DOI 10.69085/PSC2025224

ТРАНСФЕРЪТ НА ДАННИ В РАМКИТЕ НА ЕС И КЪМ ТРЕТИ СТРАНИ

Жанин Ал-Шаргаби и Никола Учкунов, студенти
Софийски университет, България

***Резюме**: Защитата на лични данни се отличава като една от най-актуалните теми през последното десетилетие. Проблемът с тяхната обработка и трансфер е многопластов, а защитата им представлява не само задължение на държавите, които следва да опазват основните права на своите граждани, но и изисква по-обстоен преглед на задълженията, които се вменяват на частния сектор. Ако през последните години се е обособила относителна яснота относно практиките на национално и европейско ниво, то все още стои отворен въпросът с трансфера на данни с трети страни. Тази разработка си поставя за цел да разгледа приложимите стандарти за защита на данни на европейско ниво, както и практиката относно трансфера на данни в трети страни. Все още съществува притеснението дали други юрисдикции с тесни икономически отношения с Европа, като САЩ, Китай и т.н., имат достатъчно стриктен режим за защита на личната информация на потребители. Как следва да постъпи тогава един администратор на данни, когато, за да предостави услугата си, трябва да прехвърля данни на свои партньори в трета страна? Какви скрити рискове крият новите технологии, като например облачните услуги, когато не можем да проследим изцяло преноса на данни? Тази разработка ще разгледа тези и други релевантни въпроси. Не на последно място, като стъпи на съществуващи законодателни инициативи, ще предложи и стандарт за защита на данните при трансфер към трети страни.*

***Ключови думи**: трансфер на данни, лични данни, облачни услуги, трети страни, стандарти за защита на личните данни, основни права*

DATA TRANSFER IN THE EU AND TOWARDS THIRD COUNTRIES

Students Zhanin Al-Shargabi and Nikola Uchkunov
Sofia University, Bulgaria

***Abstract**: The protection of personal data stands out as one of the most pressing topics of the last decade. The issue of its processing and transfer is multifaceted, and protecting personal data is not only the responsibility of states, which must safeguard the fundamental rights of their citizens, but also requires a more comprehensive review*

of the obligations imposed on the private sector. While relative clarity has emerged in recent years regarding practices at the national and European levels, the issue of data transfers to third countries is still open. This paper aims to examine the applicable data protection standards at European level, as well as the practices concerning data transfers to third countries. There is ongoing concern about whether other jurisdictions with close economic relations with Europe, such as the US, China, Saudi Arabia, etc., maintain sufficiently strict regimes to protect users' personal information. How, then, should a data controller proceed when transferring data to partners in a third country to provide service? What are the hidden risks associated with new technologies, such as cloud services, where data transfers may not be fully traceable? This paper will address these and other relevant questions. Last but not least, building on existing legislative initiatives, the paper will also propose a standard for data protection in transfers to third countries.

Key words: *data transfer, personal data, cloud services, third parties, data protection standards, fundamental rights*

I. Въведение

С приемането на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (ОРЗД), осъзнатостта ни към проблемите, свързани с неприкосновеността на личните данни, нараства все повече и повече. Ако преди обществеността не е разбирала начините, по които техните данни биват събирани и използвани, то в днешно време потребителите са по-склонни да прочитат за какво се ползват данните им, да проверяват до каква степен се споделят и да използват правата си, като правото да бъдат забравени или да бъдат подновявани събраните данни за тях.[1]

В същото време обаче технологии, които са станали неразделна част от ежедневието ни, продължават да търпят промени и подобрения, които може дори да не сме очаквали. Това от своя страна носи нови рискове относно защитата на личните данни с оглед на това, че някои нови видове технологии(например облачните услуги) не предоставят достатъчно прозрачност по отношение на това къде отиват данните на дадено лице, доколко са достъпни и доколко са защитени.[2]

[1] Goswami, S. The Rising Concern Around Consumer Data And Privacy, Forbes, 14 December 2020, updated on 14 April 2022 (https://www.forbes.com/councils/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/).

[2] Mahmood, Z. Data Location and Security Issues in Cloud Computing. – Emerging Intelligent Data and Web Technologies (EIDWT), 2011.

