4 ноября 1950 г., согласно которой «каждый человек имеет право на уважение его личной и семейной жизни, неприкосновенности его жилища и тайны корреспонденции» [2, с. 763].

Обратим внимание на то, что основным законодательством Европейского союза в сфере защиты персональных данных являются:

- Регламент Европейского парламента и Совета Европейского союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных (GDPR)) (далее – Общий регламент) [3];

- Регламент 2018/1725 Европейского парламента и Совета Европейского союза от 23 октября 2018 г. о защите физических лиц при обработке персональных данных институтами, органами, учреждениями и агентствами Союза и о свободном перемещении таких данных и отмене Регламента (ЕС) № 45/2001 и Решения № 1247/2002/ЕС (далее – Регламент 2018/1725) [4];

- Директива 2002/58/ЕС Европейского парламента и Совета Европейского союза от 12 июля 2002 г. об обработке персональных данных и защите конфиденциальности в секторе электронных коммуникаций (Директива о конфиденциальности и электронных коммуникациях) (далее – Директива 2002/58) [5];

- Директива 2016/680 Европейского парламента и Совета Европейского союза от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных компетентными органами в целях предотвращения, расследования, выявления или уголовного преследования или исполнения

уголовных наказаний, а также о свободном перемещении таких данных и отмене Рамочного решения Совета 2008/977/JHA (далее – Директива 2016/680) [6];

Одним из важных вопросов является понимание того, как трактуется дефиниция «персональные данные» в соответствии с законодательством Европейского союза, поскольку от того, насколько точно будет дано определение персональным данным, зависит и то, на что будет направлена защита по отношению к субъекту персональных данных.

Принципы и правила защиты физических лиц в отношении обработки их персональных данных должны, независимо от их гражданства или места жительства, уважать их основные права и свободы, в частности их право на защиту персональных данных. Общий регламент призван способствовать формированию пространства свободы, безопасности и правосудия и экономического союза, экономическому и социальному прогрессу, укреплению и сближению экономик в рамках внутреннего рынка, а также содействовать благосостоянию физических лиц [3, п. 2].

Согласно ст. 4 Общего регламента под персональными данными понимается любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъект данных») [3]. Такой подход к трактовке понятия «персональные данные» является оправданным, поскольку определение названной дефиниции, например, через установление закрытого перечня персональных данных, приведет к возникновению правовой неопределенности в связи с постоянным развитием информационных технологий и появлением новых способов идентификации лиц [7].

Положительный опыт Европейского союза, касающийся правового регулирования защиты персональных данных, оказал определенное влияние на развитие законодательства в этой сфере в Республике Беларусь. В частности, 7 мая 2021 г. был принят Закон Республики Беларусь «О защите персональных данных» [8] в соответствии с которым дано новое определение понятию «персональные данные». Так, согласно ст. 1 Закона Республики Беларусь от 7 мая 2021 г. «О защите персональных данных» под персональными данными понимается любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано [8]. Данное определение по сути является идентичным определению, которое дано в ст. 4 Общего регламента. Таким образом, понятие «персональные данные», согласно Закону Республики Беларусь от 7 мая 2021 г. «О защите персональных данных», стало толковаться шире, что, в свою очередь, свидетельствует о том, что объем информации, который можно отнести к персональным данным также стал значительно шире, по сравнению с предыдущим определением персональных данных.

Следует отметить, что Общий регламент вводит различного рода понятия, например, такие ка «контролер данных», «обработчик», «получатель», «третье лицо».

Кроме того, следует сделать акцент на такое понятие как «согласие» субъекта данных. Согласно ст. 4 Общего регламента под согласием субъекта данных понимается добровольное, конкретное, информированное и однозначное волеизъявление, в котором субъект данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих персональных данных [3].

