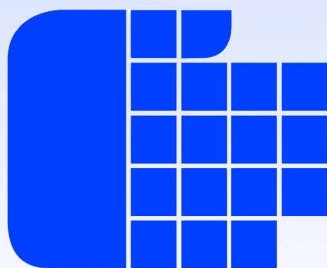


Комисия за Защита на Личните Данни

**ИНФОРМАЦИОНЕН
БЮЛЕТИН**



Брой 3 (90), май 2021 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода март и април 2021 г.)

СЪБИТИЯ И ИНИЦИАТИВИ	3
Комисията за защита на личните данни депозира в Народното събрание отчета за дейността си през 2020 г. Резюме на отчета	3
Заседание на Европейския комитет по защита на данните	7
Заседание на Комитета по чл. 93 от Общия регламент относно защитата на данните	10
ЕКЗД и ЕНОЗД приеха Съвместно становище по предложението за Регламент относно Европейска правна рамка за управление на данните (Акт за управление на данните)	11
Европейската комисия предложи създаването на Цифрово зелено удостоверение	13
ЕКЗД и ЕНОЗД приеха Съвместно становище по предложението за Регламент относно рамката за издаване, проверка и приемане на оперативно съвместими удостоверения за ваксинация, тестване и възстановяване	16
Заседание на Международната работна група по защита на данните в телекомуникациите	17
КОНТРОЛНА ДЕЙНОСТ НА КЗЛД	19
РЕШЕНИЯ НА КЗЛД	20
СТАНОВИЩА НА КЗЛД	31
Приключи студентският конкурс на тема “Личните данни и свободата в дигиталното общество”. Есета от конкурса	35

СЪБИТИЯ И ИНИЦИАТИВИ

КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ДЕПОЗИРА В НАРОДНОТО СЪБРАНИЕ ОТЧЕТА ЗА ДЕЙНОСТТА СИ ПРЕЗ 2020 Г. РЕЗЮМЕ НА ОТЧЕТА



На 30 март 2021 г. Комисията за защита на личните данни депозира в деловодството на Народното събрание Годишния отчет за дейността си през 2020 година. Отчетът се състои от 138 страници, обособени в 12 основни раздела. Депозирани са съгласно чл. 7, ал. 6 от Закона за защита на личните данни и обхваща периода от 01.01.2020 г. до 31.12.2020 г.

В годишния отчет е предоставена информация за основните направления на дейност на КЗЛД през посочения период, като е отчетено обстоятелството, че както и всички останали сфери на обществения живот, така и дейността на КЗЛД е белязана от пандемията от *COVID-19*. Дейността на Комисията е реорганизирана по начин, който да гарантира непрекъсваемост на административните услуги, защита на правата на физическите лица и спазване на противоепидемичните мерки.

В отчета е предоставена информация по разглеждането на жалби и сигнали, контролната дейност, упражняването на корективните правомощия на институцията, производствата по изразяване на становища, участието в съгласувателни процедури на нормативни актове, участието на КЗЛД в механизмите за съгласуваност и сътрудничество в рамките на Европейския комитет за защита на данните, международната дейност на КЗЛД, реализацията на проекти. Дадена е обобщена информация по въпроси, свързани със запитвания на граждани и проведените консултации по тях. Неизменна част от годишния отчет е предоставянето на информация относно наблюдението за сигурността на данните съгласно Закона за електронните съобщения, както и отчет за изпълнение на изискванията по Закона за достъп до обществената информация. Предоставена е и информация за административния капацитет и финансовото състояние на институцията. Направен е анализ на степента на постигане на целите и приоритетите за 2020 г. и са дефинирани целите и приоритетите за 2021 г.

По отношение на **изпълнението на приоритетите за 2020 г.** се отчита приемането на изцяло **нова инструкция за практическото осъществяване на надзорната дейност на КЗЛД**, в обхвата на която влизат както вече утвърдените практики за контрол (по жалби и сигнали, планови и секторни проверки и др.), така и всички нови направления и обекти на контрол (по уведомления за нарушения на сигурността на личните данни по чл. 33 и при предварителни консултации по чл. 36 от Регламент (ЕС) 2016/679, както и при сертифициране или акредитация).

И през 2020 г. КЗЛД продължава да отстоява **постоянния си приоритет за пълноправното членство на България в Шенгенското пространство**

Въпреки трудностите в осъществяването на проверки на място поради усложнената пандемична обстановка във връзка с разпространението на *COVID-19* през 2020 г. Комисията **реализира значителна по обем и обхват надзорна дейност**. За установени нарушения на Регламент (ЕС) 2016/679 и ЗЗЛД в производствата по разглеждане на жалби и сигнали са наложени санкции в общ размер 518 700 лв. Общо събраните приходи в изпълнение на постановени от КЗЛД решения и издадени от председателя на КЗЛД наказателни постановления са 334 855 лв., в т.ч. 102 684 лв., събрани от НАП.

В края на отчетния период продължава да е в ход работата по **финализирането на подзаконовата правна уредба в областта на защитата на личните данни**, която ще продължи и през 2021 г.

В Годишния отчет за 2020 г. е предоставена статистическа информация и е извършен анализ на **разглеждането на жалби на граждани**. Във връзка с осъществяване на задачите и правомощията по Регламент (ЕС) 2016/679 и Закона за защита на личните данни пред Комисията се развива производство по разглеждане на жалби по чл. 38 от ЗЗЛД, включително по механизма за сътрудничество с други надзорни органи.

През 2020 г. Комисията за защита на личните данни е сезирана с над 680 жалби, подадени от физически лица, с твърдения за нарушения при обработване на лични данни и упражняване на права. Забелязва се по-малък брой жалби в сравнение с предходните 2019 и 2018 г., когато броят на жалбите за 2019 г. надвишава 1600, а за 2018 г. е над 780.

Отчита се, че жалбите се отличават с правна и фактическа сложност, включително с намесата на международен елемент, жалбоподатели, които не са български граждани, или администратори на лични данни с основно място на установяване извън територията на Република България, а също и неиндивидуализирани от жалбоподателите ответни страни, най-често администратори на електронни сайтове, обстоятелство, което изисква и сътрудничество с органите на МВР за установяване на последните.

Секторите на дейност на АЛД, срещу които най-често са постъпвали жалби от физически лица през 2020 г. са: видеонаблюдение (159 жалби), държавни органи (62 жалби), банки и кредитни институции (49 жалби), телекомуникации (42 жалби), физически лица (38 жалби), медии (26 жалби), трудови и осигурителни услуги (25 жалби), образование (6 жалби), застраховане (3 жалби), политически субекти (2 жалби).

Наблюдава се тенденция към драстично увеличаване на жалбите срещу осъществявано видеонаблюдение. Ръст бележат и жалбите, подадени срещу банки и дружества, предлагащи кредитни услуги. В тази категория жалби попадат освен твърдения за неправомерно предоставяне на лични данни за събиране на задължения от физическите лица, така и твърдения, свързани с употребата на лични данни за отпускане на кредити, без същите да са поискани и/или усвоени, особено такива, сключени в електронна среда посредством кандидатстване и отпускане на кредити по електронен път.

Отчита се драстично намаляване на жалбите, подадени срещу държавни органи – от 820 през 2019 г. до 62 през 2020 г. Спад бележат и жалбите, подадени срещу администратори в телекомуникационния сектор, които през 2020 г. са 49, почти два пъти по-малко от подадените през 2019 г. 78 жалби.

Забелязва се голям брой жалби (38 на брой), подадени срещу физически лица, насочени предимно срещу разпространение на лични данни в социални мрежи.

От разгледаните през 2020 г. жалби преобладаващ е броят на нарушенията на чл. 6, §1 от ОРЗД – обработване на лични данни без правно основание, както и обработване на личните данни в нарушение на принципите по чл. 5, §1 от ОРЗД – „законосъобразност и добросъвестност“, „свеждане на данните до минимум“, „цялостност и поверителност“ и „точност“. Констатирани са и нарушения, свързани със сигурността на данните и предприетите от администраторите технически и организационни мерки за защита на личните данни, както и такива, свързани с произнасяне по подадени от субекти на данни заявления за упражняване на права или произнасяне извън нормативно определените срокове.

В отчета са представени специфични казуси и практиката на КЗЛД при разглеждането на жалби.

По отношение на **съдебната практика по оспорвани решения на КЗЛД** се отчита, че през 2020 г. по оспорване на издадени от КЗЛД решения по жалби са образувани общо 64 първоинстанционни съдебни дела, първоинстанционният съд се е произнесъл с решения по 74 дела. С 45 съдебни решения са потвърдени оспорените административни актове на КЗЛД, с 10 съдебни

акта решението на КЗЛД е частично отменено или изменено в санкционната част, отменени изцяло са 19 издадени от КЗЛД решения.

През 2020 г. пред Върховния административен съд (ВАС), като касационна инстанция, са образувани 52 дела, ВАС се е произнесъл с решения по 53 дела, като е потвърдил 31 решения на АССГ, с които е оставен в сила издаденият от КЗЛД индивидуален административен акт. Потвърдени са 9 решения на АССГ, с които са отменени съответните решения на КЗЛД. Тринадесет индивидуални административни акта на КЗЛД са частично отменени и върнати в Комисията за ново произнасяне.