От друга страна, икономическите отношения и цялостната бизнес обстановка също търпят съществени промени. Ако преди години Европа и САЩ са били неимоверни лидери и са диктували както търговските практики и отношения, така и правните стандарти, то стремглавият възход на някои източни държави започва да променя тези закономерности. Досега Европейският съюз (ЕС) се радваше на относителна правна хегемония, т.нар. „Брюкселски ефект" описва закономерността, при която правните стандарти, приети в рамките на вътрешния пазар на ЕС, се приемат и от други юрисдикции, за да се постигне съответствие и да могат бизнесите от трети страни да се радват на безпроблемен достъп до привлекателните европейския пазари.[3] Сега обаче се забелязва нарастващо влияние на чужди правни култури и подходи. Силно бюрократизираната система в Европа изглежда оказва влияние на конкурентоспособността и цялостното икономическо развитие на страните членки на ЕС – техните бизнеси вече не са световни лидери, а се опитват да догонят достиженията на другите континенти.[4] Това поставя релевантния въпрос дали останалият свят ще продължи да търси одобрението на ЕС и да се съобразява с неговите строги изисквания, или може да станем наблюдатели на промяна в бизнес мисленето – промяна, която неимоверно би могла да измени и правната ни култура. Ако държави като САЩ, Китай, Саудитска Арабия и т.н. решат да не спазват същите стандарти като Европа относно защитата на лични данни, ще може ли Съюзът да ограничи търговските си отношения с тях или вече няма същата сила и влияние?

Основен въпрос тук е признаването на нивото на защита на личните данни в трети страни и как е регулиран обменът на данни? Досега ЕС е установил определени стандарти и механизми за защита при обмена на лични данни с трети страни. Болезнен пример от последното десетилетие обаче са неуспешните опити да се регулира обменът на данни между САЩ и Европа на институционално ниво. Неуспешният диалог между двете водещи икономически сили и несигурността какво следва напред крият различни рискове. На първо място, следва да се запитаме дали Съюзът, в стремежа си да защити основните права на своите граждани и да запази високите си стандарти относно неприкосновеността на лични данни, не задава нереалистични очаквания

[3] Bradford, A. The Brussels Effect: How the European Union Rules the World. Oxford, Oxford University Press, 2020.

[4] Hannon, P. & Y Hayashi, Europe's Stagnating Economy Falls Further Behind the U.S. – New York Times, 30 January 2024, (https://www.wsj.com/economy/global/europes-stagnating-economy-falls-further-behind-the-u-s-1cc58ba1?msockid=05b7e13f91c86df60d47f466906e6c50).

и по този начин не се изолира от реална ползотворна кооперация с други юрисдикции. На второ място, тези неуспехи може би вещаят нарастваща тенденция трети страни да отказват да се съобразяват с европейските изисквания. Това ще постави под въпрос възможността на Съюза да поддържа лидерската си позиция по въпросите за неприкосновеността на данните.

Настоящата разработка цели да отговори на тези въпроси и да представи възможен подход занапред относно уреждането на международния трансфер на данни с трети страни. Първо, ще бъде представен най-общо режимът за защита на личните данни в рамките на ЕС. Ще бъде разгледана в детайли уредбата относно трансфера на данни, като ще се обърне внимание на съществуващите критики към настоящия режим и практическите проблеми, които частноправните субекти срещат при изпълняване на задълженията си. От особено значение са новите технологии, чието значение нараства в съвременните обществени отношения, както и рисковете, които крият, с оглед трансфера на данни. На последно място, ще се разгледат неуспешните опити за уреждане на трансфера на данни със страни като САЩ. Ще се преосмисли ролята на ЕС в тези междудържавни отношения с цел да се даде по-ефективен подход към уреждането на международния трансфер на данни с чужди юрисдикции, които все още не са напълно в съответствие с европейските стандарти. Ще се разгледат и основни насоки за преодоляването на различните нива на защита на личните данни.