Далее, обратим внимание на то, что Общий регламент имеет прямое действие по отношению к государствам-членам Европейского союза. Однако, согласно, п. 1 ст. 8 Общего регламента государства-члены Европейского союза могут установить более низкий возраст на дачу согласия по обработке персональных данных, но не ниже 13 лет, по сравнению с тем возрастом, который установлен в п. 1 ст. 8 Общего регламента (ребенок может дать согласие на обработку своих персональных данных с 16 лет, но если ребенок еще не достиг 16-го возраста, то такая обработка будет являться законной только когда согласие было дано лицом, обладающим родительскими правами в отношении ребенка, или было дано с его одобрения) [3].

Нижний возрастной порог (до 13 лет) на дачу согласия по обработке персональных данных несовершеннолетнего установлен и в п. 1 ст. 8 Регламента 2018/1725 [4].

На практике, предоставленная Общим регламентом возможность государствам-членам Европейского союза самостоятельно определять возраст ребенка при даче согласия им на обработку своих персональных данных, вызвала определенные проблемы [9].

По данным Европейской комиссии, только в девяти государствах Европейского союза (Венгрии, Германии, Ирландии, Люксембурге, Нидерландах, Польше, Румынии, Словакии и Хорватии) власти решили придерживаться установленного Общим регламентом возрастного порога: до достижения лицом 16 лет создание аккаунта и последующая обработка персональных данных ребенка допускается лишь с согласия родителей [9].

В других странах Европейского союза возраст на дачу согласия ребенком на обработку своих персональных данных, понижен до 13 лет, например, в Бельгии, Дании, Латвии, на Мальте, в Швеции, Финляндии, Эстонии; до 14 лет – в Австрии, Болгарии, Испании, Италии, на Кипре и в Литве и до 15 лет – в Чехии, Франции [9].

Существующая разница в возрасте согласия влечет неопределенность относительно прав детей на защиту персональных данных. «Это также создает проблемы для компаний с трансграничным бизнесом и тех, что разрабатывают технологические решения в сфере кибербезопасности» [9].

Следует отметить, что дети нуждаются в особой защите своих персональных данных, так как они в меньшей степени осознают риски, последствия, гарантии и права при обработке своих персональных данных. Такого рода особая защита должна применяться при использовании персональных данных детей в целях маркетинга, при создании личного профиля или профиля пользователя, а также при реализации услуг, предлагаемых непосредственно ребенку. Согласие лиц, которые несут родительскую ответственность, не требуется при профилактических и консультационных услугах, которые предлагаются непосредственно ребенку [3, п. 38].

В отчете Европейской комиссии было обращено внимание на то, что «для эффективного функционирования внутреннего рынка и чтобы избежать ненужной нагрузки на компании, важно, чтобы национальное законодательство не выходило за рамки, установленные GDPR, и не вводило дополнительных требований» [9]. По нашему мнению, такой подход является оправданным, ввиду стремления Европейского союза к гармонизации законодательства с его государствами-членами.

Кроме того, в п. 8 Директивы 2002/58 определено, что правовые, нормативные и технические положения, принятые государствами-членами в отношении защиты персональных данных, конфиденциальности и законных интересов юридических лиц в секторе электронных коммуникаций, должны быть гармонизированы, чтобы избежать препятствий для внутреннего рынка электронных коммуникаций. Гармонизация должна быть ограничена требованиями, необходимыми для гарантии того, что продвижение и развитие новых услуг и сетей электронных коммуникаций между государствами-членами не будет затруднено [5].

Далее, следует обратить внимание на Директиву 2016/680. Согласно п. 1 ст. 1 данная Директива устанавливает правила, касающиеся защиты физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, выявления или уголовного преследования или исполнения уголовных наказаний, включая защиту и от предотвращения угроз общественной безопасности [6].

В соответствии с Директивой 2016/680 государства-члены должны:

- защищать основные права и свободы физических лиц и, в частности, их право на защиту персональных данных;

- обеспечить, чтобы обмен персональными данными компетентными органами в рамках Европейского союза, если такой обмен требуется законодательством Европейского союза или государства-члена, не ограничивался и не запрещался по причинам, связанным с защитой физических лиц в отношении обработки персональных данных (п. 2 ст. 1) [6].