Наложените през 2020 г. глоби и имуществени санкции в производството по чл. 38 от ЗЗЛД за установени 76 бр. нарушения на Регламент (ЕС) 2016/679 и на ЗЗЛД са в общ размер на 496 700 лв. Санкциите варират от 100 лв. (за нарушение на чл. 12, §3 от ОРЗД) до 53 000 лв. (за нарушение на чл. 4, ал. 1 от ЗЗЛД (отм.)). Водещи за размера на наложените имуществени санкции/глоби са естеството, тежестта и продължителността на нарушението, целта на съответното обработване, броят на засегнатите субекти на данни и степента на причинената им вреда, категориите лични данни, засегнати от нарушението, действията, предприети от администратора или обработващия лични данни за смекчаване на последиците от вредите, претърпени от субектите на данни, предишни нарушения на санкционираното лице, както и дали нарушителят е физическо или юридическо лице, респективно микро-, малко или средно предприятие. Събраните през 2020 г. суми по постановени решения на КЗЛД са в размер на 327 087 лв., като от тях 101 916 лв. са събрани принудително от Националната агенция за приходите (НАП).

Годишният отчет на КЗЛД предоставя **статистика и обобщена информация по въпроси, имащи отношение към обработването и защитата на личните данни по постъпили запитвания на граждани и предоставена информация и консултация по тях**. През 2020 г. са регистрирани повече от 100 хиляди обаждания на телефоните на институцията, обявени за устни консултации по законодателството за защита на личните данни и за бързи справки по постъпили жалби, сигнали и въпроси. Предоставените през 2020 г. консултации от страна на КЗЛД по традиционните писмени канали за комуникация са 658 бр. Касае се за консултации под формата на писмени отговори на запитвания по поставени въпроси от физически лица за правата им по ЗЗЛД и Регламент (ЕС) 2016/679 и реда за тяхното упражняване и от администратори за техните задължения в областта на защитата на личните данни. Най-често задаваните писмени въпроси са свързани с видеонаблюдението в етажна собственост, случаи на публикуване на лични данни в интернет, включително в търсачки, социални мрежи, онлайн медии и др., директен маркетинг по телефон, поща, имейл или други средства за комуникация. Предоставен е сравнителен анализ на постъпилите запитвания от граждани според предмета на запитванията.

По отношение на **контролната дейност КЗЛД** отчита разработването и утвърждаването на ключови документи, свързани с прилагането на ефективен механизъм за надзор в областта на защитата на личните данни.

От началото на 2020 г. в КЗЛД са постъпили 599 бр. **сигнали, искания и запитвания** по актуални въпроси във връзка с обработването на лични данни и изложени твърдения за нарушения на Регламента и ЗЗЛД. От тях са отработени 598 бр., като на всички податели са изпратени съответни отговори, а при необходимост получените сигнали са изпращани и на съответните органи или институции за произнасяне по компетентност. Най-много запитвания и сигнали са получени срещу органи на държавната администрация – 143 бр. На следващо място са сигнали за евентуално незаконосъобразно обработване на лични данни от администратори на лични данни, предоставящи интернет услуги – 95 бр., последвани от администратори на лични данни, предоставящи услуги и продукти от сферата на банковото дело – 48 бр., за обработване на лични данни посредством изградени системи за видеонаблюдение – 29 бр., както и обработване на лични данни за целите на директния маркетинг – 24 бр., телекомуникации – 32 бр., финанси и счетоводство – 14 бр., човешки ресурси – 13 бр., медии – 17 бр., събиране на вземания – 10 бр., куриерски услуги – 13 бр., образование и обучение – 7 бр., здравеопазване – 17 бр., търговия и услуги – 18 бр., хазарт – 9 бр., и други.

През 2020 г. са назначени 178 бр. **проверки на място** по повод постъпили в КЗЛД жалби, искания и сигнали, от които са извършени 144 проверки, 10 от които по уведомления за нарушаване на сигурността на личните данни с висок риск съгласно чл. 33 от Регламента. Най-голям брой проверки са извършени след постъпили сигнали и жалби от физически лица за обработване на личните им данни посредством изградени системи за видеонаблюдение.

Въз основа на извършените проверки по искания и сигнали са съставени 3 акта за установяване на административни нарушения, издадени са 5 наказателни постановления (НП). Констатираните нарушения по постъпили сигнали, за които КЗЛД е наложила корективни мерки, са общо 36 бр.

В резултат на извършените през отчетния период проверки КЗЛД прави извода, че голяма част от администраторите на лични данни са добре запознати с нормативната база за защита на личните данни, прилагат в голяма степен необходимите технически и организационни мерки за защита на данните, уведомяват физическите лица за техните права, изпълняват задълженията си при упражняване на правата на физическите лица, както и съдействат на КЗЛД при упражняване на нейните правомощия.

През 2020 г. с НП на председателя на КЗЛД са наложени санкции на стойност 87 062,73 лв., събраните приходи по издадени наказателни постановления са 7768 лева, като 768 лв. са събрани принудително от НАП.

В Годишния отчет е предоставена подробна информация относно **производствата по изразяване на становища и участие в съгласувателни процедури на нормативни актове** по въпросите, свързани със защита на личните данни.

Предоставени са **обща статистика и по-интересни случаи от практиката на КЗЛД при изразяване на становища**. Направен е савнителен анализ на исканията за становища според предмета на запитванията и вида на администраторите, които са поискали становище в предходни години и през настоящата. През 2020 г. КЗЛД е изразила становища по различни въпроси, свързани с извънредните обстоятелства, предизвикани от пандемията и борбата с нея – обработване на данни за здравето на служителите си в контекста на пандемията от *COVID-19*; групово тестване на служителите в едно предприятие; видеонаблюдение на пациент/пациенти в болнична стая, хоспитализирани за лечение от *COVID-19*.

През изминалата година КЗЛД участва в **процедури по съгласуване на проекти на нормативни актове**, имащи отношение към въпроси, свързани със защита на личните данни.

През 2020 г. КЗЛД е **конституирана като заинтересована страна в две производства пред Конституционния съд** на Република България.

В отчета е предоставена обща информация и статистика за **участието на КЗЛД в механизмите за съгласуваност и сътрудничество** в рамките на Европейския комитет за защита на данните - участие в заседанията на Комитета и на експертните подгрупи към него, както и обмен на информация през информационната система на Вътрешния пазар.

Международната дейност на КЗЛД през 2020 г. има редица проявления - участия в международни форуми по защита на данните, засилване на участието на експерти от КЗЛД в работата на работни групи в областта на защитата на личните данни на ниво ЕС, участието на КЗЛД в работата на специално създадените съвместни надзорни органи и координационни групи по надзор на широкомащабните информационни системи на ЕС: Комитета за сътрудничество на Европол, Съвместния надзорен орган „Митници“, Координационните надзорни групи на Шенгенската информационна система (ШИС II), Визовата информационна система (ВИС), ЕВРОДАК, Митническата информационна система (МИС) и Информационната система за вътрешния пазар.

Отчетено е подпомагането на изпълнението на целите на КЗЛД **чрез реализация на проекти с национално и международно финансиране**.

Утвърждаването на фигурата на **Длъжностното лице по защита на данните** продължава и през 2020 г. и КЗЛД предоставя в годишния си отчет статистика и анализ на получените уведомления за определени ДЛЗД. През 2020 г. стартира информационната система за поддържане на регистъра на АЛД/ОЛД, определили ДЛЗД.

В своя отчет за 2020 г. КЗЛД предоставя информация за дейността си като **наблюдаващ орган относно сигурността на данните съгласно Закона за електронните съобщения**, като предоставя статистика и анализ на исканията за достъп до трафични данни и на получените протоколи за унищожени трафични данни.

В изпълнение на изискванията по Закона за достъп до обществена информация в Годишния отчет е включен **Отчет за постъпилите заявления за достъп до обществена информация и искания за повторно използване на информация от обществеността за 2020 г.**

Предоставена е подробна информация за **институционалното взаимодействие, информационно-образователната дейност, медийната политика, административния капацитет и финансовото състояние на КЗЛД.**

Годишният отчет на КЗЛД за изминалата 2020 г. завършва с дефинирането на целите и приоритетите за 2021 г.

Годишният отчет на КЗЛД за 2020 г. е публикуван на институционалния сайт – **ТУК**.

ЗАСЕДАНИЕ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ



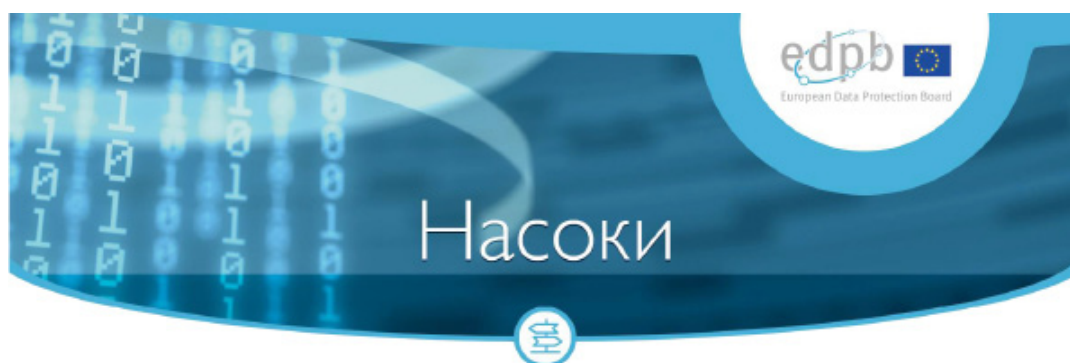
European Data Protection Board

На състоялото се на 10 март 2021 г. заседание Европейският комитет по защита на данните прие Работна програма за периода 2021-2022 г., Декларация относно Регламента за неприкосновеността на личния живот и електронните съобщения, Насоки относно виртуалните гласови асистенти, Насоки относно свързаните превозни средства и обсъди решенията за адекватно ниво на защита на

личните данни на Обединеното кралство, представени от Европейската комисия.

Двугодишна работна програма за периода 2021-2022 г. следва приоритетите, определени в **Стратегията на ЕКЗД за периода 2021-2023 г.**, и ще приложи на практика стратегическите цели на Комитета.

