УДК 341.1/8

ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ В ТРЕТЬИ СТРАНЫ И ЭКСТЕРРИТОРИАЛЬНОЕ ДЕЙСТВИЕ АКТОВ ЕВРОПЕЙСКОГО СОЮЗА О ЗАЩИТЕ ДАННЫХ

Омирзакова Диана Ахметовна

4622

Магистрант 2-го курса кафедры Международного права программы двойного диплома Евразийского национального университета им. Л.Н. Гумилева (Казахстан) и Московского государственного института международных отношений (Университет) МИД России (Россия)
Научный руководитель – Ш.В. Тлепина, д.ю.н., профессор

Как отмечает The Economist данные стали играть ту же роль что и нефть. Передвижение данных создало новую инфраструктуру, новую сферу для бизнеса, новую монополию, новую политику и в конечном итоге новую экономику. Цифровая информация не похожа ни на один классических ресурсов, она может быть извлечена, куплена, продана различными способами. Это меняет правила для рынков и требует новых подходов от регуляторов. [1] Международные потоки данных вызывают большую озабоченность в связи с тем, что обеспечение функционирования систем связи, здравоохранения, образования, розничной торговли, финансовых услуг приводят к сбору данных. Такие данные в связи с безграничностью интернет пространства могут быть переданы третьим лицам в других юрисдикциях, которые могут не предоставлять адекватный уровень защиты конфиденциальности частных лиц. Учитывая возможности которые открывает цифровой рынок и риски нарушения прав индивидов, в частности на неприкосновенность частной жизни, персональных данных Европейские институты обращают особое внимание на обеспечение защиты персональных данных индивидов без ущерба экономическим интересам интеграционных процессов.

Транснациональные вопросы защиты персональных данных с точки зрения Европейского союза (далее − ЕС) могут рассматриваться с двух позиций. Первое – это экстерриториальное действие системы защиты персональных данных ЕС. Второе – передача персональных данных в третьи страны.

В 2018 году в ЕС вступил в силу самый современный правовой режим защиты данных в мире, Регламент 2016/679 (далее − Регламент) о защите частных лиц в отношении автоматизированной обработки персональных данных и свободы передвижения таких данных, акт унификации права ЕС, который заменил ранее действовавшую Директиву о 95/46/ЕС «О защите физических лиц применительно к обработке персональных данных и свободном передвижении таких данных» и установил единые требования к защите данных, не допускающие отступления. Теперь Регламент распространяет свое действие в отношении всех компаний обрабатывающих персональные данные резидентов ЕС вне зависимости от местонахождения компании и места обработки данных, что служит подтверждением экстерриториального действия актов ЕС по защите данных. [2]

В соответствии с Регламентом персональные данные могут передаваться за рамки ЕС только в ограниченных случаях − если третья страна обеспечивает адекватный уровень защиты персональных данных.

Новшеством, введенным Регламентом является возможность правомерной передачи данных без установления адектватности уровня защиты: это принять Обязательные корпоративные правила (ст.47) или использовать Стандартные договорные оговорки (ст.46) либо использовать утвержденные правила поведения (ст.40), которые являются механизмами разрешающими передачу данных. Также возможно принятие режим конфиденциальности, уровень защиты которого эквивалентен уровню защиты, который гарантируется в ЕС. Новый регламент оказывает серьезное влияние на торговлю, которая зависит от передвижения данных, в связи с чем, перед развивающимися странами стоит задача: либо принять национальные законы о защите данных такого же содержания как и в ЕС либо их компании должны будут нести транзакционные издержки при использовании Обязательных корпоративных правил и Стандартных договорных оговорок. [3] ЕС оказывает значительное влияние по вопросам защиты персональных данных, так как многие государства для того, чтобы соответствовать требованиям адекватности уровня защиты данных Европейской Комиссии (далее - Комиссия), принимают свои национальные законы о защите данных на основе требований законодательства ЕС. В этой связи можно отметить позицию многих авторов, которые утверждают, что Регламент может быть признан не только региональным правовым актом по защите персональных данных, но и международным стандартом защиты персональных данных. [4] Таким образом, ЕС может косвенно воздействовать на интернет таргетинг и призывать к соблюдению норм об обработке данных ЕС вне зависимости от места происхождения сайта, тем самым укреплять экстерриториальное действие Регламента. [5] Согласно другой позиции, например, позиции Кунера К., глобальная конвергенция регулирования защиты персональных данных вокруг стандартов Регламента маловероятна [6], так как концепция ЕС в отношении неприкосновенности частной жизни в качестве фундаментального права закрепленного в Хартии ЕС об основных правах, является продуктом истории и культурной траектории ЕС, которую не разделяют многие страны. [3]

