

## **PNR ДАННИ – ИСТОРИЧЕСКО РАЗВИТИЕ И ЗАЩИТА КЪМ НАСТОЯЩИЯ МОМЕНТ**

*Проф. д-р Габриела Белова, гл. ас. д-р Анна Христова, Катедра „Международно право и международни отношения“, Правно-исторически факултет, Югозападен университет „Неофит Рилски“ – Благоевград*

**Резюме:** *В статията е проследена уредбата на резервационните данни на пътниците (PNR данни) първоначално в Директива 95/46/ЕО, а впоследствие и Директива (ЕС) 2016/681, както и в поредицата споразумения за PNR данни главно между ЕС и САЩ, но също така между ЕС и Австралия, ЕС и Канада. Разгледана е оценката на Комисията относно прилагането на Директивата на ЕС за резервационните данни на пътниците през първите две години, която като цяло е положителна. Посочено е, че в решението си по делото C-817/19, Ligue des droits humains преди по-малко от година – на 21 юни 2022 г. Съдът на Европейския съюз (СЕС) постанови, че „при липса на действителна и настояща или предвидима терористична заплаха за държава членка, правото на ЕС не допуска национално законодателство, предвиждащо предаване и обработка на резервационни данни на пътниците (PNR данни) на вътрешни за ЕС полети и транспортни операции, извършвани с други средства в рамките на Европейския съюз“. В този смисъл, Съдът на ЕС зае по-рестриктивна позиция, особено по отношение на два въпроса: (1) по-строги ограничения по отношение на полетите и транспортните операции в рамките на ЕС; (2) по-строг подход към периодите на съхранение.*

**Ключови думи:** *PNR данни, Директива (ЕС) 2016/681, споразумения ЕС – САЩ, съдебна практика на Съда на Европейския съюз.*

## **PNR DATA – HISTORICAL DEVELOPMENT AND CURRENT PROTECTION**

*Prof. Gabriela Belova, PhD, Ch. Assist. Prof. Anna Hristova, PhD, Department of International Law and International Relations, Faculty of Law and History, South-West University “Neofit Rilski” – Blagoevgrad*

**Abstract:** *The article observes development of the EU legislation concerned Passenger Name Record (PNR) data, initially in Directive 95/46/EC, and subsequently in Directive (EU) 2016/681, as well as in the several PNR agreements mainly between the EU and the US, but also between the EU and*

*Australia, the EU and Canada. The Commission's assessment of the implementation of the EU PNR Directive in the first two years is examined, which is generally positive. In its judgment in case C-817/19 Ligue des droits humains of 21 June 2022, the Court of Justice of the European Union (CJEU) ruled that "in the absence of a genuine and present or foreseeable terrorist threat to a Member State, EU law precludes national legislation providing for the transfer and processing of Passenger Name Record (PNR) data on intra-EU flights and transport operations; carried out by other means within the framework of the European Union". In this sense, the CJEU has taken a more restrictive stance, especially with regard to two issues: (1) greater restrictions on intra-EU flights and transport operations; (2) a more rigorous approach to retention periods.*

**Keywords:** PNR data, Directive (EU) 2016/681, EU-US agreements, Court of Justice of the European Union's case-law.

Достъпът и предаването на резервационни данни на пътниците (PNR данни) безспорно попадат в обхвата на европейското законодателство за защита на личните данни. Самият термин PNR (Passenger Name Record) включва данни относно имената на пътниците; дестинацията; детайли, свързани с издаването на билета; агенцията, през която се закупува билетът; лицето / компанията, извършващи резервацията. Първоначално Международната асоциация за въздушен транспорт (IATA) определя рамките и съдържанието на тези данни, като те се предоставят само при самолетните пътувания. Впоследствие PNR данните започват да се използват и при резервация на хотели, рент-а-кар и други дейности. След събитията от 11 септември 2001 г. PNR данните включват пълните имена на пътниците (дотогава практиката е да се използва фамилното име и инициалите на собственото), паспортните данни (националност, номер на паспорта / документ за самоличност и срок на валидност), както и датата и мястото на раждане. Разширяването на обхвата на PNR данните предизвиква загрижеността на редица НПО, тъй като данните могат да съдържат домашен ли служебен адрес, телефонни номера, данни от кредитни карти, инвалидност и др. Най-напред тяхната уредба се съдържа в Насоките за защита на личните данни на Организацията за икономическо сътрудничество и развитие (ОИСР) от 1980 г., а впоследствие и в Директивата на Европейския съюз от 1995 г. относно защитата на данните (Директива 95/46/ЕО)<sup>1</sup>, която прогласява, че PNR

---

<sup>1</sup> Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното

данните могат да се прехвърлят само към трети държави със сравними стандарти за защита на данните. Също така е въведен принципът, че правоприлагащите органи имат право на достъп до данните на пътниците само във всеки отделен случай и когато съществува конкретно подозрение.

След атаките от 11 септември 2001 г. администрацията на САЩ определя, че PNR данните (както архивирани, така и в реално време) са безценни инструменти за разследване и осуетяване на терористични атаки. Съответно американското федерално правителство поиска събирането, прехвърлянето и задържането на PNR данни да се извършва от Бюрото за митническа и гранична защита към Министерството на вътрешната сигурност на САЩ (Department of Homeland Security).

## **1. Споразумения за трансфер на резервационни данни**

През м. май 2004 г. между Европейската комисия и правителството на САЩ е договорено Споразумение за прехвърляне на данни за резервационните данни на пътниците (известно още като Споразумение за PNR данни между ЕС и САЩ), с което се въвежда възможност за предаване на PNR данни от т.нар. „сфера на неприкосновеност“ (Safe Harbor). По-конкретно Европейската комисия счита, че степента на защита, предоставена за предаване на подобни PNR данни, би отговаряла на стандарта за „адекватност“, изискван от Директива 95/46/ЕО, доколкото данните ще бъдат предавани и използвани единствено за целите, за които са събрани. Тези цели се ограничават до „предотвратяване и борба срещу тероризма и свързаните с него престъпления; срещу други тежки престъпления, включително организирана престъпност, които имат транснационален характер; както и бягство от заповеди за арест или задържане под стража за тези престъпления“<sup>2</sup>. Споразумението ЕС – САЩ изисква европейските авиокомпании да предоставят PNR данни на компетентните органи на САЩ в рамките на 15 минути след излитането на самолета, като за неизпълнение на своето задължение заплащат глоба от 5 хиляди долара за информацията за всеки пътник. Европейският парламент инициира производство пред Съда на Европейските общности. Споразумението бе обявено за невалидно от

---

движение на тези данни, заменена от Общия регламент за защита на данните (ОРЗД). Защита на личните данни (europa.eu).

<sup>2</sup> Agreement between the European Community. and the U.S. on the processing and transfer of PNR data by air carriers to the U.S. Dep't of Homeland Sec., Bureau of Customs and Border Prot. Council Directive 2004 O.J. (L 183) 94 (EC).

Съда на 30 май 2006 г. поради несъответстващо правно основание. Всъщност Съдът на Европейските общности прие, че споменатото споразумение следва да бъде сключено не въз основа на общата транспортна политика на Съюза, а трансферът на PNR данни се извършва с оглед на дейности, причислявани към втория и третия стълб на Договора от Маастрихт, а именно „обществена сигурност, отбрана и наказателноправно сътрудничество“<sup>3</sup>. Въпреки това Европейският съвет усилено продължаваше да работи за възобновяване на споразумението преди определения от съда краен срок – 30 септември 2006 г.