В изявлението относно **проекта за Регламент за неприкосновеността на личния живот и електронните съобщения** се приветства постигнатото от Съвета съгласие по мандата за водене на преговори като положителна стъпка към приключване на обсъжданията по Регламента. ЕКЗД припомня, че надзорът върху спазването на разпоредбите за неприкосновеност на личния живот в бъдещия Регламент следва да бъде възложен на националните органи, отговарящи за прилагането на ОРЗД, за да се осигури хармонизирано тълкуване и прилагане в целия ЕС и да се гарантират еднакви условия в единния цифров пазар. Председателката на ЕКЗД Андреа Йелинек заяви, че Регламентът за неприкосновеността на личния живот и електронните съобщения не трябва при никакви обстоятелства да понижава равнището на защита, предлагано от действащата Директива за правото на неприкосновеност на личния живот и електронни комуникации, и следва да допълва ОРЗД, като предоставя допълнителни силни гаранции за поверителност и защита на всички видове електронни съобщения.



ЕКЗД прие **Насоки относно виртуалните гласови асистенти**, които имат за цел да определят някои от най-значимите предизвикателства пред виртуалните гласови асистенти и да предоставят препоръки на заинтересованите страни относно начините за справяне с тях. Насоките са предоставени за обществена консултация за период от шест седмици – до 23 април 2021 г.

След провеждането на обществена консултация ЕКЗД прие окончателната версия на **Насоките относно свързаните превозни средства**. Акцентът в документа е поставен върху обработването на лични данни във връзка с непрофесионалната употреба на свързани превозни средства от субектите на данни. Окончателната версия включва актуализирани формулировки и допълнителни пояснения, които да отговорят на коментарите и обратната информация, получени по време на обществената консултация.

Прието бе **Съвместно становище на ЕКЗД и ЕНОЗД относно Акта за управление на данните**.

На същото, състояло се на 10 март заседание, Комитетът обсъди получените от Европейската комисия **проекти на решения относно адекватното ниво на защита на данните на Обединеното кралство**.

На състоялото се на 13 април заседание ЕКЗД прие две становища по проектите за решения за адекватност на Обединеното кралство. **Становище 14/2021** се основава на ОРЗД и оценява включените в проекта за решение за адекватност общи аспекти на защитата на данните, както и достъпа на държавни органи до лични данни, прехвърлени от ЕИП за целите на правоприлагането и националната сигурност. Тази оценка се основава на **Референтния документ относно адекватното ниво на защита (WP254)**. **Становище 15/2021** се основава на **Директивата относно правоприлагането в областта на защитата на данните (ДПЗД)** и анализира проекта на решение за адекватност в светлината на **Препоръки 01/2021 относно изискванията за адекватно ниво на защита съгласно ДПЗД**, както и съответната съдебна практика, отразена в **Препоръки 02/2020 г. относно европейските основни гаранции при прилагане на мерките за наблюдение**. Това е първият проект за решение за прилагане на адекватността на трета държава съгласно **Директивата относно правоприлагането в областта на защитата на данните**, представен от Европейската комисия и оценен от ЕКЗД.

Комитетът отбелязва, че има ключови области със силно съответствие между ЕС и Обединеното кралство по отношение на рамките за защита на данните по някои основни разпоредби като: основания за законна и справедлива обработка за легитимни цели; ограничаване на целите; качество на данните и пропорционалност; срокове за запазване на данните, сигурност и поверителност; прозрачност; специални категории данни; автоматизирано вземане на решения и профилиране.

По думите на председателя на ЕКЗД, Андреа Йелинек, „рамката за защита на данните в Обединеното кралство се основава до голяма степен на рамката на ЕС за защита на данните. Законът за защита на данните на Обединеното кралство от 2018 г. допълнително определя прилагането на GDPR в законодателството на Обединеното кралство, в допълнение към транспонирането на **Директивата относно правоприлагането в областта на защитата на данните**, както и предоставяне на правомощия и налагане на задължения на националния надзорен орган за защита на данните

(ICO). Поради това ЕКЗД приема, че Обединеното кралство отразява в по-голямата част от своята рамка за защита на данните Общия регламент за защита на данните и **Директивата относно правоприлагането в областта на защитата на данните**. При анализ на законодателството и практиката, ЕКЗД определя много аспекти като еквивалентни по същество. Въпреки че законите могат да се развиват, това привеждане в съответствие трябва да се запази. Затова приветстваме решението на Комисията да ограничи във времето приемането за адекватност и намерението да следи отблизо развитието в Обединеното кралство.“

Комитетът подчертава, че няколко аспекта трябва да бъдат допълнително оценени и/или внимателно наблюдавани от Европейската комисия във връзка с нейното решение въз основа на ОРЗД, като например:

- Изключения в случаи, свързани с имиграцията, и съответните последици във връзка с ограниченията на правата на субекта на данни;
- Прилагането на ограничения при по-нататъшно предаване на лични данни от ЕИП към Обединеното кралство, например въз основа на бъдещи решения за адекватност, приети от Обединеното кралство, международни споразумения, сключени между Обединеното кралство и трети държави, или дерогации.

Що се отнася до достъпа на държавните органи до лични данни, прехвърлени в Обединеното кралство за целите на националната сигурност, Комитетът приветства създаването на Трибунал за разследване на правомощията (Investigatory Powers Tribunal - IPT) за справяне с предизвикателствата относно прилагането на правото на ефективни правни средства за защита в областта на националната сигурност и въвеждането на Съдебни комисари в Закона за правомощията при разследване от 2016 г., за да се осигури по-добър надзор в тази област. ЕКЗД все още открива редица аспекти, изискващи допълнителни разяснения и/или наблюдение:

- Събиране на огромни количества данни от световния интернет трафик
- Независима оценка и надзор върху използването на автоматизирани инструменти за обработка;
- Гаранции, предвидени в законодателството на Обединеното кралство, когато става въпрос за разкриване в чужбина, по-специално, по отношение на изключенията, свързани с националната сигурност.

На същото заседание Комитетът прие Насоки относно прилагането на член 65, параграф 1, буква а) от ОРЗД, за да очертае основните етапи на процедурата и да изясни компетентността си при приемане на правно обвързващо решение въз основа на член 65, параграф 1, буква а) ОРЗД. Насоките включват и описание на приложимите, процедурно заложи, гаранции и правни средства за защита. Насоките са предмет на обществена консултация за период от шест седмици - до 28 май 2021 г. и са публикувани **ТУК**.

Комитетът прие, след публична консултация, окончателна версия на **Насоките относно таргетиране на потребителите на социални медии**. Целта на насоките е да изясни ролите и отговорностите на доставчиците на социални медии и лицата, обект на таргетиране. Окончателната версия включва актуализирани формулировки, отразяващи коментарите и обратната връзка, получени по време на обществената консултация.

ЕКЗД прие Декларация относно международните споразумения, включващи трансфери, в която приканва държавите-членки на ЕС да оценят и, ако е необходимо, да преразгледат своите международни споразумения, които включват международни трансфери на лични данни и които са сключени преди 24 май 2016 г. (за тези, които имат отношение към ОРЗД) и 6 май 2016 г. (за тези, които имат отношение ДПЗД), и ако е необходимо, да ги приведат в съответствие със законодателството на ЕС за защита на данните.

ЗАСЕДАНИЕ НА КОМИТЕТА ПО ЧЛ. 93 ОТ ОБЩИЯ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ

На 22 март 2021 г. с е състоя заседание на комитета по член 93 от Общия регламент относно защитата на данните, чиито фокус бе представяне и обсъждане на предложенията на Европейската комисия за Решение за изпълнение съгласно Регламент (ЕС) 2016/679 относно адекватното ниво на защита на личните данни от страна на Обединеното кралство Великобритания и Северна Ирландия, както и за Решение за изпълнение съгласно Директива (ЕС) 2016/680 относно адекватното ниво на защита на личните данни от страна на Обединеното кралство.

Участниците в заседанието бяха запознати в детайли със съдържанието на двата проекта на документи, контекста на съпътстващите излизането на Великобритания от ЕС събития, законодателната рамка за защита на личните данни на Обединеното кралство Великобритания и Северна Ирландия (Обединеното кралство, ОК), процес по правоприлагане в ОК, достъп на държавни институции до личните данни, както и мониторинга, срока на действие и подновяване на предложените решения.

Съгласно настоящото Споразумение за търговия и сътрудничество между ЕС и Обединеното кралство (ТСА) сега действащият режим за прехвърляне на данни ще се запази непроменен до края на месец юни 2021 г. Сред условията, поставени на ОК, са:

- Запазване на правилата за защита на данните, основани на правото на ЕС и приложими по време на преходния период;
- Недопускане на упражняването на автономни регулаторни правомощия в сферата на защита на личните данни.

По отношение на законодателната рамка за защита на личните данни на Обединеното кралство беше представено, че международните актове, по които Обединеното кралство е страна (напр. Конвенция 108), заедно с националното законодателство (напр. Закон за човешките права от 1998 г.) са изключително важен елемент от оценката, на която се основават двете проекторешения. Прилагането на правото на Съюза, а оттам и на ОРЗД, се гарантира от инкорпорираното му в националното законодателство на ОК чрез EU Withdrawal Act 2018 (EUWA). По отношение гарантиране прилагането на разпоредбите на Директива (ЕС) 2016/680 се прилага националния Закон за защита на личните данни, както и Раздел 3 на EUWA. Следва да се отбележи, че гореспоменатите разпоредби се разглеждат от националния съд при спазване принципите на Съюза и практиката на Съда на Европейския съюз. При подготовката на проекторешения са взети предвид насоки, препоръки, вкл. приетите от Информационния комисар по защита на данните (ICO).