II. Правна рамка на защитата на лични данни в Европа

На първо място, разглеждайки режима за трансфер на данни, следва да установим какво представляват личните данни и как са регламентирани на европейско ниво. Могат да се установят три нива на регулация. Всички държави в рамките на ЕС са уредили защитата на лични данни на национално ниво, като упоменаването им може да се открие дори в конституционната им уредба.[5] Понякога принципите за защита на лични данни са облечени под формулировката на 'неприкосновеност на личния живот', но границите на защита съвпадат. Освен това всички държави членки на ЕС са и членки на Съвета на Европа и на Европейската конвенция за защита правата на човека (ЕКПЧ). Самата ЕКПЧ в член 8 урежда защитата на личните данни. Макар при създаването и темата за личните данни да не е била все още широко дискутирана, и защитата на личните данни да не е била обхваната от формулировката на член 8, то с времето и чрез практиката на Европейския съда по защита правата на човека (ЕСПЧ) личните

[5] В България например уредбата може да бъде намерена в чл. 32 от Конституцията.

данни също започват да попадат под защитата на ЕКПЧ.[6] Следва да се отбележи, че стандартите на ЕКПЧ също са високи и подлежат на постоянно подновяване и подобряване в следствие на практиката на ЕСПЧ. Това е от значение, тъй като съгласно член 52, ал. 3 от Хартата на основните права на ЕС стандартите, поддържани от ЕС, не бива да падат нов нивото на защита, предоставяно от ЕКПЧ. В този смисъл, ЕКПЧ не е единственият правен инструмент, който предоставя защита на личните данни, но практиката по него създава и общоевропейски стандарт, под който не бива да се пада.

Тази разработка обаче ще обърне най-съществено внимание на уредбата, която съществува на ниво ЕС. Защитата на личните данни от десетилетия подлежи на регулация от правото на ЕС, но по-голямо внимание на тази тематика се обръща след приемането на ОРЗД. Много автори обясняват това явление с високите санкции, които предвижда този регламент, които от своя страна не само създадоха високо ниво на съответствие от страна на частноправните субекти, но и успяха да подбудят обществения интерес към темите за защита на личните данни.[7] Особената важност, която има уредбата на ЕС в сферата на защитата на личните данни, може да се обясни в няколко аспекта. На първо място, както беше отбелязано, ОРЗД предвижда санкции към самите частноправни субекти, които го нарушават. Това е най-силният мотиватор за спазването на режима на защита, което превръща и самия режим в един от най-значимите. На второ място, ОРЗД вмени задължения на държавните членки да създадат изрични надзорни органи, които да следят за спазване на законовите изисквания – това също превърна режима на защита в един от най-прилаганите.[8] На трето място, международният характер на уредбата предполага постоянен обмен на опит и знания в рамките на вътрешния пазар, което създава повече експертиза за съобразяване с актуални проблеми, като особеностите на новите технологии. Също така Европейският комитет за защита на личните данни, създаден посредством ОРЗД, има изричната задача да публикува препоръки и становища с оглед уеднаквяване на режима и подобряване на стандартите за защита, което пак подпомага модернизацията на уредбата.[9] На последно място,

[6] Department for the execution of Judgments of the European Court of Human Rights DG1, Personal Data Protection, Thematic factsheet, September 2022.

[7] Voss, WG. & H. Bouthinon-Dumas, EU General Data Protection Sanctions in Theory and in Practice. – Santa Clara High Tech. L.J. 2021, 37(1).

[8] Съгласно чл. 51 от Регламент (ЕС) 2016/679.

[9] Bolognini, L., T Bonettti & E Guarnieri, The „super-powers" of the European Data Protection Board (EDPB) and the principle of due administrative procedure. – Diritto, Economia e Tecnologie della Privacy, 2025, № 1.

ЕС, като орган на влияние, е в позицията да преговаря с други юрисдикции по въпросите относно защитата на данните, особено в контекста на трансфер на данни. Съюзът все още се ползва с авторитета на стожер в тази област и оказва влияние на световните тенденции. Тези и други особености обясняват защо ОРЗД може да се опише като един от най-важните актове в сферата на защита на личните данни и е основен обект на интерес за настоящата разработка.