На практика американският модел на защита на личните данни и неприкосновеността на личния живот е напълно различен от европейския – аспект, който понякога води до конфликти в трансатлантическите отношения, както в случая относно PNR данните. Ако в рамките на Европейския съюз опитът е в посока на по-строга регулация, която ограничава манипулирането на личните данни до това, което е строго необходимо, то ситуацията в САЩ е почти обратната и позволява събиране и натрупване на огромни масиви от лични данни. Освен това, за разлика от Европейския съюз, Съединените щати доскоро нямаша надзорен орган.

Друга голяма разлика е фактът, че докато в ЕС е налице законодателство, което регулира обработването на лични данни в цялостен обхват, то в Съединените щати се развива законодателство на парче, създавайки секторна система. Следва да се има предвид, че приетият от Конгреса през 1974 г. Закон за неприкосновеността на личния живот, всъщност е създаден в резултат на аферата „Уотъргейт“, замесила тогавашния президент Никсън, който трябваше да подаде оставка. Именно това извежда абсолютната необходимост да се поставят граници на злоупотребите, които са извършени от публични органи срещу граждани във връзка с неправомерното използване на информация, отнасяща се до тях. Въпреки десетилетията, изминали от неговото приемане, този закон все още представлява водещ инструмент в защитата на неприкосновеността на личния живот в САЩ, но трябва да се има предвид, че той се прилага само по отношение на американски граждани<sup>4</sup>.

---

<sup>3</sup> Белова Г. Европейският съюз и международното право, *сп. „Дипломация“*, издание на Дипломатическия институт при Министъра на външните работи, бр. 2 / 2009, с. 26.

<sup>4</sup> Anggriawan, Rizaldy, Andi Agus Salim, Yordan Gunawan, and Mohammad Hazyar Arumbinang. “Passenger Name Record Data Protection under EU and US Agreement: Security over Privacy?” *Hasanuddin Law Review* 8 no. 2 (2022): 95-1110. DOI: 10.20956/halrev.v8i2.2844, P-ISSN: 2442-9880, E-ISSN: 2442-9899, 2844-8546-1-PB.pdf.

Относно Споразумението за трансфер на PNR данни между ЕС и САЩ има два метода за предаване на данни: „push“ и „pull“. Чрез метода „push“ авиокомпаниите изпращат исканите данни в базите данни на органите, които ги искат. С метода „издърпване“, от друга страна, властите искат да получат свободен достъп до архивите на въздушните превозвачи и следователно могат директно да вземат копие от информацията за пътника<sup>5</sup>. По този начин европейските авиокомпании се озоваха под кръстосан огън. От една страна, американските власти изискваха те да предоставят личните данни на пътниците, като тези искания можеха да доведат и до забрана за кацане в САЩ. От друга страна, бе налице законодателството на Европейския съюз, което категорично забраняваше това прехвърляне. Съгласно Директива 95/46/ЕО е забранено всякакво предаване на данните на физически лица, събирани за търговски цели, на трети държави, които не гарантират съответното ниво на защита. От съществено значение бе и принципът на пропорционалност, забраняващ събирането на прекомерна и ирелевантна информация.

През м. юли 2007 г. е подписано ново, противоречиво споразумение между ЕС и САЩ относно PNR данните<sup>6</sup>. Малко след това администрацията на американския президент Джордж Буш-младши освобождава Министерството на вътрешната сигурност, както и системата за пристигане и заминаване (ADIS – Arrival and Departure System) от спазване на Закона за неприкосновеността на личния живот от 1974 г., което поражда опасения относно защитата на личните данни на гражданите на ЕС. През м. февруари 2008 г. Джонатан Фол (Jonathan Faull), по онова време Директор на Генерална дирекция „Правосъдие и вътрешни работи“ в Европейската комисия, се оплаква от нееднозначната политика на САЩ по отношение на PNR данните<sup>7</sup>. Така например, Съединените щати подписват същия месец меморандум за разбирателство с Чешката република в замяна на схема за премахване на визите, без предварително да се консултират с Брюксел. Напрежението между Вашингтон и Брюксел се дължи главно на пониското ниво на защита на данните в САЩ, особено след като чужденците не могат да се възползват от закрилата на горепосочения Закон за неприкосновеността на личния живот в САЩ от 1974 г. Неприкосновеността на личните данни в ЕС се регулира от Директива

---

<sup>5</sup> *Ibidem.*

<sup>6</sup> Jean-Pierre Masse. "New EU-US PNR Agreement on the processing and transfer of Passenger Name Record (PNR) data". Libertysecurity.org. Archived from the original on 12 January 2012.

<sup>7</sup> Brussels attacks new US security demands, European Observer. Вж. също Statewatch newsletter February 2008.

95/46/ЕО, а споразумението за т.нар. сфера на неприкосновеност на личния живот в САЩ, направено за сближаване с европейските норми, все още е спорно поради предполагаема липса на защита. Други страни, към които бе насочен инструментът на двустранните меморандуми за разбирателство, са Обединеното кралство, Естония, Германия и Гърция<sup>8</sup>. Меморандумите предвиждат допълнителни по-тежки изисквания от американска страна при предоставянето на данни (биометрични данни, данни за откраднати или изгубени паспорти), както и осигуряване на т.нар. въздушни шерифи на борда на трансокеанските полети. Поради това Джонатан Фол окачествява новите американски изисквания като „неприемливи и отиващи твърде далеч“<sup>9</sup>.

Споразумението между ЕС и САЩ относно трансфера на PNR данни веднага е последвано от нова порция критика от страна на Европейския парламент. Още повече, че след влизането в сила на Договора от Лисабон на 1 декември 2009 г. се променя един изключително важен фактор, а именно одобрението на Европейския парламент става необходимо за влизането в сила на споразумението. Всъщност съгласно член 218 от Договора за функционирането на Европейския съюз (ДФЕС) одобрението на Европейският парламент беше необходимо условие за сключване на споразумения относно сектори, в които се прилага обикновената законодателна процедура. След премахването на тристълбовата архитектура, създадена с Договора от Маастрихт, тази процедура вече се отнася и за съдебното и полицейското сътрудничество.

На 28 ноември 2011 г. бе изготвено ново споразумение относно предаването и използването на PNR данни между ЕС и Department of Homeland Security на САЩ. През м. април 2012 г. споразумението бе одобрено и прието от Европейския парламент, което бе горещо приветствано от Съвета на министрите по правосъдие и вътрешни работи. Споразумението осигурява защита на PNR данните, но критиците отново изразяват опасения, че няма достатъчно средства за защита в случай на злоупотреба с данните. Така например Чешката служба за защита на личните данни има сериозни съмнения поради следните причини:

1. Съгласно споразумението се събира огромно количество лична информация за всички пътници, които влизат и излизат от ЕС, независимо дали са заподозрени в извършването на определена

---

<sup>8</sup> Statewatch, March 2008.