Във връзка с прегледа на националната система от институции за защита на личните данни беше обърнато специално внимание на ефективните административни и съдебни процедури, вкл. обезщетения за вреди, както и на правомощията на ICO, като беше подчертано, че Офисът на Информационния комисар има правомощия независимо да осъществява:

- наблюдение на правилата за защита на личните данни;
- пълна гама от разследващи правомощия;
- пълна гама от корективни правомощия, вкл. налагането на административни глоби.

Специално внимание беше отделено на достъпа на националните административни органи до данни, предадени от ЕС, за целите на правоприлагането и националната сигурност. Подчертано бе, че проекторешението отразява последните решения на Съда на ЕС, вкл. решението на „Schrems II”. Сред основните критерии за оценката са:

- Качеството и яснотата на приложимата национална правна рамка (обхват, ограничения от значение за правото на защита на личните данни);

- Необходимостта и пропорционалността на мерките (вкл. предпазни мерки срещу риска от злоупотреба с данни);

- Ефективна съдебна защита: упражняване на права срещу административни органи пред независим и безпристрастен съд (по-конкретно за упражняване правото на достъп, коригиране и изтриване на данни).

Подчертано бе, че националната система от правила за защита на данните на Обединеното кралство се уповава силно на стандартите за необходимост и пропорционалност и има възможност за предварително разрешение от независим съд, включително чрез достъп на субектите на данни за упражняване на права. Обработването на лични данни от страна на правораздавателните, както и на разузнавателните органи е обект на подробен режим за защита на данните. Обединеното кралство прилага разпоредбите на Европейска конвенция за защита правата на човека и основните свободи и се придържа към практиката на Европейския съд по правата на човека по отношение на националната сигурност и неприкосновеността на личния живот, като по този начин следва същите правни стандарти както всяка държава членка на ЕС.

Участниците в заседанието бяха уверени от представителите на ЕК, че Комисията ще продължи да наблюдава развитието на съотносимото законодателство и практика в Обединеното кралство. Беше подчертана възможността за ограничаване във времето на действието на проекторешението – до 4 години след приемането му, както възможността за инициране на процес по приемане на последващо не по-късно от 6 месеца преди изтичането на 4-годишния период на действие (предвидена е т. нар. „Sunset clause”). Обединеното кралство има ангажимент да прилага механизъм по „демонстриране на адекватност“ (adequacy findings) в рамките на четиригодишния период.

По отношение на процедурата и следващите стъпки беше отбелязано, че в средата на месец февруари е иницирана консултация с Европейския комитет по защита на данните (ЕКЗД), като се очаква становището на ЕКЗД до 19 април 2021 г.¹ След приемането му ще бъде стартиране на процедура по разглеждане от страна на държавите членки на ЕС в настоящия формат, като планираният срок за приключване ѝ е края на месец май 2021 г. Приемането на двете проекторешения се планира за началото на месец юни 2021 г.

ЕКЗД И ЕНОЗД ПРИЕХА СЪВМЕСТНО СТАНОВИЩЕ ПО ПРЕДЛОЖЕНИЕТО ЗА РЕГЛАМЕНТ ОТНОСНО ЕВРОПЕЙСКА ПРАВНА РАМКА ЗА УПРАВЛЕНИЕ НА ДАННИТЕ (АКТ ЗА УПРАВЛЕНИЕ НА ДАННИТЕ)

Европейският комитет по защита на данните (ЕКЗД) и Европейският надзорен орган по защита на данните (ЕНОЗД) приеха **Съвместно становище по предложение на Европейския парламент и на Съвета за Регламент относно европейска рамка за управление на данните** (Акт за управление на данните). Целта на **предложения Акт за управление на данните** е да се насърчи наличността на данни чрез увеличаване на доверието в посредниците на данни и чрез укрепване на механизмите за обмен на данни в целия ЕС. По-специално, с Акта за управление на данните се възнамерява насърчаване на наличието на данни от публичния сектор за повторна употреба, споделяне на данни между предприятията, позволяване използването на лични данни с помощта на „посредник за споделяне на лични данни“, както и позволяване използването на данни за алтруистични цели.

¹ На състоялото се на 13 април заседание ЕКЗД прие две становища – 14/2021 и 15/2021, отразени във втория материал на настоящия бюлетин



ЕКЗД и ЕНОЗД приемат законната цел на Акта за управление на данните да подобри условията за обмен на данни на вътрешния пазар. В същото време защитата на личните данни е съществен и неразделен елемент на доверието в цифровата икономика. В съвместното становище ЕКЗД и ЕНОЗД приканват съзаконодателите да гарантират, че бъдещият Акт за управление на данните е напълно в съответствие със законодателството на ЕС за защита на личните данни, като по този начин се укрепва доверието в цифровата икономика и се поддържа предвидено в законодателството на ЕС ниво на защита, под надзора на надзорните органи на държавите-членки на ЕС.

В прессъобщение относно съвместното становище, председателят на ЕКЗД, Андреа Йелинек заявява: „Правната рамка на ЕС за защита на данните не пречи на развитието на икономиката, основана на данните. Точно обратното подпомага го: доверието във всякакъв вид споделяне на данни може да бъде постигнато само при спазване на съществуващите правила за защита на данните. Общият регламент относно защита на данните (ОРЗД, GDPR) е основата, върху която трябва да се изгради европейският модел за управление на данните. Ето защо подчертаваме необходимостта да се осигури съгласуваност с ОРЗД по отношение на компетенциите на надзорните органи, ролите на различните субекти, правното основание за обработка на лични данни, необходимите гаранции за защита и упражняването на правата на субектите на данни.“

В същото прессъобщение Вийчех Виевиоровски, ЕНОЗД, заявява: „Ние разбираме нарастващото значение на данните за икономиката и обществото, както е посочено в Европейската стратегия за данни. Въпреки това, „големите данни пораждаат голяма отговорност“, следователно трябва да се предвидят подходящи мерки за защита на данните. Всеобхватната рамка за европейските пространства за данни трябва да гарантира, че достиженията на ЕС в областта на защитата на данните не са засегнати. „

ЕКЗД и ЕНОЗД считат, че законодателят на ЕС трябва да гарантира, че формулировките на Акта за управление на данните ясно и недвусмислено няма да засегнат защитата на личните данни на физическите лица, нито ще променят каквито и да е права и задължения, посочени в законодателството за защита на данните.

По отношение на повторната употреба на лични данни, съхранявани от органи от публичния сектор, ЕКЗД и ЕНОЗД препоръчват Актът за управление на данните да се приведе в съответствие със съществуващите правила за защита на личните данни, заложи в Общия регламент относно защитата на данните, както и с Директивата за отворените данни. Освен това следва да се изясни, че повторната употреба на лични данни, съхранявани от органи от публичния сектор, може да бъде разрешена само ако това е основано на законодателството на ЕС или на държава-членка. Тези закони трябва да включват списък на ясни съвместими цели, за които по-нататъшната обработка може да бъде законно разрешена, или представлява необходима и пропорционална мярка в демократичното общество за защита на целите, посочени в член 23 от ОРЗД.

По отношение на доставчиците на услуги за споделяне на данни, съвместното становище подчертава необходимостта да се осигури предварителна информация и контрол за физическите лица, като се вземат предвид принципите на защита на данните при проектиране и по подразбиране,

прозрачност и ограничаване на целите. Освен това трябва да бъдат изяснени условията, при които такива доставчици на услуги биха подпомогнали ефективно лицата при упражняване на техните права като субекти на данни.

Що се отнася до алтруизма по отношение на данните, ЕКЗД и ЕНОЗД препоръчват Актът за управление на данните да определи по-добре целите от общ интерес на такъв „алтруизъм по отношение на данните“. Алтруизмът по отношение на данните трябва да бъде организиран по такъв начин, че да позволява на хората лесно да дават, но и да оттеглят своето съгласие.

В светлината на възможните рискове за субектите на данни, когато техните лични данни могат да бъдат обработвани от доставчици на услуги за споделяне на данни или организации за алтруистично споделяне на данни, ЕКЗД и ЕНОЗД считат, че декларативните режими за регистрация на тези субекти, както са определени в Актът за управление на данните, не предвиждат за достатъчно строга процедура за проверка, приложима за такива услуги. Ето защо препоръчват да се проучат алтернативни процедури, които предвиждат по-систематично включване на инструменти за отчетност, по-специално спазването на кодекс за поведение или механизъм за сертифициране.

Съвместното становище включва също препоръки относно определянето на надзорните органи като основни компетентни органи за контрол на спазването на разпоредбите на Актът за управление на данните, при консултация с други съответни секторни органи.

ЕВРОПЕЙСКАТА КОМИСИЯ ПРЕДЛОЖИ СЪЗДАВАНЕТО НА ЦИФРОВО ЗЕЛЕНО УДОСТОВЕРЕНИЕ



С цел спазване на мерките за ограничаване на разпространението на коронавируса, пътуващите в ЕС са задължени да предоставят различни документи като медицински удостоверения, резултати от тестове и декларации. Липсата на стандартизирани формати доведе до проблеми за пътниците при придвижването им в рамките на ЕС. Докладвано бе и за фалшиви или подправени документи.

В изявлението си, прието след неформалните видеоконференции от 25 и 26 февруари 2021 г., членовете на Европейския съвет призоваха за продължаване на работата по общ подход спрямо удостоверенията за ваксинация. Комисията работи с държавите членки в рамките на [мрежата за електронно здравеопазване](#) - доброволна мрежа, свързваща националните органи, отговарящи за електронното здравеопазване, по подготовката на оперативната съвместимост на удостоверенията за ваксинация. На 27 януари бяха приети насоки, които бяха [актуализирани на 12 март](#), като на същата дата бе приет [проектът на рамката за доверие](#).