С оглед темата за трансфер на данни, няма да се съсредоточаваме върху конкретната уредба относно защитата на лични данни под ОРЗД. Единствено може да се отбележи дефиницията на лични данни, а именно всяка информация, свързана с идентифицирано или идентифицируемо живо физическо лице.[10] От интерес са и основните принципи на защита: законосъобразност, ограничаване на целите за обработка, свеждане на данните до минимум, точност на данните, ограничение на периода на съхранение, цялостност и поверителност на данните, отчетност.[11] Те обаче няма да се разглеждат подробно, а следва да обрисуват единствено подхода, предприет на ниво ЕС, който се характеризира с изчерпателност и пълна защита на правата и интересите на субектите на лични данни. Тези характеристики са важни, за да може впоследствие да се обърне внимание на пропуските, които съществуват в уредбата на защитата на лични данни в трети страни и рисковете, които се повдигат.

III. Правна уредба на трансфера на данни – какви механизми съществуват и какви са техните слабости?

Преди да разгледаме подробно уредбата за трансфера на данни извън рамките на ЕС, трябва да определим в кои ситуации се счита, че има трансфер на данни. Критериите за това са определени от Европейския комитет за защита на личните данни – има администратор или обработващ лични данни, който е обвързан с ОРЗД и прехвърля или прави достъпни тези лични данни на други физически или юридически лица, които са разположени извън Европейското икономическо пространство или са част от международна организация.[12] Такива ситуации ще стават все по-чести с напредването на глобализацията и съвременните икономически процеси. От една страна, все повече компании интернационализират своята дейност, аутсорсват процесите си в трети страни, къ-

[10] Съгласно чл. 4, т. 1 от Регламент (ЕС) 2016/679.
[11] Уредени в глава 2 от Регламент (ЕС) 2016/679.
[12] International data transfers, Data Protection Guide for small businesses, (https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en).

дето разходите са по-малко.[13] От друга страна, някои съвременни технологии, като облачните услуги, действат на принципа на качването на данни на сървъри, които често може да са разположени в трети страни или поне да дават достъп на лица, които са разположени в трети страни.[14] С оглед на тези тенденции, темата за трансфера на данни и неговата уредба в ЕС ще расте по важност.

Именно заради това следва да разгледаме подробно механизмите, които урежда трансфера на данни. Накратко, съществуват няколко защитни механизма за уреждане на трансфера на данни между ЕС и трети страни. Те са установени в самия ОРЗД, както и в практиката на Съда на Европейския съюз (СЕС). Важно е все пак да се отбележи, че за да е законосъобразно обработването на лични данни, те трябва да са събрани на валидно законово основание под ОРЗД и в съответствие с принципите на обработка.

3.1. Решения за адекватност

На първо място, съгласно уредбата в ОРЗД, Европейската комисия има компетентността да издаде решение относно адекватното ниво на защита на конкретна трета страна.[15] При наличието на такова решение не следва да възникнат притеснения относно законосъобразността на трансфера на данни. Такива решения към днешния момент има за: Обединеното Кралство, Андора, Нова Зеландия, Швейцария, Канада, Япония, т.н.[16] Интересно е да се отбележи, че признаването на нивото на адекватност на защитата на личните данни може да обхваща цялата територия на трета страна, определени администратори и тяхната сфера на дейност или определени програми за обмен на данни или видове обработка.

Основен проблем с този механизъм е свързан с началната несигурност на подобен подход на регулиране. Следва да се отбележи, че тези решения във всеки момент може да бъдат изменени или дори отменени. Може да се отбележи и явно противоречие между интересите на Комисията, която все пак иска да способства по-бързия граждански оборот и сътрудничество, и СЕС, който трябва да защити строгите стандарти за защита, установени от ОРЗД. Това създава риск двата

[13] What Is Globalization in Business? – Harvard Business School Online, (https://online.hbs.edu/blog/post/what-is-globalization-in-business).
[14] Ibid.
[15] Съгласно чл. 45 от Регламент (ЕС) 2016/679.
[16] Adequacy decisions, European Commission (https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

органа да влязат в противоречие и решения за адекватност, които на първо време са давали сигурност, да бъдат отменени от СЕС.[17]

От друга страна, друг проблем би бил свързан с прекомерното уповаване на тези решения. В случай, че органите на Съюза, с оглед повече стабилност, рядко поставят под въпрос първоначално издадени решения за адекватност, това би накърнило правата и интересите на субектите на лични данни. Така нареченият „*rubber stamping*" може да се наблюдава на регулативно ниво, когато институциите не преразглеждат решенията си, за да се избегнат противоречия и негодуване от страна на обвързаните с тях субекти.[18] Но не бива с оглед тези интереси да се позволява трансфер на данни към трети страни, чието ниво на защита не е било обстойно проверено и одобрено.