<sup>9</sup> Цитирано по Белова Г. Европейският съюз и международното право, *сп. „Дипломатия“*, издание на Дипломатическия институт при Министъра на външните работи, бр. 2 / 2009, с. 26.

терористична / престъпна дейност, или не. Събирането и обработването на PNR данни в рамките на ЕС не следва да дава възможност за цялостно проследяване на всички пътници.

2. До този момент поддръжниците на споразумението не са успели да докажат полезността и необходимостта му в съответствие с член 8, параграф 2 от Европейската конвенция за защита правата на човека и основните свободи и член 52 от Хартата на основните права в ЕС.

3. До момента не е доказано, че при действията срещу тероризма и тежките престъпления са необходими други освен API данни<sup>10</sup>. За разлика от API информацията, PNR данните не се проверяват и следователно следва да се считат за ненадеждни.

4. Определението на понятието „тежко престъпление“ въз основа на спецификацията в Рамковото решение относно европейската заповед за арест (което включва категории като престъпления, свързани с компютри или ксенофобия), е доста широко, ако не и подвеждащо, тъй като европейската заповед за арест първоначално не е била създадена с оглед PNR цели.

5. Елементите от данни, изброени в приложението към споразумението, са уточнени твърде общо, като много от тях имплицитно включват допълнителни подгрупи от данни.

6. Проактивното използване на PNR данните означава извършване на анализ и създаване на критерии за оценка от отделните държави членки. Не са ясни критериите, въз основа на които трябва да бъдат идентифицирани заподозрените.

7. Обхватът на събраните данни изглежда прекомерен, периодът на съхранение от 5 години е непропорционален, дори ако данните трябва да бъдат маскирани.

8. Последниците от потенциалните изисквания за реципрочност не са разгледани в достатъчна степен. Европейският PNR модел би могъл да доведе до реципрочно повдигане на подобни изисквания от недемократични, корумпирани държави, които не осигуряват адекватно ниво на защита на основните права и свободи, включително личните данни. PNR данните, притежавани от такива държави, биха могли да представляват сериозен проблем.

9. Морските и сухопътните гранични контролно-пропускателни пунктове ще останат незащитени от PNR мярката, факт, водещ до предположението, че терористите и престъпниците най-

---

<sup>10</sup> API е съкращение от Application Programming Interface. В контекста на API думата Application се отнася до всеки софтуер с отделна функция. Интерфейсът може да се разглежда като договор за услуга между две приложения. Този договор определя как двете комуникират помежду си, като използват въпроси и отговори.

вероятно ще започнат да използват именно тези входи, а не летищата, увеличавайки по този начин заобикалянето на закона.

10. Предложеното решение изглежда непропорционално и по отношение на финансовите разходи и административната тежест за въздушните превозвачи, както и за публичния сектор, който ще трябва да създаде звената за данни за пътниците (ЗДП) и да ги оборудва със софтуер, хардуер и квалифициран персонал.

11. Чешката служба за защита на личните данни е категорично против намерението за разширяване на системата за полети в рамките на ЕС, както е предложено от Обединеното кралство. Разпространението на PNR схемата за полети в рамките на ЕС би означавало обработване на други видове лични данни, без да се предоставят конкретни доказателства относно необходимостта и пропорционалността<sup>11</sup>.

Въпреки критичното си становище чешката служба за защита на личните данни е готова да участва в преговорите по предложението за Директива, която да сведе до минимум отрицателното въздействие върху неприкосновеността на личния живот на индивидите.

През м. април 2012 г. Европейският парламентът отново бе призван да гласува новото споразумението относно предаването на PNR данни и той го одобри, въпреки отрицателното становище на Работната група по член 29<sup>12</sup>. Значителна тежест в това решение, за разлика от избора, направен по-рано от Парламента, несъмнено имаше политическият натиск, упражняван от САЩ. Американското правителство наистина заплашваше с отмяна на безвизовото пътуване на европейски граждани за САЩ. Както посочва М. Mendez, *„независимо от тази променена среда, накрая Европейският парламент все пак даде одобрението си за споразумението между ЕС и САЩ за трансфер на PNR данни през 2012 г., въпреки че то бе изпълнено с недостатъци в областта на защитата на данните“*.

## 2. Директива (ЕС) 2016/681

Пет години по-късно такъв акт на вторичното законодателство е приет, а именно Директива (ЕС) 2016/681, която е част от цялостния

---

<sup>11</sup> Czech DPA's opinion on the Commission's PNR directive proposal – document archive, Czech DPA's opinion on the Commission's PNR directive proposal – document archive: International relations: The Office for Personal Data Protection (uouu.cz)

<sup>12</sup> Работната група по член 29 (от Директива 95/46/ЕО) е независимата европейска работна група, която се занимаваше с въпроси, свързани със защитата на неприкосновеността на личния живот и личните данни до 25 май 2018 г. (датата на влизане в сила на ОРЗД).



пакет, регулиращ защитата на личните данни, включително Общия регламент за защита на данните, известен като GDPR<sup>13</sup>. Тя е приета на 24 май 2016 г. и влезе в сила на 25 май 2018 г. в държавите членки след изтичане на срока за транспонирането ѝ. За да се защити правото на лични данни, са поставени някои ограничения върху прехвърлянето, използването и съхранението на лични данни. На първо място, PNR данните могат да бъдат обработвани само за разследвания в борбата срещу тероризма или друго тежко престъпление. На второ място, събирането и обработването на чувствителни данни е забранено. На следващо място, запазването на PNR данни се разрешава до максимум 5 години, като след първоначален период от 6 месеца те трябва да бъдат маскирани и направени анонимни, така че индивидът да не може да бъде идентифициран директно. Всяка държава членка трябва да създаде информационно звено и прозрачно и ясно да информира пътниците относно събирането на PNR данни. На последно място, предаването на PNR данни на трети държави следва да се преценява за всеки отделен случай. Според българския изследовател Светлозар Марков, „Директивата за PNR въвежда уникална система за контрол на човешката мобилност“<sup>14</sup>. Същевременно според Европейския надзорен орган по защита на данните това е „първото широкомащабно и безразборно събиране на лични данни в историята на Съюза“ и може да засегне „милиони пътници, които не са заподозрени“<sup>15</sup>.

Директивата има за цел да регулира предаването на резервационните данни на пътниците (PNR данни) на международни полети от авиокомпаниите към държавите членки на Европейския съюз. Тя също така урежда обработката на тези данни от компетентните органи на държавите членки.

В съответствие с Директива (ЕС) 2016/681 PNR данните се състоят от информация относно резервациите, съхранявана от авиокомпаниите в техните системи за резервации и контрол на заминаването на пътниците. Събираната информация включва данни като:

- дати на пътуването;
- маршрут на пътуването;
- информация за билетите;
- данни за контакт;

---

<sup>13</sup> Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. 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 (Общ регламент относно защитата на данните).

<sup>14</sup> Пол-и-сиг-3-2019-22-29 (1).pdf.

<sup>15</sup> edps-2015-12-eu\_pnr\_en.pdf (europa.eu).

- използвани платежни средства;
- информация за багажа.