На 17 март 2021 г. Европейската комисия прие [законодателно предложение за създаване на обща рамка за цифрово зелено удостоверение](#). Комисията прие също така допълнително предложение, за да се гарантира, че цифровото зелено удостоверение се издава също и на граждани на държави извън ЕС, които пребивават в държавите членки или в асоциираните към Шенген държави, както и на посетители, които имат право да пътуват до други държави членки. Поради правни причини са необходими отделни предложения за обхващане на граждани на ЕС и на граждани на държави извън ЕС, като за целите на удостоверенията няма разлика в третирането на граждани на ЕС и на отговарящи на условията граждани на държави извън ЕС.

Във връзка с това, на 17 март 2021 г. Европейската комисия публикува следното прессъобщение:

„Днес Европейската комисия предлага създаването на цифрово зелено удостоверение за улесняване на безопасното свободно движение на гражданите в рамките на ЕС по време на пандемията от COVID-19. Цифровото зелено удостоверение ще представлява доказателство, че дадено лице е било ваксинирано срещу COVID-19, е получило отрицателен резултат от теста или е преболедувало COVID-19. То ще бъде налично безплатно в електронен формат или на хартиен носител. Ще включва QR код за гарантиране на сигурността и автентичността на удостоверението. Комисията ще създаде портал с цел да се гарантира, че всички удостоверения могат да бъдат проверявани навсякъде в ЕС, както и ще съдейства на държавите членки при техническото изпълнение на удостоверенията. Държавите членки продължават да носят отговорност за решаването кои ограничения, свързани с общественото здраве, могат да бъдат отменени за пътуващите, но ще трябва да прилагат тази отмяна по същия начин за пътниците, притежаващи цифрово зелено удостоверение.

Заместник-председателят на Комисията по въпросите на ценностите и прозрачността Вера Йоурова заяви: *Цифровото зелено удостоверение предлага общоевропейско решение за гарантиране, че гражданите на ЕС се възползват от хармонизиран цифров инструмент в подкрепа на свободното движение в ЕС. Това е добро послание в подкрепа на възстановяването. Основните ни цели са да осигурим лесен за използване, недискриминационен и сигурен инструмент, който изцяло зачита защитата на данните. Продължаваме да работим за международно сближаване с други партньори.*

Комисарят по въпросите на правосъдието Дидие Рейндерс каза: *Благодарение на цифровото зелено удостоверение ще постигнем европейски подход, за да се гарантира, че гражданите на ЕС и членовете на техните семейства могат да пътуват безопасно и при минимални ограничения това лято. Цифровото зелено удостоверение няма да бъде предварително условие за свободно движение и няма да води до дискриминиране по никакъв начин. Общоевропейският подход ще спомогне не само за постепенното възстановяване на свободното движение в рамките на ЕС, но и за избягване на фрагментирането. Той е също така възможност за оказване на влияние върху световните стандарти и за даване на пример, основан на нашите европейски ценности като защитата на данните.*

Основни елементи на регламента, предложен днес от Комисията:

1. Достъпни и сигурни удостоверения за всички граждани на ЕС:

- **Цифровото зелено удостоверение ще обхваща три вида удостоверения** – удостоверения за ваксинация, удостоверения за направен тест (NAAT/RT-PCR тест или бърз тест за антигени), и удостоверения за лицата, преболедували COVID-19.

- **Удостоверенията се издават в електронен формат или на хартиен носител.** И при двете версии ще е налице QR код, който ще съдържа необходимата ключова информация, както и цифров подпис, гарантиращ автентичността на удостоверението.

- **Комисията ще създаде портал** и ще съдейства на държавите членки да разработят софтуер, който органите могат да използват за проверка на всички удостоверения навсякъде в ЕС. Личните данни на притежателите на удостоверение не преминават през портала, и не се запазват от проверяващата държава членка.

- **Удостоверенията ще бъдат достъпни безплатно** и на официалния език или езици на издаващата държава членка и на английски език.

2. Недискриминация:

- **Всички граждани — ваксинирани и неваксинирани, следва да се възползват от цифрово зелено удостоверение**, когато пътуват в ЕС. С цел избягване на дискриминация на лицата, които не са ваксинирани, Комисията предлага да се създаде не само оперативно съвместимо удостоверение за ваксинация, но също и удостоверения за направен тест за COVID-19 и удостоверения за лица, които за преболедували COVID-19.

- **Едни и същи права за пътуващите с цифрово зелено удостоверение** - когато държавите членки приемат доказателство за ваксинация, за да отменят някои ограничения, свързани с общественото здраве, като тестване или поставяне под карантина, от тях ще се изисква да приемат при същите условия удостоверения за ваксинация, издадени в рамките на системата за „цифрово зелено удостоверение“. Това задължение ще бъде ограничено до ваксини, които са получили **валидно в ЕС разрешение за търговия**, но държавите членки могат да решат да приемат допълнително и други ваксини.

- **Уведомяване за други мерки** - ако държава членка продължава да изисква от притежателите на цифрово зелено удостоверение да останат под карантина или да се тестват, тя трябва да уведоми Комисията и всички останали държави членки, както и да обоснове причините за такива мерки.

3. Само съществена информация и защитени лични данни:

- **Удостоверенията ще включват ограничен набор от информация** като име, дата на раждане, дата на издаване, релевантна информация за ваксината/теста/преболедването и уникален идентификатор на удостоверението. Тези данни могат да бъдат проверени само за да се потвърди или провери автентичността и валидността на удостоверенията.

Цифровите зелени удостоверения ще бъде валидни във всички държави — членки на ЕС, както и отворени за използване за Исландия, Лихтенщайн, Норвегия и Швейцария. Цифровото зелено удостоверение следва да се издава на граждани на ЕС и на членове на техните семейства без значение националността им. То следва да се издава и на граждани на държави извън ЕС, които пребивават в ЕС и на посетители, които имат право да пътуват до други държави членки.

Системата за „цифрово зелено удостоверение“ е временна мярка. Тя ще бъде прекратена след като Световната здравна организация (СЗО) обяви края на извънредната ситуация в областта на общественото здраве, свързана с COVID-19.

Следващи стъпки

За да бъде готова преди лятото, предложението трябва да бъде прието бързо от Европейския парламент и от Съвета.

Успоредно с това държавите членки трябва да изпълнят **рамката за доверие** и техническите стандарти, договорени в рамките на мрежата за електронно здравеопазване, да гарантират навременното прилагане на цифровото зелено удостоверение, тяхната оперативна съвместимост и пълното съответствие със законодателството за защита на личните данни. Целта е техническата работа и предложението да приключат през следващите месеци.“

**ЕКЗД И ЕНОЗД ПРИЕХА СЪВМЕСТНО СТАНОВИЩЕ
ПО ПРЕДЛОЖЕНИЕТО ЗА РЕГЛАМЕНТ ОТНОСНО РАМКата ЗА ИЗДАВАНЕ,
ПРОВЕРКА И ПРИЕМАНЕ НА ОПЕРАТИВНО СЪВМЕСТИМИ УДОСТОВЕРЕНИЯ
ЗА ВАКСИНАЦИЯ, ТЕСТВАНЕ И ВЪЗСТАНОВЯВАНЕ**

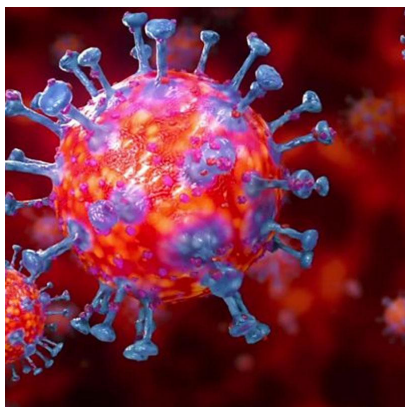


Европейският комитет по защита на данните (ЕКЗД) и Европейският надзорен орган по защита на данните (ЕНОЗД) приеха **Съвместно становище относно предложенията на Европейската комисия за цифрово зелено удостоверение**, чиято цел е да се улесни упражняването на правото на свободно движение в рамките на ЕС по време на пандемията от COVID-19 чрез установяване на обща рамка за издаване, проверка и приемане на оперативно съвместими удостоверения за ваксинация, тестване и пребулдуване от COVID-19. Становището е публикувано на 31 март 2021 г.

Със съвместното становище ЕКЗД и ЕНОЗД приканват съзаконодателите да гарантират, че цифровото зелено удостоверение е напълно в съответствие със законодателството на ЕС за защита на личните данни. Органите по защита на данните от всички държави от ЕС и Европейското икономическо пространство подчертават необходимостта от намаляване на рисковете за основните права на гражданите и живеещите в ЕС, които могат да произтекат от издаването на цифрово зелено удостоверение, включително възможните непредвидени повторни употреби. ЕКЗД и ЕНОЗД подчертават, че използването на цифрово зелено удостоверение не трябва по никакъв начин да води до пряка или непряка дискриминация на физически лица и трябва да бъде напълно в съответствие с основните принципи за необходимост, пропорционалност и ефективност. Предвид естеството на мерките, предложени в предложението, ЕКЗД и ЕНОЗД считат, че въвеждането на цифрово зелено удостоверение следва да бъде придружено от изчерпателна правна рамка.