И двата проблема на този подход на регулиране на трансфера на данни лесно могат да се превъзмогнат чрез балансиран подход и правилна преценка относно противоречивите интереси, които са обхванати. Спорно е обаче до каква степен усложнената машина от институции на ЕС може да постигне бърз и ефективен баланс на интереси.

3.2. Механизми за защита при липсата на решение за адекватност

Съгласно уредбата на ОРЗД и практиката на СЕС, при липсата на решение за адекватност, администраторите и обработващите лични данни може да се уповават на защитни механизми като 1) стандартни договорни клаузи между компании, че ще се спазват стандартите на защита при обмен на данни; 2) създаването на задължителни корпоративни правила, когато данни трябва да се споделят в рамките на икономическа група или 3) разчитането на механизми за сертифициране от страна на трети лица или организации на нивото на съответствие с основните стандарти за защита на лични данни.[19] Тези механизми целят да предоставят относителна сигурност относно стандарта за защита, който ще се спазва при обработката на лични данни от страна на физически и юридически лица в трети страни.

Тези механизми обаче не дерогират задължението на администраторите и обработващите лични данни да следят за нивото на защита на личните данни в конкретния случай и как определени промени в об-

[17] „In the EU-US data transfer and privacy quarrel, the end is not in sight" (https://www.euronews.com/next/2024/05/21/in-the-eu-us-data-transfer-and-privacy-quarrel-the-end-is-not-in-sight).

[18] „Europe cannot rubber stamp the UK's data laws", Open Rights Group, 18 March 2021 (https://www.openrightsgroup.org/blog/europe-cannot-rubber-stamp-the-uks-data-laws/).

[19] Съгласно чл. 46 – 47 от Регламент (ЕС) 2016/679.

стоятелствата биха се отразили на сигурността на споделяните лични данни. Макар много администратори и обработващи лични данни да смятат, че със сключването на стандартен договор за спазване на стандартите на защита или чрез приемането на корпоративни правила в този смисъл са изчерпали задълженията си под ОРЗД, това съждение е далеч от истината. Напротив, от съществено значение е постоянният контрол на обработването на данни и създаването на адекватни проверки и механизми за контрол, за да се създаде сигурност, че европейските стандарти биват спазвани и от представителите на трети страни. Задължението за пълно съответствие с ОРЗД не се изчерпва в един конкретен момент при трансфера на данни, а е трайно и обвързва администраторите и обработващите по време на целия процес на обработка. Следва да се обръща повече внимание на това обстоятелство и защитата на личните данни да е приоритет при всяка стъпка в рамките на дадения процес на работа.

3.3. Използване на някое от изключенията като основание за обработка

На последно място, съгласно ОРЗД, има и някои изключения, които биха могли да оправдаят трансфера на лични данни. Основания за това са: субектът на лични данни е дал съгласие за трансфера; трансферът е необходим за изпълнение на договор; трансферът е необходим с оглед на обществения интерес.[20]

Това са само някои от изключенията, но не бива да се забравя, че тези изключения не следва да стават правило и принцип на работа. Те биха могли да се използват само където другите механизми за защита са неприложими или трудно приложими.[21] Също така важно е да се отбележи, че необходимостта е критерий, който изисква индивидуална преценка спрямо конкретните обстоятелства.[22] Тоест общото уповаване на изключението за трансфер на данни с оглед абстрактната необходимост от това не може да се използва от администраторите или обработващите данни.

[20] Съгласно чл. 49 от Регламент (ЕС) 2016/679.

[21] International data transfers, Data Protection Guide for small businesses, n. 12 (https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en).