Всяка държава членка на ЕС трябва да създаде звено за данни за пътниците (ЗДП). ЗДП отговаря за събиране, съхраняване и обработване на данните, както и за предаване на данните или резултатите от обработването им на компетентните национални органи, а също така и за обмена на PNR данните и резултатите от обработката с други държави членки и Европол. Авиокомпаниите трябва да предоставят на ЗДП в държавите членки PNR данните за полетите, които кацат или излитат от ЕС. Директивата също така позволява, но не изисква държавите членки да събират PNR данни за избрани полети вътре в рамките на ЕС. Събраните данни могат да бъдат обработвани само за предотвратяване, разкриване, разследване и наказателно преследване на терористична дейност и други тежки престъпления.

Данните обаче следва да се обработват само в случаите, когато е налице предварителна оценка на пътниците по предварително определени критерии за риск и съответни бази данни за правоприлагане; за използване в конкретни разследвания / преследвания; като принос в разработването на критерии за оценка на риска.

По отношение на прехвърлянето и обмена на данните държавите членки не следва да имат безусловен достъп до базите данни на авиокомпаниите, а PNR данните се изпращат от авиокомпанията до ЗДП на съответната държава членка. Когато е необходимо и уместно, държавата членка трябва да предостави PNR данни за идентифицирано лице на компетентните органи на друга държава членка, а в определени случаи PNR данните могат да бъдат прехвърлени и към трета държава извън ЕС.

Данните, предоставени от авиокомпаниите, трябва да се съхраняват в база данни от ЗДП в продължение на 5 години от момента на прехвърлянето им в държавата членка, в която полетът каца или от която излита. След 6 месеца прехвърлените данни трябва да бъдат „деперсонализирани“, за да се прикрие определена информация, включително име, адрес и контактна информация, както и цялата информация за плащането, включително адреса за фактуриране. Разкриването на пълната PNR информация след изтичането на този 6-месечен срок се разрешава само при наличие на искания за PNR данни, отправени от компетентните органи или от Европол във всеки отделен случай, или ако подобно оповестяване е одобрено от съдебен или друг компетентен национален орган, съгласно вътрешното законодателство.

Както посочва Св. Марков, на 8.12.2017 г. в България Държавна агенция „Национална сигурност“ (ДАНС) откри Национално звено за

получаване и обработване на резервационни данни за пътниците в Република България, превозвани по въздух. В Инструкция № I-8 от 2.11.2016 г.<sup>16</sup> са определени и основните елементи на методиката за

---

<sup>16</sup> ИНСТРУКЦИЯ № I-5 от 3.08.2016 г. за методиката за определяне на критериите при съвпадения, по които Националното звено за получаване и обработване на резервационни данни за пътниците в Република България, превозвани по въздух, незабавно предоставя резервационни данни и резултатите от тяхното обработване на компетентните структури на Министерството на вътрешните работи и реда за предоставянето на данните. Издадена от председателя на Държавна агенция „Национална сигурност“ и министъра на вътрешните работи, обн., ДВ, бр. 73 от 16.09.2016 г., в сила от 16.09.2016 г. В съответствие с чл. 42б от Закона за Държавна агенция „Национална сигурност“ (Нов – ДВ, бр. 15 от 2016 г.) (1) (Доп. – ДВ, бр. 56 от 2018 г.) въздушните превозвачи са длъжни за своя сметка, самостоятелно или чрез упълномощен доставчик на услуги да предават на Националното звено резервационни данни на пътниците и данни на екипажа за всички полети до, във или от Република България.

(2) Резервационните данни по ал. 1 включват:

1. първоначален код на досието на пътника;
2. дата на резервация / издаване на билета;
3. планирана/планирани дата/дати на пътуването;
4. имена на пътника, дата на раждане;
5. адрес и координати за връзка (телефонен номер, електронен адрес);
6. информация относно плащането, включително адрес за издаване на фактура;
7. данни за пълния маршрут на предвиденото пътуване;
8. информация за често (редовно) пътуващ пътник;
9. пътническа агенция или пътнически агент;
10. пътнически статус на пътника, включително потвърждения, регистрационен статус, информация за неявяване на пътник за полет или за пътник без резервация, купувач си билет в последния момент;
11. индикации за разделяне на досието на пътника;
12. общи забележки (налична информация за непридружавани лица под 18-годишна възраст – име, пол, възраст, говорим език, име и данни за контакт с настойник при заминаване и пристигане, агент при заминаване и пристигане и други);
13. данни от самолетния билет (номер, дата на издаване, еднопосочен билет, тарифа);
14. номер на мястото в самолета;
15. информация относно споделянето на кодове на полети;
16. пълна информация за багажа;
17. брой и други имена на пътници, които фигурират в досието на пътника;
18. всички събрани предварителни данни за пътниците (вид и номер на документа за пътуване, националност, държава на издаване, дата на валидност, фамилно име, собствено име, пол, дата на раждане, въздушен превозвач, номер на полета, дата на отпътуване, дата на пристигане, място на отпътуване, място на пристигане, време на отпътуване, време на пристигане, както и общия брой превозвани пътници), както и когато не се съхраняват като част от резервационните данни на пътниците;
19. пълна история на промените в данните по т. 1 – 18.

(3) (Нова – ДВ, бр. 56 от 2018 г.) Данните на екипажа са данните по ал. 2, т. 18.

(4) (Нова – ДВ, бр. 56 от 2018 г.) В случай на съвместно използване на кодове при полети от един или повече въздушни превозвачи задължението за предаване на

определяне от НКТЦ на критерии за съпоставяне с получените и обработвани резервационни данни от Националното звено<sup>17</sup>.

Следва да се има предвид, че Част трета, дял III от Споразумението за търговия и сътрудничество между ЕС и Обединеното кралство разглежда въпроса за предаването, обработката и използването на PNR данни във връзка с полети между ЕС и Обединеното кралство. В него също така се определят правилата за полицейско и съдебно сътрудничество по наказателноправни въпроси между Обединеното кралство и ЕС по отношение на PNR данните.

Към момента ЕС има подписано споразумение относно предаването на PNR данни с Австралия. Настоящите правила между ЕС и Австралия датират от 2012 г. и в неотдавнашен преглед (през 2021 г.) на действието на споразумението Европейската комисия заключи, че Австралия трябва да изпраща повече данни на европейските правоприлагащи органи:

*„Що се отнася до въпросите, които трябва да бъдат разгледани допълнително, Австралия се приканва да увеличи усилията си за гарантиране на реципрочност и проактивно да споделя аналитична информация, получена от PNR данни, с държавите членки и, когато е целесъобразно, с Европол и Еврост“<sup>18</sup>.*

На 18 февруари 2020 г. Съветът прие решение, с което се разрешава започването на преговори между ЕС и Япония за споразумение относно предаването и използването на резервационни данни на пътниците (PNR данни).

Срокът на споразумението с Канада изтече през 2009 г. След възражението на Съда на ЕС от м. юли 2017 г.<sup>19</sup> срещу предложеното

---

резервационни данни на пътниците за всички пътници от полета и данните на екипажа е на въздушния превозвач, който го извършва.

<sup>17</sup> Пол-и-сиг-3-2019-22-29 (1).pdf.

<sup>18</sup> Statewatch | EU to Australia: send us your travel surveillance data.