Тем не менее, в отчете Комиссии о применении Хартии ЕС об основных правах за 2017 год отмечается, что наряду с усилением защиты посредством принятия пакета реформ по защите данных, Комиссия также стремиться обеспечить высокий уровень защиты данных на международном уровне в контексте глобального информационного общества. [7]

Конвергенция регулирующих механизмов по примеру стандартов и прав закрепленных в Регламенте также может быть нежелательно по экономическим соображениям, особенно в отношении развивающихся стран. Регламент отражает баланс между неприкосновенностью частной жизни, экономикой и возможностями торговли от перемещения данных, что может не быть оптимальным для развивающихся стран. Принятие стандартов, закрепленных в Регламенте, вероятно, уменьшит сферу применения персональных данных во внутренних рынках услуг, и уменьшит

конкурентоспособность цифрового экспорта на рынки третьих стран, считает Мато А. [3]

Регламент не ограничивает полностью трансграничную передачу данных, однако все еще продолжает политику ограничения, предусмотренной Директивой о защите данных. В частности персональные данные не могут быть переданы за рамки Европейского Экономического пространства если законы в других юрисдикциях не обеспечивают адекватный уровень защиты. Между тем, в Регламенте подчеркивается, что в рамках Союза свобода передвижения персональных данных не может быть ограничена или запрещена в связи с обработкой персональных данных. Требование об адекватности уровня защиты было закреплено в статье 25 Директивы о защите данных в качестве одного из основных принципов передачи данных в третьи страны. С принятием Регламента в статье 46 уточняется, что персональные данные могут передаваться не только в третьи страны, но и международным организациям. Передача персональных данных в третьи страны и международные организации имеет место только в том случае если Комиссия примет решение о том, что третьей страной, регионом третьей страны или международной организацией обеспечивается адекватный уровень защиты и такая передача не нуждается в специальном разрешении. В соответствии со ст.45 Регламента, при определении адекватности уровня защиты, Комиссия принимает во внимание несколько элементов: 1) норму закона, уважение прав человека и основных свобод, соответствующие законы, включая законы касающиеся общественной, национальной безопасности, уголовное законодательство, доступ публичных властей к персональным данным, также как и применение данного законодательства, норм о защите персональных данных и мер безопасности, включая уже осуществляющуюся передачу персональных данных в третьи страны и международные организации, судебную практику, обеспечение прав субъекта персональных данных, административное и судебное восстановление прав субъекта персональных данных, чьи данные были переданы; 2) существование и эффективное функционирование одного или более независимых надзорных органов в третьих странах или международных организациях, с возможностью обеспечения и приведения в соответствие с нормами о защите данных, включая наличие соответствующих полномочий по принуждению исполнения, оказанию помощи и предложению рекомендаций субъектам данных по осуществлениюс своих прав и сотрудничества с надзорными органами государств-членов; 3) международные обязательства которые взяли на себя третьи страны и международные организации или другие обязательства, возникшие из юридически обязательных конвенций или других документов, также как и из участия в многосторонних либо региональных системах, связанные с защитой персональных данных. После изучения адекватности уровня защиты Комиссия принимает имплементирующий акт, который должен предусматривать механизм пересмотра адекватности уровня защиты

как минимум каждые четыре года. Комиссия периодически проводит мониторинг изменений в отношении защиты персональных данных в третьих странах и международных организациях. Если третья страна или международная организация более не обеспечивают адекватный уровень защиты, то в таком случае Комиссия отменяет, вносит изменения либо приостанавливает действие принятого имплементирующего акта который не имеет обратного действия. [2]

Комиссия установила, что в Андоре [9], Аргентине [10], Канаде [11], Фарерских островах [12], Израйле [13], Японии, Острове Мэн [14], Новой Зеландии [15], Швейцарии [16], Уругваях, США (в рамках Privacy Shielt) обеспечивается адекватный уровень защиты. В настоящее время ведутся переговоры с Северной Кореей.