В целях обеспечения безопасности и предотвращения обработки, нарушающей Директиву 2016/680, контролер или обработчик должны оценить

риски, связанные с обработкой персональных данных, и должны принять меры для снижения этих рисков, такие как шифрование. Данные меры должны обеспечивать надлежащий уровень безопасности, включая конфиденциальность, и учитывать уровень техники, затраты на внедрение в зависимости от риска и характера защищаемых персональных данных. При оценке рисков безопасности данных следует учитывать риски, связанные с обработкой данных, такие как случайное или незаконное уничтожение, потеря, изменение или несанкционированное раскрытие или доступ к передаваемым, хранящимся или иным образом обрабатываемым персональным данным, которые могут, в частности, привести к физическому, материальному или нематериальному ущербу. Контролер и обработчик должны обеспечить, чтобы обработка персональных данных не осуществлялась неуполномоченными лицами [6, п. 60].

В общей сложности в процессе становления и развития законодательства о защите персональных данных в Европейском союзе «стало очевидным, что потребуется внедрение новых способов защиты данных таких, как профилирование и псевдонимизация, так как современная глобализация обусловливает активное развитие и совершенствование информационных технологий, стирание границ передачи данных, использование новых типов персональных данных (например, биометрических, генетических) и автоматизированных систем обработки» [10].

Таким образом, правовое регулирование защиты персональных данных в Европейском союзе достаточно развито, а Общий регламент является основополагающим законодательным актом, который, в свою очередь, направлен на унификацию защиты персональных данных в государствах-членах Европейского союза.

Библиографический список

1. Всеобщая декларация прав человека: принята резолюцией 217 А (III) Генер. Ассамблеи ООН, 10 дек. 1948 г. // Права человека: сб. междунар.-правовых док. / сост. В.В. Щербов. – Минск: Белфранс, 1999. – С. 1–5.

2. Конвенция о защите прав человека и основных свобод: совершено г. Рим, 4 нояб. 1950 г. // Права человека: сб. междунар.-правовых док. / сост. В.В. Щербов. – Минск: Белфранс, 1999. – С. 761–772.

3. 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [Electronic resource] // EUR-Lex. – Mode of access: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679. – Date of access: 31.05.2022.

4. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such

data, and repealing Regulation (EC) № 45/2001 and Decision № 1247/2002/EC [Electronic resource] // EUR-Lex. – Mode of access: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725. – Date of access: 31.05.2022.

5. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [Electronic resource] // EUR-Lex. – Mode of access: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058. Date of access: 31.05.2022.

6. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision [Electronic resource] // EUR-Lex. – Mode of access: 2008/977/JHA https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680. – Date of access: 31.05.2022.

7. Gabel, D., Hickman, T. The International Comparative Legal Guide to: Data Protection [Electronic resource] / D. Gabel, T. Hickman. – 6th Edition. – 2019. – Mode of access: https://by1lib.org/book/5631910/353f79?id=5631910&secret=353f79. – Date of access: 11.04.2022.

8. О защите персональных данных : Закон Респ. Беларусь, 7 мая 2021 г., № 99-З // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

9. Как ЕС реализует обязательства по внедрению GDPR [Электронный ресурс] // RSpectr.com. – Режим доступа: https://rspectr.com/articles/kak-es-realizuet-obyazatelstva-po-vnedreniyu-gdpr. – Дата доступа: 31.05.2022.

10. Шадрин, С.А. Правовое регулирование защиты персональных данных в Европейском Союзе: генезис и перспективы развития: дис. … канд. юрид. наук: 12.00.10 [Электронный ресурс] / С.А. Шадрин; ФГАОУ ВО «Казанский (Приволжский) федеральный университет» // disserCat – электронная библиотека диссертаций. – 2019. – Режим доступа: https://www.dissercat.com/content/pravovoe-regulirovanie-zashchity-personalnykh-dannykh-v-evropeiskom-soyuze-genezis-i-perspek**.** – Дата доступа: 01.06.2022.