<sup>19</sup> Становище 1/15 на Съда на ЕС се очерта като мощно допълнение към съществуващата трилогия за поверителност на данните, установена от Съда на ЕС в ерата след Сноудън в опит да се балансират условията на международното сътрудничество в обмена на данни между ЕС и други държави. Тези термини до голяма степен бяха моделирани около интересите на националната сигурност, които придобиха значителна известност след 11 септември. Преди самият Съд на ЕС да разгледа Споразумението за трансфер на PNR данни с Канада, той постанови две основополагащи решения, основавайки се на решението си за DRI, което не остави никакво съмнение, че Споразумението няма да бъде подписано. През м. октомври 2015 г. Голямата камера в решението си по делото Schrems обезсилва дългогодишното решение за адекватност на сферата на неприкосновеност на личния живот Safe Harbour, според което прехвърлянето на лични данни към дружества, базирани в САЩ, е допустимо, когато дружествата са се регистрирали, за да се съобразят с набор от принципи за защита на данните. Второто решение на Голямата камера дойде през

ново проектоспоразумение за трансфер на PNR данни между ЕС и Канада поради несъвместимостта му с Хартата на основните права в Европейския съюз Комисията и канадските органи преговориха нов проект на споразумение, който беше финализиран от главните преговарящи през м. март 2019 г. Почти четири години по-късно този нов проект на споразумение обаче все още не е подписан поради желанието на Канада да преговори разпоредбата за запазване на данни.

На 24 юли 2020 г. Комисията представи своя преглед на Директива (ЕС) 2016/681 на Европейския парламент и на Съвета от 27 април 2016 г. относно използването на резервационни данни на пътниците (PNR данни) за предотвратяване, разкриване, разследване и наказателно преследване на престъпления, свързани с тероризъм, и на тежки престъпления<sup>20</sup>.

Отчетено е, че Директивата предвижда по-специално задължението на въздушните превозвачи да предават на държавите членки PNR данните, които са събрали в хода на обичайната си дейност. Държавите членки трябва да създадат специални структури, които да отговарят за съхранението и обработката на PNR данни (звена за данни за пътниците – ЗДП). Докладът за преглед на Комисията се придружава от работен документ на службите на Комисията, който съдържа по-подробна информация и изчерпателен анализ на всички въпроси, подкрепящи констатациите в доклада за преглед. Документите определят директивата в нейния общ контекст и представят основните констатации от оценката след две години прилагане на разпоредбите на директивата. Основните констатации са:

- Като цяло създаването на система за PNR данни в целия ЕС работи добре. По-специално по-голямата част от държавите членки са създали напълно функциониращи ЗДП. Те са достигнали добро ниво на сътрудничество. Две държави членки обаче не са транспонирали (изцяло) директивата в края на периода на преразглеждане. Словения е уведомила за частично транспониране, като има предвид, че на 2 юли

---

декември 2016 г. в Tele2/Watson във връзка с националното законодателство за запазване на данни. Тъй като PNR схемите са форма на общо и безразборно запазване на данни, перспективите пред Споразумението за PNR данни между ЕС и Канада не бяха оптимистични. За повече информация вж. Mendez M. *Opinion 1/15: The Court of Justice Meets PNR Data (Again!)*, EP\_eJ\_2017\_3\_3\_Overview\_Mario\_Mendez\_00176.pdf.

<sup>20</sup> Commission: EU PNR Directive Delivered Tangible Results – eucrim; Explanatory Memorandum to COM(2020)305 – Review of Directive 2016/681 on the use of passenger name record (PNR) data for prevention, detection, investigation and prosecution of terrorist offences and serious crime – EU monitor.

2020 г. Комисията сезира Съда на ЕС с иск за неизпълнение на директивата.

- Националните мерки за транспониране като цяло са в съответствие с гаранциите за защита на данните на директивата. Някои държави членки обаче не са успели да отразят всички гаранции в националното си законодателство. Националните органи ги прилагат на практика. Предпазните мерки гарантират пропорционалността на обработването на PNR данни и имат за цел предотвратяване на злоупотреби. На практика сътрудничеството между ЗДП и длъжностните лица по защита на данните, отговарящи за наблюдението на операциите по обработване на данни, очевидно работи добре.

- Използването на PNR данни е дало осезаеми резултати в борбата срещу тероризма и тежката престъпност: правоприлагащите органи съобщават, че PNR данните са били успешно използвани за предварително планиране на техните интервенции, за идентифициране на неизвестни досега заподозрени, за установяване на връзки между членове на престъпни групи и за проверка на предполагаемия „начин на действие“ на тежките престъпници.

- Широкият обхват на директивата, който засяга всички пътници на входящи и изходящи полети към / извън ЕС, се е оказал необходим.

- Петгодишният срок на съхранение на PNR данните е необходим за постигане на целите за гарантиране на сигурността и защита на живота и безопасността на индивидите.

- Тъй като само малка част от данните на пътниците са предадени на правоприлагащите органи за проверка, PNR системата работи в съответствие с целта за идентифициране на високорискови пътници, без да се засягат добросъвестните пътници<sup>21</sup>.

Прегледът на Комисията разглежда и въпроса за евентуално разширяване на задълженията по Директивата за резервационните данни на пътниците. В него се посочва, че всички държави членки, с изключение на една, са разширили събирането на PNR данни от вътрешни за ЕС полети, което е заложено като опция в директивата. От оперативна гледна точка държавите членки желаят разширяване на обхвата на информацията от икономическите оператори, които не са превозвачи. Комисията също така отбелязва, че някои държави членки допълнително събират PNR данни от други видове транспорт, например морски, железопътни и автомобилни превозвачи, въз основа на националното си законодателство. Комисията обаче се колебае дали да установи общоевропейски правила в това отношение и посочва, че

---

<sup>21</sup> *Ibidem*.

първо е необходима задълбочена оценка на въздействието, тъй като удължаването на срока повдига значителни правни, практически и технологични въпроси. В крайна сметка няколко държави членки са посочили, че PNR данните биха могли да бъдат полезни и за защита на общественото здраве и за предотвратяване на разпространението на инфекциозни заболявания, например COVID-19, чрез улесняване на проследяването на контактите на болелите лица<sup>22</sup>.

В заключение, оценката на Комисията относно прилагането на Директивата на ЕС за резервационните данни на пътниците през първите две години като цяло е положителна. Комисията смята, че онзи момент няма нужда от изменения. В този контекст се подчертава, че поставените въпроси ще се нуждаят от задълбочена оценка в светлината на изхода по дело Case C-817/19, *Ligue des droits humains*.

### 3. Case C-817/19, *Ligue des droits humains*

Преди по-малко от година – на 21 юни 2022 г., Съдът на Европейския съюз (ЕС) постанови, че „при липса на действителна и настояща или предвидима терористична заплаха за държава членка правото на ЕС не допуска национално законодателство, предвиждащо предаване и обработка на резервационни данни на пътниците (PNR данни) на вътрешни за ЕС полети и транспортни операции, извършвани с други средства в рамките на Европейския съюз“<sup>23</sup>. Така според Съда държавите членки могат да събират данни за пътниците във въздушния транспорт за полети вътре в рамките на ЕС само ако докажат, че са налице достатъчно солидни основания да се счита, че са изправени пред терористична заплаха, която е действителна или настояща, или предвидима за срок, който е ограничен до строго необходимото. Ако тези условия не са изпълнени, събирането на PNR данни не може да бъде разширено до всички полети в рамките на ЕС, а трябва да бъде ограничено до полети в рамките на ЕС, свързани, *inter alia* с определени маршрути или модели на пътуване или до определени летища, за които по преценка на съответната държава членка има индикации, които биха оправдали това прилагане. Или както е посочено в някои коментари: „в своето горчиво-сладко решение Съдът на ЕС позволява схема за наблюдение на границите в целия ЕС, но уточнява неговите цели“<sup>24</sup>.