[22] Европейски комитет по защита на данните, Насоки № 2/2018 относно дерогациите по член 49 от Регламент 2016/679, 25 май 2018 г.

VI. Правни аспекти на трансфера на данни извън ЕС – Шремс и пътят напред

Един от най-важните въпроси, които вълнуват бизнеса и институциите в ЕС, е как да осъществят законосъобразно международни трансфери на лични данни, без да нарушават основополагащите права и гарантираните свободи на субектите на данни. Този въпрос става още по-сложен, когато се отчете фактът, че ЕС има един от най-високите стандарти за защита на данните в света и като се има предвид, че международният трансфер на данни е неизбежна и жизненоважна необходимост за много предприятия. Изискванията на Европейския съюз за защита на данните поставят значителни предизвикателства пред режимите за защита на данните в други държави, като например САЩ.

4.1. Защита на данните в САЩ

Защитата на данните между ЕС и САЩ привлече голямо внимание през последните години (поради критичната роля на данните в глобалната икономика и сигурност) с приемането на споразуменията „Безопасно пристанище“ (*Safe Harbour*) и „Щит за защита на личните данни“ (*Data Privacy Shield*), които съответно бяха посечени от СЕС в поредицата от решения „Шремс“. Първоначално защитата на данните при трансфери между ЕС и САЩ се основаваше главно на споразумение, известно като „Безопасно пристанище“, което предвиждаше самосертификация на американски организации, които да декларират, че спазват определени принципи за защита на данните, съгласувани с правните изисквания на ЕС.[23] В решението **„Шремс I“** Съдът на ЕС обаче обяви за невалидно това споразумение с аргумент, че не гарантира адекватна защита за гражданите на ЕС.[24] Основното опасение беше, че достъпът на американски разузнавателни органи до лични данни не е достатъчно ограничен и контролът върху това обработване е недостатъчен. Впоследствие Европейската комисия и САЩ договориха нов механизъм – т.нар. „Щит за защита на личните данни“, който също трябваше да осигури адекватно ниво на защита за личните данни, предавани в САЩ.[25]

---

[23] Решение на Комисията от 26 юли 2000 година съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, гарантирана от принципите за „сфера на неприкосновеност на личния живот“ и свързаните с това често задавани въпроси, публикувани от Департамента по търговия на САЩ.

[24] Case C-362/14 Maximillian Schrems v Data Protection Commissioner (CJEU 2015) ECLI:EU:C:2015:650.

[25] Решение за изпълнение (ЕС) 2016/1250 на Комисията от 12 юли 2016 година съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адек-

През 2020 г. обаче в решението **„Шремс II“** Съдът на ЕС отново обяви за невалидно и това споразумение, като изтъкна подобни причини – липса на адекватни гаранции срещу прекомерните правомощия на американските разузнавателни служби и ограничен достъп до ефективна защита за субектите на данни от ЕС.[26]

В отговор на последното решение Комисията прие разрешения в две направления. Първо, тя прие преработен набор от стандартни договорни клаузи през юни 2021 г., за да улесни спазването на изискванията на Съда, които биват два вида: първият – за използване между администратори и обработващи лични данни в рамките на Европейското икономическо пространство (ЕИП)[27], а другият – за предаване на лични данни на държави извън ЕИП.[28] В новите клаузи може да се забележи детерминизмът на ЕС за значително засилване на защитата на данните. Налагането на строги задължения при международния трансфер на данни е в съответствие именно с екстериториалния обхват на ОРЗД. В края на краищата правата на субектите на данни биха били изложени на риск, ако защитата им е ограничена до границите на ЕИП, но данните биват използвани от субекти извън стандартите на ЕС.

Второто разрешение на Комисията беше в насока на ново (трето) споразумение със САЩ за адекватна защита на личните данни между двете територии – т.нар. **Рамка за защита на личните данни** (*Data Privacy Framework*) – в сила от 10 юли 2023 г.[29] Това е най-новата версия, разработена от Комисията, с цел улесняване на трансатлантическата търговия чрез предоставяне на американските организации на надеждни механизми за предаване на лични данни в Съединените щати от ЕС и ЕИП, както и Обединеното кралство (и Гибралтар) и Швейцария, които са в съответствие със законо-

ватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ (EU-U.S. Privacy Shield).