Андреа Йелинек, председател на ЕКЗД, заявява: „Цифровото зелено удостоверение, което се приема във всички държави-членки, може да бъде основна стъпка напред във възобновяване на пътуванията в ЕС. Всяка мярка, приета на национално или европейско ниво, която включва обработка на лични данни, трябва да зачита общите принципи за ефективност, необходимост и пропорционалност. Ето защо ЕКЗД и ЕНОЗД препоръчват всяко по-нататъшно използване на цифрово зелено удостоверение от държавите-членки да има подходящо правно основание в държавите-членки и да бъдат предвидени всички гаранции.“

Войчех Виевиоровски, ЕНОЗД, заявява: „Трябва да е ясно, че предложението не позволява и не трябва да води до създаването на каквато и да е централна база данни с лични данни на ниво ЕС. Освен това трябва да се гарантира, че личните данни не се обработват по-дълго от строго необходимото и че достъпът и използването на тези данни не е разрешен след приключване на пандемията. Винаги съм подчертавал, че мерките, предприети в борбата срещу COVID-19, са временни и наш дълг е да гарантираме, че те не са тук, за да останат след кризата.“



В своето становище ЕКЗД и ЕНОЗД настояват в настоящата извънредна ситуация, причинена от пандемията от COVID-19, да се спазват принципите на ефективност, необходимост, пропорционалност и недискриминация. Двата органа подчертават, че към момента са налице малко научни доказателства, че ваксинирането срещу COVID-19 (или преболедуването от COVID-19) осигурява имунитет, както и продължителността на този имунитет. Въпреки това, научни доказателства се появяват ежедневно. Освен това редица фактори все още са неизвестни за ефикасността на ваксинацията по отношение на намаляване разпространението на заразата. Предложението трябва да установи ясни и точни правила, регулиращи обхвата и прилагането на цифровото зелено удостоверение, и да наложи подходящи предпазни мерки. Това ще даде достатъчни гаранции на лицата, чиито лични данни са засегнати, че ще бъдат защитени по ефективен начин срещу риска от потенциална дискриминация.

В становището се заявява, че предложението трябва изрично да включва твърдението, че не е разрешен достъпът до и последващото използване на лични данни от държавите-членки на ЕС след приключване на пандемията. В същото време ЕКЗД и ЕНОЗД подчертават, че прилагането на предложената регулация трябва да бъде строго ограничено до настоящата криза от COVID-19.

Съвместното становище включва конкретни препоръки за допълнителни разяснения относно засегнатите от предложението категории данни, съхранението на данните, задължения за прозрачност и идентифициране на администраторите и обработващите лични данни.

ЗАСЕДАНИЕ НА МЕЖДУНАРОДНАТА РАБОТНА ГРУПА ПО ЗАЩИТА НА ДАННИТЕ В ТЕЛЕКОМУНИКАЦИИТЕ

Международната работна група по защита на личните данни в телекомуникациите (позната още като Берлинска група) включва представители на органите за защита на данните и международни организации от целия свят, занимаващи се с въпросите на неприкосновеността на личния живот. Тя е основана през 1983 г. в рамките на Международната конференция на защита на личните данни и неприкосновеността на личния живот по инициатива на берлинския комисар по защита на данните. Членове на Групата са както специалисти в областта на високите технологии, така и юристи, тъй като работата на Групата има както технологичен, така и правен аспект.

На 24 март 2021 г. се състоя 67-то, дистанционно заседание на Международната работна група по защита на личните данни в телекомуникациите. Участваха 38 представители на надзорните органи по защита на данните на държави членки на Европейския съюз, международни организации, държавни органи и неправителствени организации от Европа, Азия и Северна Америка.

На заседанието бе представен националният опит в периода от предходното заседание в края на 2019 г. Българският представител запозна участниците с дейностите на КЗЛД, свързани с прилагането на ефективни надзорни механизми, извънредно нарасналият брой на уведомления за нарушенията на сигурността и главните причини за тях, както и дейностите на Комисията по прилагане на мерки за повишаване на осведомеността и предоставяне на разяснения за съвременната законодателна рамка за защитата на личните данни. Бе поставен акцент върху непрекъсваемостта на дейността на Комисията и последователното прилагане на ефективни механизми за надзор чрез актуализирането на Инструкцията за практическото осъществяване на надзорната дейност на КЗЛД, Методиката за определяне нивото на риска при нарушения на сигурността на личните данни и Въпросника за извършване на проверки при осъществяване на надзорната дейност на КЗЛД. Изтъкнат бе извънредно

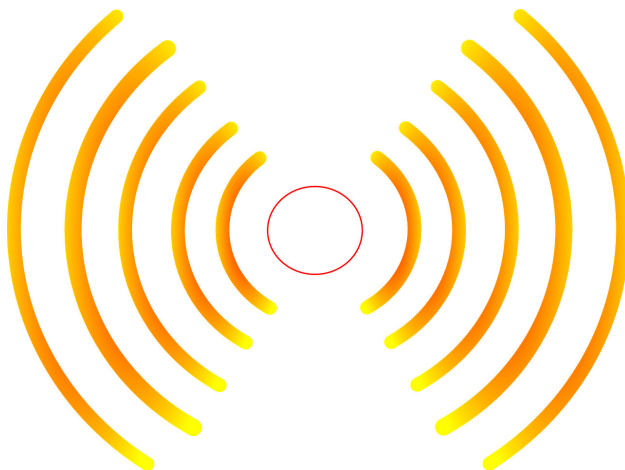
нарасналият брой на уведомления за нарушенията на сигурността и главните причини за тях, между които използването на несъвременен софтуер, непроверени приложения по отношение на сигурността, както и хакерските атаки, като част от все по-набиращото сила предизвикателство пред националните органи по защита на данните – кибер сигурността. Бяха представени и дейностите на Комисията по отношение на повишаване на информираността относно законодателната рамка по защита на данните, като специално място бе отделено на признанието от страна на бизнеса – КЗЛД е победител в категорията „Публична администрация” на конкурса „Наградите на Българската асоциация по информационни технологии” за 2019 г.

На заседанието бяха разисквани въпроси, свързани с прилагането на мерки за ограничаване разпространението на Covid-19. Националните делегации запознаха останалите участници основно с разработените мобилни приложения за проследяване разпространението на заболяването, както и с предизвикателствата пред защитата на данните, включително на специалните категории лични данни. Независимо от избора на централизирана или децентрализирана архитектура за изграждане на националните мобилни приложения, в голямата си част участниците потвърдиха, че са извършили предварителни консултации, тъй като обществените оценки на въздействието върху защитата на данните са показали, че планираното обработване поражда висок риск. Всички участващи потвърдиха, че на териториите на техните държави подобни мобилни приложения се използват само доброволно.

Обсъдено бе предложението за съдържание на работния документ на Групата за сензорните мрежи (sensor networks). В детайли бяха представени отделните части на документа, сред които кратко описание на технологията, връзката ѝ със защитата на личните данни, произтичащите рискове за неприкосновеността на личния живот, както и препоръки към администраторите, разработчиците и регулаторите. Сред основните рискове бяха посочени прекомерното събиране на данни, липсата на прозрачност при обработването на данни, възможната липса на контрол, препятствията пред демонстрирането на отчетност, незаконосъобразно обработване на данни, неадекватно ниво на защита, както и непозволеното повторно обработването на данни. Следвайки правилата на Групата, съдържанието на работния документ ще бъде предложено за приемане чрез писмена процедура.

Представена бе детайлна информация за дейността по подготовка на работния документ относно гласово контролираните устройства (voice-controlled devices). Необходимостта от разработване на работен документ по тази тема бе обсъждана на предходното 66-то заседание на Групата, а първите обсъждания по темата са осъществени в началото на 2020 г. Отбелязано бе, че работата по документа не продължава ритмично поради предизвикателствата, наложени от разпространението на Covid-19, и бяха обсъдени варианти за по-нататъшни действия, включително прекратяване на разработването на такъв документ поради наличието на Насоки относно виртуалните гласови асистенти на Европейския комитет по защита на данните.

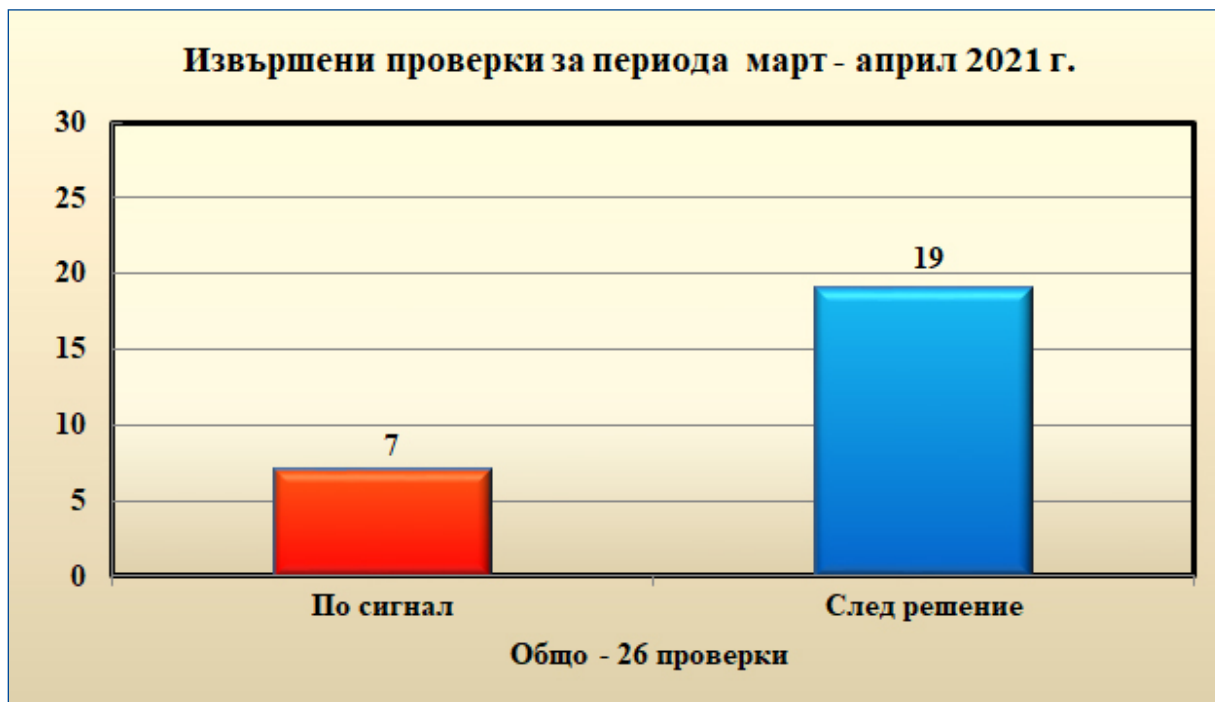
Сред обсъдените теми за разработване на работни документи бяха „умните градове”, лицевото разпознаване, блокчейн технологията, както и квантова изчислителна техника и сигурност.