---

<sup>22</sup> *Ibidem*.

<sup>23</sup> Ruling of the CJEU on the implementation of the PNR Directive | ERA (eraa.org)

<sup>24</sup> In a bittersweet ruling, EU Court of Justice allows EU-wide border surveillance scheme but clarifies its limits - Access Now

Всъщност в съответствие с Директивата за резервационните данни на пътниците авиокомпаниите трябва да събират PNR данните на пътниците за полети извън ЕС, които влизат и излизат от Европейския съюз с цел предотвратяване и разкриване на престъпления, свързани с тероризъм, и на тежки престъпления. В настоящата си редакция Директивата дава възможност на държавите членки да я прилагат към вътрешните за ЕС полети. Запитването идва след преюдициално запитване, отправено от белгийския Конституционен съд през м. октомври 2019 г. относно валидността и съвместимостта на Директивата за резервационните данни на пътниците с правото на ЕС<sup>25</sup>. През м. юли 2017 г. Ligue des droits humains (LDH) подава жалба за отмяна на Закона от 25 декември 2016 г., с който във вътрешното белгийско право се транспонират Директивата за резервационните данни на пътниците, Директивата за API 2 и Директива 2010/65 относно формалностите за даване на сведения за кораби, пристигащи във и / или напускащи пристанища на държавите членки, и чрез който са нарушени права на човека като зачитане на личния живот и защита на личните данни, гарантиран според белгийското право и правото на ЕС. През м. октомври 2019 г. Конституционният съд на Белгия отправя до Съда на ЕС десет преюдициални въпроса, включително и относно валидността на Директивата за резервационните данни на пътниците и съвместимостта на Закона от 25 декември 2016 г. с правото на Съюза.

В постановеното решение Съдът приема, на първо място, че тъй като тълкуването на разпоредбите на Директивата за резервационните данни на пътниците с оглед на основните права, гарантирани от членове 7, 8 и 21 и член 52, параграф 1 от Хартата на основните права в Европейския съюз, гарантира съответствието на тази директива, разглеждането на преюдициалните въпроси не разкрива нищо, което може да засегне валидността на посочената директива.

В самото начало следва да се отбележи, че даден акт на Съюза трябва да се тълкува, доколкото е възможно, по начин, който не засяга неговата валидност и в съответствие с първичното право като цяло, и по-специално с разпоредбите на Хартата. Следователно държавите членки трябва да гарантират, че не се позовават на тълкуване на този акт, което би било в противоречие с основните права, защитени от правния ред на Съюза, или с другите общи принципи, признати от

---

<sup>25</sup> В съответствие с процедурата за преюдициално запитване Съдът на ЕС не решава спора, а дава на националните съдилища само указания относно тълкуването на правото на Съюза или на валидността на акт на Съюза. Националният съд или правораздавателен орган следва да се произнесе по делото в съответствие с решението на Съда, което по подобен начин е задължително за други съдилища или правораздавателни органи, пред които е повдигнат подобен въпрос.



правото на Съюза. Съдът уточнява, че много от съображенията и разпоредбите на Директивата за резервационните данни на пътниците изискват такова тълкуване, като подчертава значението, което законодателят на Съюза, като се позовава на високото равнище на защита на данните, отдава на пълното зачитане на основните права, закрепени в Хартата.

Съдът уточнява, че PNR Директивата води до безспорно сериозна намеса в правата, гарантирани в членове 7 и 8 от Хартата, тъй като се стреми да въведе режим на наблюдение, който е непрекъснат, нецеленасочен и систематичен, включително автоматизирана оценка на личните данни на всеки, който използва услугите на въздушния транспорт. Той отбелязва, че въпросът дали държавите членки могат да обосноват тази намеса, трябва да се преценява с оглед нейната тежест, като се провери дали значението на преследваната цел от общ интерес е пропорционално на тази тежест. Съдът стига до извода, че предвиденото в тази директива предаване, обработване и запазване на PNR данни може да се счита за ограничено до строго необходимото за целите на борбата с престъпленията, свързани с тероризъм, и с тежките престъпления, при условие че предвидените в тази директива правомощия се тълкуват ограничително.

В това отношение в решението се посочва по-специално, че системата, установена с Директивата за резервационните данни на пътниците, трябва да обхваща само ясно идентифицируема и ограничена информация, съдържаща се в категориите на приложение I към нея относно извършения полет и съответния пътник. Прилагането на системата, установена с Директивата за резервационните данни на пътниците, трябва да бъде ограничено до престъпленията, свързани с тероризъм, и тежките престъпления, които имат обективна връзка, макар и непряка, с въздушния превоз на пътници. Що се отнася до тези престъпления, прилагането на тази система не може да се разпростре върху престъпления, които, въпреки че отговарят на предвидения в тази директива критерий за прага на тежестта и са посочени в приложение II към нея, представляват обикновена престъпност с оглед на специфични характеристики на вътрешната наказателноправна система. Евентуалното разширяване на прилагането на Директивата за резервационните данни на пътниците по отношение на избрани или на всички полети в рамките на ЕС, което държава членка може да реши, като упражни правомощието, предвидено в посочената директива, следва да бъде ограничено до строго необходимото<sup>26</sup>. За тази цел то

---

<sup>26</sup> Подобно на заключението на генералния адвокат Съдът счита, че някои елементи на PNR данни, по-специално областта на „общите бележки“, не отговарят на

трябва да подлежи на ефективен контрол или от съд, или от независим административен орган, чието решение е задължително. В този смисъл Съдът уточнява, че:

- единствено когато държавата членка установи, че са налице достатъчно солидни основания да се счита, че е изправена пред терористична заплаха, за която е доказано, че е действителна и настояща или предвидима, прилагането на тази директива за всички полети в рамките на ЕС от или към посочената държава членка може да удължи срока, при условие че не надхвърля строго необходимото;
- при липсата на такава терористична заплаха прилагането на директивата не може да се разпростре върху всички вътрешни за ЕС полети, а трябва да се ограничи до полети в рамките на ЕС, свързани по-специално с определени маршрути или модели на пътуване, или с определени летища, за които по преценка на съответната държава членка има признаци, които биха обосновали това прилагане. Строго необходимият характер на това заявление за избраните полети в рамките на ЕС трябва редовно да се преразглежда в съответствие с промените в обстоятелства, които оправдават техния избор.