[26] Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (CJEU 2020) ECLI:EU:C:2020:559.

[27] Решение за изпълнение (ЕС) 2021/915 на Комисията от 4 юни 2021 година относно стандартни договорни клаузи между администратори и обработващи лични данни съгласно член 28, параграф 7 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета и член 29, параграф 7 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета.

[28] Решение за изпълнение (ЕС) 2021/914 на Комисията от 4 юни 2021 година относно стандартни договорни клаузи за предаването на лични данни на трети държави съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета.

[29] Решение за изпълнение (ЕС) 2023/1795 на Комисията от 10 юли 2023 година съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни в Рамката за защита на личните данни в отношенията между ЕС и САЩ.

дателството на ЕС. То е продължение на принципа, че всяко споразумение за международен трансфер на данни между Европейската комисия и трети държави трябва стриктно да спазва принципите на Договорите, като същевременно предоставя на гражданите на ЕС гаранции за защита на личните данни, които по същество са равностойни на предвидените в ОРЗД и ХОПЕС.

4.2. Критики към новото решение

Въпреки усилията на Европейската комисия и значителния обем от работата по изграждане на правната рамка, критиките към новата Рамка за защита на личните данни (Data Privacy Framework) не закъсняха:

Първо, САЩ се ангажират да ограничават събирането на разузнавателни данни до пропорционални и необходими цели, но остава отворен въпросът доколко американската правна система действително отразява в пълна степен вижданото за „пропорционалност", залегнало в правото на ЕС. Самата концепция за пропорционалност има различни нюанси в ЕС и САЩ, което поражда съмнения дали обещаното ограничение ще бъде приложено на практика достатъчно ефективно и дали европейските субекти ще имат ефективни средства за защита, ако правата им бъдат нарушени. В тази връзка е от съществено значение да бъдат въведени допълнителни механизми за прозрачност и отчетност.

Второ, основният проблем, повдигнат в решенията „Шремс I" и „Шремс II", остава – дали разузнавателните органи на САЩ ще разполагат с прекомерен достъп до личните данни на гражданите на ЕС и дали европейските субекти ще имат ефективни средства за защита, ако правата им бъдат нарушени. Въпреки създаването на специални механизми за надзор и жалба, мнозина все още са скептични дали тези средства са достатъчно силни, за да ограничат безконтролното наблюдение. Следователно, остава неясно дали ще има значителна промяна във възможността разузнавателните органи на Съединените щати да осъществяват следене на гражданите на ЕС.

Трето, остава въпросът дали механизмите, предвидени в новата рамка, ще бъдат достатъчно устойчиви срещу бъдещи правни предизвикателства. Историята на предишните споразумения показва, че недостатъчните гаранции водят до правна несигурност. Все пак не можем още да отметнем риска новото споразумение в крайна сметка отново да бъде атакувано пред Съда на ЕС и да се стигне до вариант „Шремс III", ако Съдът приеме, че гаранциите отново не покриват високите стандарти, изисквани от правото на ЕС. Освен това, би могло да се мисли и по отношение на нуждата от по-голяма синхронизация между правните системи на ЕС и САЩ, което би минимизирало риска от бъдещи конфликти и би улеснило трансфера на данни.

Четвърто, подчертава се, че гражданите на ЕС все още може да не разполагат с достатъчно ефективни средства за защита на своите права. Въпреки че новата рамка включва механизми за подаване на жалби и надзор, остават опасенията дали тези механизми ще бъдат достатъчно достъпни, ефективни и прозрачни за всички засегнати страни. Този въпрос е от ключово значение, особено в контекста на бързо развиващите се технологии и нарастващата нужда от ефективна защита на личните данни.

Критиките към новата рамка за защита на личните данни подчертават не само сложността, но и важността на международното регулиране на трансфера на данни. Докато ЕС и САЩ полагат усилия за укрепване на правната рамка, остава ясно, че изграждането на ефективни и устойчиви механизми изисква значителна синергия, прозрачност и съобразяване с високите стандарти за защита на личните данни.