КОНТРОЛНА ДЕЙНОСТ

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА МАРТ - АПРИЛ 2021 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. през месеците март и април 2021 г. са извършени общо 26 проверки – 7 след постъпили в КЗЛД сигнали и 19 след решение на КЗЛД.



Разгледани са 54 искания, включително различни запитвания по актуални въпроси, относно защита на физическите лица във връзка с обработването на лични данни. На всички податели са изпратени съответни отговори, а когато е необходимо са изпращани и на съответните органи или институции, за отношение по компетентност.

Във връзка с констатации, че с определени операции по обработване на лични данни са нарушени разпоредби на регламента, за отчетния период КЗЛД е упражнила корективни правомощия по чл. 58, § 2 от Регламент (ЕС) 2016/679, като на съответните администратори на лични данни са издадени 6 Разпореждания и са отправени 19 Предупреждения и 1 Официално предупреждение.

РЕШЕНИЯ ПО ЖАЛБИ

КЗЛД публикува в своя бюлетин и на институционалния си сайт решения по жалби, с цел да се осигури прозрачност за обществеността относно практиката на Комисията при разглеждането на жалби на граждани. За постигането на тази цел не е необходимо публикуване на всички решения на КЗЛД по жалби, а отразяване произнасянето на Комисията по различни казуси. Всички публикувани решения на КЗЛД са с анонимизирани лични данни на физическите лица и голяма част от имената на юридическите лица.

РЕШЕНИЕ № ППН-01-574/2020 София, 17.03.2021 г.

Комисията за защита на личните данни („Комисията”/„КЗЛД”) в състав: Председател – Венцислав Караджов и членове – Цанко Цолов и Мария Матева, на редовно заседание, проведено на 17.02.2021 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни във връзка с чл. 57, параграф 1, буква „е” от Регламент 2016/679, разглежда жалба № ППН-01-574/10.08.2020 г., подадена от М.С.

Административното производство е по реда на чл. 38 от Закона за защита на личните данни (ЗЗЛД).

Жалбоподателката посочва, че на 15.07.2020 г. в заседание по гр.д. *** по описа на Районен съд Асеновград, по което е ответник, ищецът Б.Т. представил удостоверение, отразяващо нейните задгранични пътувания.

Удостоверението от 11.06.2020 г. на сектор „Български документи за самоличност“ при ОДМВР Пловдив е издадено на Б.Т. като ответник по дело ***** по описа на Районен съд Пловдив. Справка по това дело установила, че жалбоподателката и Б.Т. не са страни по него.

Г-жа М.С. моли за съдействие, за да бъде установено кой, защо и на какво основание е използвал личните ѝ данни, за да бъде издадено въпросното удостоверение.

В условията на залегалото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството е уведомен заинтересованият орган – министърът на вътрешните работи, който е администратор на лични данни по смисъла на ЗМВР. Предоставена е възможността по чл. 34, ал. 3 АПК за изразяване на становище с относими доказателства по предявените в жалбата твърдения.

Представител на министъра посочва, че на 10.06.2020 г. в сектор „Български документи за самоличност“ при ОДМВР Пловдив е подадено заявление от Б.Т. за издаване на удостоверение с данни от информационните фондове на МВР.

В заявлението се посочва, че г-н Б.Т. желае да му бъде издадено удостоверение, от което да е видно какви задгранични пътувания е извършила г-жа М.С. в периода от 2018 г. до настоящия момент. При подаване на заявлението си г-н Б.Т. представил удостоверение № *****, издадено от РС Асеновград, което му дава право да получи информацията. Видно от съдебното удостоверение, Б.Т. е ищец по гр.д. № ***, по което е страна и жалбоподателката.

Сектор „Български документи за самоличност“ при ОДМВР Пловдив издала приложеното към жалбата удостоверение. При изготвянето му е допусната явна фактическа грешка като е записано гр.д. ***** на РС Пловдив, вместо действителното гр.д. *** на РС Асеновград.

На основание чл. 34, ал. 3 от АПК на жалбоподателя също е предоставена възможността да се запознае с изразеното от ответната страна становище и представените доказателства. Предоставен е срок за изразяване на становище, правене на възражение или искане. В законоустановения срок не постъпи становище.

При така установеното КЗЛД разгледа жалбата, като установи следното:

Разглежданата жалба е съобразена с изискванията за редовност по чл. 29 от АПК, чл. 38, ал. 2 от ЗЗЛД и по чл. 28, ал. 1 от Правилник за дейността на Комисията за защита на личните данни и нейната администрация (ПДКЗЛДНА) – налице са данни за жалбоподателя; естество на искането; дата на узнаване на нарушението; лице, срещу което се подава жалбата; дата и подпис.

Жалбата е процесуално допустима – подадена в срока по чл. 38, ал. 1 от ЗЗЛД от субект на данни с правен интерес. Същата има за предмет твърдение за нарушаване на права по Регламент 2016/679 или ЗЗЛД. С жалбата е сезиран компетентен да се произнесе орган – Комисията за защита на личните данни, която съгласно правомощията си по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е” от Регламент 2016/679 разглежда жалби, подадени от субекти на данни. Налице са предпоставките за допустимост и по чл. 27, ал. 2 от АПК.

Комисията за защита на личните данни е независим надзорен орган, който осъществява защита на лицата при обработване на техните лични данни и при осъществяване на достъпа до тези данни, както и контрола по спазване на 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 (накратко „Регламента” или Регламент 2016/679) и Закона за защита на личните данни (ЗЗЛД). Една от задачите на КЗЛД по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е” от Регламент 2016/679 е да разглежда жалби, подадени от субекти на данни, и да разследва предмета на жалбата, доколкото това е целесъобразно. Целесъобразността при разглеждане на жалбите е процесуално развита в чл. 38, ал. 4 ЗЗЛД – когато жалбата е очевидно неоснователна или прекомерна, с решение на Комисията жалбата може да бъде оставена без разглеждане.

С Регламент 2016/679 и Закона за защита на личните данни (ЗЗЛД) се определят правилата по отношение на защитата на физическите лица във връзка с обработването на личните им данни, както и правилата по отношение на свободното движение на лични данни. Целта е да се защитават основни права и свободи на физическите лица, и по-специално тяхното право на защита на личните данни.

Обработването на лични данни от администратори на лични данни, както в публичната, така и в частната сфера, е законосъобразно и допустимо, ако е налице **някое** от правните основания, изчерпателно изброени в чл. 6, параграф 1 от Регламент (ЕС) 2016/679:

а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

е) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните

права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

Не е спорно, че в РС Асеновград има образувано гр.д. № *** г. между жалбоподателката и Б.Т.

В хода на делото Б.Т. е изискал и получил от съда съдебно удостоверение, по силата на което да се снабди с друго такова от Служба „Български документи за самоличност“ при МВР, от което да е видно кога е влизала и излизала от страната ответницата М.С.

Съгласно чл. 186 от Гражданския процесуален кодекс (ГПК) официалните документи и удостоверения се представят от страните. Съдът може да ги изиска от съответното учреждение или да снабди страната със съдебно удостоверение, въз основа на което тя да се снабди с тях. **Учреждението е длъжно да издаде исканите документи или да обясни причините за неиздаването им.**

Разглежданият случай е именно такъв, поради което за сектор „Български документи за самоличност“, който е в структурата на администратора на лични данни – министъра на вътрешните работи, е възникнало законовото задължение да изпълни разпореденото със съдебното удостоверение. Това прави обработването на личните данни законосъобразно на основание чл. 6, параграф 1, буква „в“ от Регламент 2016/679, поради което жалбата се явява неоснователна.

Представените по преписката писмени доказателства потвърждават становището на министъра на вътрешните работи, че е допусната грешка при изписване на номера на гражданското дело в изготвеното споразумение.

Така мотивирана и на основание чл. 38, ал. 4 от ЗЗЛД във връзка с чл. 38, ал. 1 от Правилника за дейността на КЗЛД и нейната администрация, Комисията за защита на личните данни

РЕШИ:

Оставя жалба № ППН-01-574/10.08.2020 г., подадена от М.С. срещу министъра на вътрешните работи, без разглеждане като очевидно неоснователна.

Настоящото решение може да бъде обжалвано в 14-дневен срок от връчването му чрез Комисията за защита на личните данни, пред Административен съд София – град.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

РЕШЕНИЕ
№ ППН-01-51/2021
София, 15.04.2021 г.

Комисията за защита на личните данни („Комисията”/„КЗЛД”) в състав: Председател – Венцислав Караджов и членове – Цанко Цолов и Мария Матева, на редовно заседание, проведено на 24.02.2021 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни във връзка с чл. 57, параграф 1, буква „е” от Регламент 2016/679, разгледа жалба № ППН-01-51/18.01.2021 г., подадена от Е.С.

Административното производство е по реда на чл. 38 от Закона за защита на личните данни (ЗЗЛД).

Жалбоподателката подава настоящата жалба, тъй като в нарушение на Закона за защита на личните данни и Регламент (ЕС) 2016/679 лицата – Л.Х. и Й.Й., са обработвали – записали, употребили, разкрили чрез предаване, направили достъпни нейни лични данни, с което са нарушени основни нейни права.