За целите на предварителната оценка на PNR данните, чиято цел е да се идентифицират лицата, които се нуждаят от допълнителна проверка преди пристигането или заминаването си, която първоначално се извършва чрез автоматизирано обработване, звеното за данни за пътниците (ЗДП) може да сравнява тези данни само с бази данни за търсени лица или предмети или по сигнал. Тези бази данни трябва да бъдат недискриминационни и да се използват от компетентните органи в рамките на тяхната мисия за борба с престъпленията, свързани с тероризъм, и тежката престъпност, които имат обективна връзка, макар и непряка, с въздушния превоз на пътници. Освен това, що се отнася до предварителната оценка с оглед на предварително определените критерии, ЗДП не може да използва технология за изкуствен интелект в системи за самообучение („машинно обучение“), способна да променя без човешка намеса или преглед на процеса на оценяване, и по-специално на критериите за оценка, на които се основава резултатът от прилагането на този процес, както и претеглянето на тези критерии. Тези критерии трябва да бъдат определени по такъв начин, че тяхното прилагане да е насочено по-специално към лица, които биха могли да

---

изискванията за яснота и точност на правото на Съюза. Държавите членки трябва да пропуснат тези PNR елементи при прилагането на директивата. Това е важно, тъй като полето „обща забележка“ може да съдържа чувствителни лични данни, например искания за храна, които косвено разкриват религиозните практики или политическите ориентации на пътника. Вж. също *Mass surveillance of external travellers may go on, says EU's highest court - European Digital Rights (EDRi)*.

бъдат основателно заподозрени в участие в престъпления, свързани с тероризъм, или в тежки престъпления, и да се вземат предвид както „уличаващите“, така и „оневиняващите“ доказателства, като този начин на преценка не трябва да води до пряка или непряка дискриминация<sup>27</sup>.

Като се имат предвид допустимата грешка, присъща на такова автоматизирано обработване на PNR данни, и сравнително значителният брой „фалшиви положителни резултати“, получени в резултат на прилагането им през 2018 г. и 2019 г., целесъобразността на създадената с Директивата система за постигане на преследваните цели зависи основно от правилното функциониране на проверката на положителните резултати, получени при тези операции по обработване, извършвани от ЗДП като втора стъпка чрез неавтоматизирани средства. В това отношение държавите членки трябва да установят ясни и точни правила, които могат да предоставят насоки и подкрепа за анализа, извършван от служителите на ЗДП, отговарящи за този индивидуален контрол, за да се гарантира пълното зачитане на основните права, закрепени в членове 7, 8 и 21 от Хартата, и по-специално гарантиране на единна административна практика в рамките на ЗДП, която спазва принципа на недискриминация. По-специално те трябва да гарантират, че ЗДП установява обективни критерии за преразглеждане, които позволяват на неговите представители да проверяват, от една страна, дали и до каква степен положителното съвпадение („попадение“) засяга ефективно лице, което може да участва в престъпления, свързани с тероризъм, или тежко престъпление, както и, от друга страна, недискриминационния характер на операциите по автоматизирано обработване.

В този контекст Съдът подчертава също, че компетентните органи трябва да гарантират, че заинтересованото лице може да разбере действието на предварително определените критерии за оценка и програми, прилагащи тези критерии, така че да може това лице да реши при пълно познаване на релевантните факти дали да упражни правото си на защита по съдебен ред. По същия начин, в рамките на такъв иск, съдът, натоварен с контрола за законосъобразност на решението, прието от компетентните органи, както и, освен в случай на заплахи за държавната сигурност, самите засегнати лица трябва да са имали възможност да разгледат както всички основания, така и доказателствата, въз основа на които е взето решението, включително предварително определените критерии за оценка и действието на програмите, прилагащи тези критерии. Последващото разкриване и оценка на PNR данните след пристигането или заминаването на

---

<sup>27</sup> Ruling of the CJEU on the implementation of the PNR Directive | ERA (eraa.org).

съответното лице може да се извърши само въз основа на нови обстоятелства и обективни доказателства, които могат да породят основателно подозрение за участие на това лице в тежко престъпление, имащо обективна връзка, дори и косвена, с въздушния превоз на пътници или от които може да се заключи, че тези данни биха могли в дадения случай да допринесат ефективно за борбата с тероризма при престъпления с такава връзка<sup>28</sup>.

Разкриването на PNR данни за целите на такава последваща оценка трябва, като общо правило, освен в случай на надлежно обоснована спешност, да подлежи на предварителен преглед, извършен от съд или от независим административен орган при мотивирано искане от компетентните органи, независимо дали това искане е било подадено преди, или след изтичането на срок от шест месеца след предаването на тези данни на ЗДП.

В съответствие със своето Становище 1/15 Съдът на ЕС като цяло има голямо доверие в различните прегледи за защита на PNR данните от неправомерно използване, както и в наблюдението от страна на длъжностното лице по защита на данните на ЗДП, надзора от страна на националния орган за защита на данните, и в крайна сметка съдебен контрол<sup>29</sup>.

На второ място, Съдът счита, че Директивата за резервационните данни на пътниците във връзка с Хартата не допуска национална правна уредба, която разрешава обработването на PNR данни, събрани в съответствие с тази директива, да се извършва за цели, различни от изрично посочените в член 1, параграф 2 от Директивата.

На трето място, що се отнася до срока на съхранение на PNR данните, Съдът приема, че в случаите, когато липсват индикации за участието и съпричастността на пътниците в терористични престъпления или тежки престъпления, тази уредба „по принцип не изглежда да надхвърля строго необходимото“<sup>30</sup>. За сметка на това петгодишният срок на общо запазване на PNR данните на всички пътници във въздушния транспорт, предвиден в член 12, параграф 3 от Директивата за резервационните данни на пътниците, без да е налице връзка между конкретните PNR данни и целите на Директивата за резервационните данни на пътниците, „води до присъщ риск от непропорционално използване и злоупотреба“<sup>31</sup>. По този начин член 12

---

<sup>28</sup> *Ibidem*.

<sup>29</sup> Repairing the EU Passenger Name Record Directive: the ECJ's judgment in *Ligue des droits humains* (Case C-817/19) – European Law Blog.

<sup>30</sup> Case C-817/19, *Ligue des droits humains ASBL v. Conseil des ministres*, Judgment of the Court (Grand Chamber) of 21 June 2022, ECLI identifier: ECLI:EU:C:2022:491, par. 255.

<sup>31</sup> *Ibidem*, par. 256.

от Директивата за резервационните данни на пътниците във връзка с членове 7 и 8, както и с член 52, параграф 1 от Хартата не допуска национална правна уредба, която предвижда общ срок на съхранение от пет години за такива данни, приложим безразборно за всички пътници във въздушния транспорт. Следователно тълкуването, съответстващо на Хартата, на Директивата за резервационните данни на пътниците „не допуска национална правна уредба, която предвижда общ срок на съхранение от пет години за PNR данните, приложим безразборно за всички пътници във въздушния транспорт“<sup>32</sup>. Обратно, той счита, че през първоначалния шестмесечен период запазването на PNR данните на всички пътници във въздушния транспорт, за които се прилага установената с тази директива система, по принцип не изглежда да надхвърля строго необходимото<sup>33</sup>. В този смисъл, в сравнение със заключението на Генералния адвокат, Съдът на ЕС отчасти зае по-рестриктивна позиция, особено по отношение на два въпроса: (1) по-строги ограничения по отношение на полетите и транспортните операции в рамките на ЕС; (2) по-строг подход към периодите на съхранение<sup>34</sup>.