V. Основни насоки към бъдещето на трансферите

Разгледаните проблеми създават ред въпроси относно начина на тяхното решаване. Бъдещето на трансфера на данни мъжделее все поплахо, особено на фона на другите глобални проблеми, пред които са изправени днешните демокрации. За щастие, проблематиката е толкова практична, колкото е техническа и заради това възможни решения винаги съществуват. Тук ще се спрем на три насоки, към които може да се обърнем в бъдеще по отношение на трансфера на данни свързан с трети страни.

Първата посока от решения е свързана с дейността на фирмите и частноправните субекти като цяло. Един от основните акценти за организациите ще бъде постоянната необходимост от извършване на задълбочени оценки на въздействието на трансфера. Тези вътрешни оценки са от съществено значение за определянето и прилагането на подходящи допълнителни мерки за поддържане на равностойно ниво на защита на данните, предавани на трети държави. Това обаче ще създаде нови пречки за бизнесите да оперират плавно в международен план.

На второ място, тъй като технологиите продължават да се развиват, разпоредбите за защита на данните и неприкосновеността на личния живот ще трябва да се адаптират съответно. Развитието на технологии като изкуствен интелект, блокчейн и интернет на нещата поставя предизвикателства пред спазването на принципите на ОРЗД.[30] Организациите например ще трябва да гарантират, че ефек-

[30] Kuner, C. et al., Blockchain versus Data Protection. – International Data Privacy Law, 2018, No 8, 103-104.

тивно информират субектите на данни за самоличността на вносителите на данни, което надхвърля настоящите задължения за прозрачност.

Не на последно място, когато данните се предават на юрисдикции, които не разполагат с адекватно ниво на защита, трябва да се приемат допълнителни мерки за защита на данните. Тези мерки могат да включват комбинация от технически, организационни и договорни предпазни мерки. ЕКЗД е издала препоръки, които предоставят неизчерпателен списък на технически мерки, като например най-съвременно криптиране, псевдонимизиране и обработка чрез криптографски ключове.[31] ***Криптирането*** е основна техническа мярка, която може ефективно да защити личните данни по време на предаването им. Чрез преобразуването на информацията в шифрован код криптирането гарантира, че неоторизирани страни нямат достъп до информацията без правилния ключ. ***Псевдонимизирането*** заменя идентификатора между информацията в даден набор от данни и физическото лице, което стои зад тях. Личните идентификатори (например име, възраст и др.) се заменят с псевдоним, например произволно число или хеш, а връзката между идентификатора и псевдонима се защитава чрез отделно съхраняване на допълнителната информация, необходима за идентифициране на физическото лице. Накрая, ***криптографските ключове*** са инструмент за декриптиране на криптирани данни. Новост тук обаче представлява т.нар. хомоморфно криптиране, където личните данни са криптирани с таен ключ, който е известен само на потребителя. Това предоставя освен защита за самите лични данни и възможност данните да бъдат включвани в изчисления на обработващи лица без да се компрометират.

VI. Заключение

Новата технологична революция на 21. век тича стремглаво напред, проправяйки път за нови проблеми по отношение на защитата на личните данни, но и по отношение на тяхната защита. Както беше разгледано, нивото на защита в ЕС и ЕИП е силно повлияно както от вторичното право на ЕС, така и от юриспруденцията на наднационални структури като ЕСПЧ. В резултат може да се очертае една що-годе сложна система от правила, забрани и дерогация от тях, която обхваща все повече физически и юридически лица.

[31] Juliussen, B. et al., The Third Country Problem under the GDPR: Enhancing Protection of Data Transfers with Technology. – International Data Privacy Law, 2023, No 13, p. 225, 231–239.

Важността на новите технологии си проличава и в самите възможности, които правната рамка на личните данни ни предоставя. Използвайки най-съвременните технологични инструменти като криптиране, администраторите на лични данни биха успели да уцелят така тънкия баланс между строгите регулации на ЕС, от една страна, и защитата на основните права на клиентите им, от друга страна. В ръцете на европейските институции остава все пак възможността да продължават да прецизират уредбата за защита на лични данни и да насърчават използването на новите технологии за законосъобразната им обработка.