Примером экстерриториального действия актов ЕС по защите данных являются такие дела как C-131/12 Google Spain [20] и C-362/14 Max Schrems [21]. В деле Max Schrems, заявитель с 2008 года использовавший социальную сеть Facebook подал жалобу на Уполномоченного по защите данных Ирландии в связи с передачей его данных от ирландских серверов Facebook США связанные с раскрытием Едвардом Сноуденом деятельности американских служб. В жалобе заявитель утверждал, что в данном случае не было соблюдено требование актов ЕС об обеспечении адекватного уровня защиты. Передача была осуществлена на основании решения Комиссии, которая посчитала, что США обеспечивает адекватный уровень защиты. Ирландское агентство по защите данных отклонило заявление основываясь на том, что адекватный уровень защиты обеспечивается соглашением «О безопасной гавани» между ЕС и США. Дело рассматривалось высоким судом Ирландии и соответственно было передано на рассмотрение Суда ЕС. Суд ЕС в своем решении признал недействительным решение Комиссии, так как перед тем как принять решение об адекватности уровня защиты, предполагается, что Комиссия должна подтвердить, что национальное законодательство третьей страны или его международные обязательства обеспечивают право на защиту персональных данных на уровне эквивалентном уровню защиты Директивы о защите данных и Хартии ЕС об основных правах. Европейская Комиссия приняла решение, основываясь на Соглашении «О безопасной гавани» не изучив правовых основ национального законодательства США. Соглашение о безопасной гавани не вмешивается и не исключает компетенцию национальных органов по защите данных в отношении Директивы о защите данных и Хартии ЕС об основных правах. [22]

Таким образом через призму права ЕС можно проследить два подхода в отношении передачи персональных данных в третьи страны, первый заключается в необходимости обеспечения, фундаментального для ЕС, права на защиту персональных данных. Второй подход – это необходимость обеспечения свободы передвижения данных, ограничение которых может негативно сказаться на развитии торговли и экономики. Важно отметить

экстерриториальное действие актов ЕС, которые косвенным образом могут менять систему защиты персональных данных в связи с отсутствием других аналогов правовой защиты персональных данных на международном уровне, что является свидетельством неодинакового обеспечения права человека на защиту данных на международном и региональном уровнях.

Список использованных источников:

1. The Economist. Data is giving rise to a new economy. // URL: https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy (дата обращения 10.03.2019)
2. 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) // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 (дата обращения 11.03.2019)
3. Mattoo A. and Meltzer P.J. International Data Flows and Privacy: The Conflict and its Resolution. Journal of International Economic Law. Oxford. no.21 (2018). – p. 770.
4. Bu-Pasha S. Cross-border issues under EU data protection law with regards to personal data protection. Information & Communications Technology Law. Taylor&Francis Group. DOI: 10.1080/13600834.2017.1330740. – p.6.
5. Paul D.H. & Papakonstantinou V. Three Scenarios for international Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? // I/S: A Journal of Law and Policy for the Information Society, vol. 9, no. 2 (2013). – p. 313.
6. Christopher K., 'Reality and Illusion in EU Data Transfer Regulation Post Schrems',German Law Journal 18 (04) (2017), at 881.
7. Доклад Комиссии о применении Хартии ЕС об основных правах за 2017 год // URL: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/application-charter/annual-reports-application-charter_en − С. 48.
8. Commission Decision of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra. *OJ L 277, 21.10.2010, p. 27–29*
9. Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina. *OJ L 168, 5.7.2003, p. 19–22*
10. Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act. *OJ L 2, 4.1.2002, p. 13–16*

11. Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data. *OJ L 58, 9.3.2010, p. 17–19*
12. Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data. *OJ L 27, 1.2.2011, p. 39–42*
13. Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man. *OJ L 151, 30.4.2004, p. 48–51*
14. Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand. *OJ L 28, 30.1.2013, p. 12–14*
15. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland. *OJ L 215, 25.8.2000, p. 1–3*
16. Решение Большой Палаты Суда ЕС от 13 мая 2014 года по делу «Гугл против Испании» // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (дата обращения 15.03.2019)
17. Решение Большой Палаты Суда ЕС от 6 октября 2015 года по делу «Шремс» // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 (дата обращения 15.03.2019)
18. Martin A. Weiss and Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield' (Congressional Research Service, 19 May 2016) – p.7.