На четвърто място, Съдът приема, че правото на Съюза не допуска национална правна уредба, която при липсата на действителна и настояща или предвидима терористична заплаха, пред която е изправена съответната държава членка, предвижда система за предаване от въздушните превозвачи и туроператорите, както и за обработване от компетентните органи на резервационните данни на пътниците на всички вътрешни за Съюза полети и транспортни операции, извършвани с други средства в рамките на Съюза, и заминаване от, отиване или транзитно преминаване чрез тази държава членка, за целите на борбата с престъпленията, свързани с тероризъм и с тежка престъпност. В такъв случай прилагането на системата, установена с Директивата за резервационните данни на пътниците, трябва да се ограничи до предаването и обработването на PNR данни за полети и / или транспортни операции, свързани по-специално с определени маршрути или начини на пътуване, или с определени летища, гари или морски пристанища, за които има признаци, които биха обосновавали това прилагане. Освен това Съдът уточнява, че правото на Съюза не допуска национална правна уредба, предвиждаща такава система за предаване и обработване на тези данни за целите на

---

<sup>32</sup> *Ibidem*, пар. 262.

<sup>33</sup> Ruling of the CJEU on the implementation of the PNR Directive | ERA (eraa.org).

<sup>34</sup> CJEU: PNR Directive Valid if Limited to the “Strictly Necessary” – eucrim. За повече подробности вж. Заключение на Генералния адвокат – CONCLUSIONS DE L’AVOCAT GÉNÉRAL M. GIOVANNI PITRUZZELLA présentées le 27 janvier 2022.

подобряването на граничния контрол и борбата с незаконната имиграция.

Европейският комитет по защита на данните (The European Data Protection Board)<sup>35</sup> прави изявление във връзка с постановеното решение на Съда на ЕС (Case C-817/19) относно използването на резервационни данни на пътниците с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и тежки престъпления съгласно Директива (ЕС) 2016/681. Комитетът приема, че изложените в решението на Съда строги ограничения, които трябва да се спазват при транспониране и прилагане на Директивата, значително стесняват начините, по които държавите членки могат да обработват PNR данни. В тази връзка ги призовава да предприемат всички необходими мерки (законодателни и предприети от съответните Звена за информация за пътниците), за да гарантират, че тълкуването и прилагането на Директивата е в съответствие с Хартата на основните права в Европейския съюз, по-специално – с основните права на субектите на данни.

Европейският комитет отбелязва, че настоящите операции по обработване на резервационни данни в много от държавите членки на Съюза не съответстват в цялост на тълкуването на Директивата, постановено от Съда на ЕС, и логично излага своите опасения относно непропорционалното намесване на системите за обработване на резервационни данни в основните права на европейските граждани. Ето защо Комитетът приканва в изявлението си държавите членки да предприемат всички необходими мерки на законодателно и / или административно ниво, за да гарантират, че националното транспониране и съответно прилагане на Директивата за PNR данни на пътниците е в съответствие с Хартата за основни права на ЕС, както е тълкуването на Съда на ЕС.<sup>36</sup>

Използването на резервационни данни на пътниците в качеството им на лични данни винаги следва да бъде с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични и тежки престъпления. Неправомерното използване на лични данни на лица, които не са свързани с престъпни организации,

---

<sup>35</sup> На 25 май 2018 г. започва да работи Европейският комитет по защита на данните. Създаването му е предвидено в разпоредбите на чл. 68 – 76 на ОРЗД. Той заменя работната група по чл. 29 от Директива 95/46/ЕО. Неговата задача е да постигне унифицирано прилагане на законодателството за защита на личните данни в ЕС.

<sup>36</sup> Statement 5/2022 on the implications of the CJEU judgement C-817/19 regarding the implementation of the Directive (EU) 2016/681 on the use of PNR in Member States [https://edpb.europa.eu/system/files/2022-12/edpb\\_statement\\_20221213\\_on\\_the\\_pnr\\_judgement\\_en.pdf](https://edpb.europa.eu/system/files/2022-12/edpb_statement_20221213_on_the_pnr_judgement_en.pdf).

представлява безспорна злоупотреба с право и противоречи на европейското законодателство за защита на личните данни. В този смисъл органите за защита на данните са изцяло компетентни да разследват съответствието на националното право с изискванията на европейското законодателство за защита на данните.

Забележка: Изследването е проведено и финансирано по проект № 101047808 с наименование „European Data Protection: Post pandemic effects and new dimensions“ (EDP-PPEND), който се реализира с финансовата подкрепа на Програма „Еразъм +“ 2021-2027, действие по инициативата „Жан Моне“ в областта на висшето образование.

### Библиография:

1. Белова Г. Европейският съюз и международното право, *сп. „Дипломатия“*, издание на Дипломатическия институт при Министеръта на външните работи, бр. 2/2009, с. 20-37.
2. Белова Г. Защитата на личните данни в рамките на Европейския съюз, *Бюлетин на Асоциацията на прокурорите в България*, бр. 1/2010, с. 124-150.
3. Белова Г., Н. Марин, Г. Георгиева, Й. Кочев *Нови моменти в защитата на личните данни в Европейския съюз*, в: Научни трудове на Института за държавата и правото, 2017, т. XVI, ISSN 1314-6459, с. 54-65. CEEOL - Article Detail
4. Марин, Н., Авг. Янчев *Нарушенията на сигурността на личните данни като основно предизвикателство за националната сигурност*, *сп. „Право, политика, администрация“*, том 8, бр. 2/2021, с. 1-9.
5. Марков, Св. *Директивата за резервационни данни на пътниците – модерен инструмент в борбата с тероризма*, Пол-и-сиг-3-2019-22-29 (1).pdf.
6. Тошкова-Николова, Д., Н. Фети, *Защита на личните данни*. София: ИК „Труд и право“, 2019.
7. Целков, В., Д. Петков, Г. Средков, Пл. Георгиев, *Защита на данните принципи и практики*. София, Нова Звезда, 2019.
8. Anggriawan, Rizaldy, Andi Agus Salim, Yordan Gunawan, and Mohammad Hazyar Arumbinang. “Passenger Name Record Data Protection under EU and US Agreement: Security over Privacy?” *Hasanuddin Law Review* 8 no. 2 (2022): 95-1110. DOI: 10.20956/halrev.v8i2.2844, P-ISSN: 2442-9880, E-ISSN: 2442-9899, 2844-8546-1-PB.pdf.

9. Belova, Gabriela & Gergana Georgieva. “A New Data Protection Development in The EU Judicial and Criminal Area” in: Volume of papers of International conference *Knowledge-Based Organization*, vol.23, no.2, 2017, pp.144-149. <https://doi.org/10.1515/kbo-2017-0103>.

10. Belova, Gabriela & Gergana Georgieva. “Legal, Political and Security aspects of the Pandemic Language” in: Volume of Papers of International conference *Knowledge-Based Organization*, vol.27, no.2, 2021, pp.105-110. <https://doi.org/10.2478/kbo-2021-0056>.

11. Masse, Jean-Pierre. „New EU-US PNR Agreement on the processing and transfer of Passenger Name Record (PNR) data“. Libertysecurity.org. Archived from the original on 12 January 2012.

12. Mendez M. *Opinion 1/15: The Court of Justice Meets PNR Data (Again!)*, EP\_eJ\_2017\_3\_3\_Overview\_Mario\_Mendez\_00176.pdf.