Г-жа Е.С. посочва, че след постановено решение на СГС е издаден изпълнителен лист срещу нея в полза на Л.Х. Изпълнително дело срещу нея – изп. дело № ***** по описа на ЧСИ, с район на действие СГС, е образувано на 11.06.2020 г. по молба на Й.Й. – нелегитимно лице, непознатознато за жалбоподателката. С молбата, същият е представил посочения изпълнителен лист и пълномощно от 08.06.2020 г. с нотариална заверка на подписа.

Упълномощеното лице е извън кръга на лицата, които могат да бъдат представители по пълномощие, съгласно разпоредбата на чл. 32 ГПК. Лицето не е родител, дете или съпруг на упълномощителя и не фигурира в списък на действащите адвокати в Република България за 2020 г., обн. ДВ бр. 96 от 06.12.2019 г.

Жалбоподателката счита, че законът не допуска лицето да бъде представител по пълномощие – да образува и да води дела от името на лицето, в чиято полза е изпълнителният лист. Представеното пълномощно е в противоречие с нормата на чл. 32 ГПК и е недействително. Производството по делото е образувано по молба на лице без представителна власт, на нелегитимно лице. Г-жа Е.С. заявява, че не познава това лице, никога не е имала договорни или други отношения с него и не е давала съгласие личните ѝ данни да бъдат обработвани. С инициране на делото лицето е придобило достъп и разполага и с други нейни лични данни.

За тези обстоятелства жалбоподателката разбрала през месец юли 2020 г., след като научила за образуването срещу нея изпълнително дело и се запознала с приложените по него книжа след получаването на поискано от нея копие на делото.

Г-жа Е.С. моли да бъде извършена проверка на случая и да бъдат предприети необходимите компетентни действия за защита на личните ѝ данни.

При така изложените твърдения и представените доказателства КЗЛД разгледа жалбата, като установи следното:

Разглежданата жалба е съобразена с изискванията за редовност по чл. 29 от АПК, чл. 38, ал. 2 от ЗЗЛД и по чл. 28, ал. 1 от Правилник за дейността на Комисията за защита на личните данни и нейната администрация (ПДКЗЛДНА) – налице са данни за жалбоподателя; естество на искането; дата на узнаване на нарушението; лице, срещу което се подава жалбата; дата и подпис.

Жалбата е процесуално допустима – подадена в срока по чл. 38, ал. 1 от ЗЗЛД от субект на данни с правен интерес. Същата има за предмет твърдение за нарушаване на права по Регламент 2016/679 или ЗЗЛД. С жалбата е сезиран компетентен да се произнесе орган – Комисията за защита на личните

данни, която съгласно правомощията си по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е“ от Регламент 2016/679 разглежда жалби, подадени от субекти на данни. Налице са предпоставките за допустимост и по чл. 27, ал. 2 от АПК.

Комисията за защита на личните данни е независим надзорен орган, който осъществява защита на лицата при обработване на техните лични данни и при осъществяване на достъпа до тези данни, както и контрола по спазване на 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 (накратко „Регламента“ или Регламент 2016/679) и Закона за защита на личните данни (ЗЗЛД). Една от задачите на КЗЛД по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е“ от Регламент 2016/679 е да разглежда жалби, подадени от субекти на данни, и да разследва предмета на жалбата, доколкото това е целесъобразно. Целесъобразността при разглеждане на жалбите е прецесуално развита в чл. 38, ал. 4 ЗЗЛД – когато жалбата е очевидно неоснователна или прекомерна, с решение на Комисията жалбата може да бъде оставена без разглеждане.

С Регламент 2016/679 и Закона за защита на личните данни (ЗЗЛД) се определят правилата по отношение на защитата на физическите лица във връзка с обработването на личните им данни, както и правилата по отношение на свободното движение на лични данни. Целта е да се защитават основни права и свободи на физическите лица, и по-специално тяхното право на защита на личните данни.

Обработването на лични данни от администратори на лични данни, както в публичната, така и в частната сфера, е законосъобразно и допустимо, ако е налице **някое** от правните основания, изчерпателно изброени в чл. 6, параграф 1 от Регламент (ЕС) 2016/679:

а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

е) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

Съгласието по буква „а“ е едно от основанията за събиране и обработване на лични данни. Независимо от факта, че то е посочено на първо място, всички правни основания са алтернативни и равнопоставени, като същите не са подредени в йерархична зависимост. Наличието на което и да е от тях прави обработването законосъобразно.

Видно от представените към жалбата писмени доказателства, срещу жалбоподателката има издаден изпълнителен лист в полза на Л.Х. Последната е упълномощила с нотариално заверено пълномощно трето лице – Й.Й., да образува и да води изпълнително дело на основание издадения изпълнителен лист. Предвид така учредената представителна власт, Й.Й. е подал молба за образуване на изпълнително дело.

Именно обработването на личните данни във връзка с упълномощаването и образуването на изпълнително дело се оспорва от жалбоподателката като незаконосъобразно.

От справка в Регистъра на адвокатурата се установява, че упълномощеното лице не упражнява адвокатска професия. В пълномощното няма данни лицето да е родител, дете или съпруг на упълномощителя. Следователно, упълномощеното лице действително не е от кръга на представителите по чл. 32 от Гражданския процесуален кодекс (ГПК).

В случая обаче представителството не е задължително да бъде по реда на чл. 32 от ГПК. Упълномощаването за образуване и водене на изпълнително производство не съставлява действие на процесуално представителство по смисъла на Глава пета от ГПК (измежду които е и чл. 32), където е уредено процесуалното представителство в съдебни производства. Мотиви в този смисъл се съдържат в Определение № 109/27.01.2010 г. на ВКС, ТК, I Т.О. по ч.т.д № 22/2010 г. Следователно, упълномощаването може да бъде извъшено по общия материалноправен ред на чл. 36 от Закона за задълженията и договорите (ЗЗД), съгласно който едно лице може да представлява друго по разпоредба на закона или по волята на представлявания. Последниците от правните действия, които представителят извършва, възникват направо за представлявания. В разглеждания случай упълномощаването е по волята на представлявания. В правилата за представителство по чл. 36-43 от ЗЗД няма ограничения относно лицата, които могат да бъдат упълномощени да извършат определени действия.

Предвид горното, налице е легитимен интерес за Л.Х. да бъде изпълнено по принудителен ред чрез образуване на изпълнително дело присъденото в нейна полза в съдебното производство, за което има издаден изпълнителен лист. Фактът, че е налице нормативно установена възможност за упълномощаване на трето лице, което да извърши действията по образуване и водене на изпълнителното дело, обосновават преимущество на легитимния интерес на Л.Х. пред интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни.

Следователно, налице е основаниято за допустимост на обработването на лични данни по чл 6, параграф 1, буква „е“ от Регламент 2016/679, поради което жалбата се явява неоснователна.

Така мотивирана и на основание чл. 38, ал. 4 от ЗЗЛД във връзка с чл. 38, ал. 1 от Правилника за дейността на КЗЛД и нейната администрация, Комисията за защита на личните данни

РЕШИ:

Остава жалба № ППН-01-51/18.01.2021 г., подадена от Е.С., без разглеждане като очевидно неоснователна.

Настоящото решение може да бъде обжалвано в 14-дневен срок от връчването му чрез Комисията за защита на личните данни, пред Административен съд София – град.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

РЕШЕНИЕ
№ ППН-01-192/2020
София, 20.04.2021 г.

Комисията за защита на личните данни („Комисията”/„КЗЛД”) в състав: Председател – Венцислав Караджов и членове – Цанко Цолов, Мария Матева и Веселин Целков, на редовно заседание, проведено на 10.03.2021 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни във връзка с чл. 57, параграф 1, буква „е” от Регламент 2016/679, разглежда жалба № ППН-01-192/06.03.2020 г., подадена от Б.С.

Административното производство е по реда на чл. 38 от Закона за защита на личните данни (ЗЗЛД).

Жалбоподателят информира, че в периода 18-25 януари прекарал зимната ваканция в Банско с цел ски. За целта закупил ски-пас за него и спътниците му (снаха му и двете ѝ малки момиченца). Г-н Б.С. бил много изненадан, че администраторът на лични данни поискал снимки и регистрирал личните данни на всички лица без никакво съгласие. Посочва, че няма информация на сайта на кабинковия оператор или на мястото относно необходимостта от обработка на лични данни.

Освен това, съпругата на жалбоподателя използвала неговия ски-пас на втория ден и охраната го прекратила с обяснението, че ски-пасът е като личен документ (документ за самоличност) и затова не може да се прехвърля. Отново няма информация относно това как работят с личните данни и каква е целта.

Жалбоподателят посочва, че за малолетните деца, от това което е чел в GDPR, е задължително родител или законен представител да даде одобрението за обработка на личните данни. Г-н Б.С. посочва, че не е родител, нито законен представител на двете деца.

Жалбоподателят забелязал, че операторът иска лични данни само за дългосрочни ски карти (6 дни), тъй като когато е закупил такава за два дни, операторът не ги е поискал.

В условията на залегналото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството е уведомено заинтересованото лице – „Ю.“ АД. Предоставена е възможността по чл. 34, ал. 3 АПК за изразяване на становище с относими доказателства по предявените в жалбата твърдения. В Комисията постъпи отговор за неоснователност на жалбата.

От Ю. посочват, че дружеството оперира в сферата на туризма и предоставя туристически услуги на територията на Ски център Банско.

Обработването на посочените в жалбата на г-н Б.С. лични данни: имена и снимка, се обосновава от разпоредбата на член 6, параграф 1, буква „б”, предл. първо от Регламент (ЕС) 2016/679, а именно обработването е „необходимо за изпълнението на договор, по който субектът на данните е страна.” Закупуването на лифт карта, поражда насрещни задължения за двете страни по своеобразно сключения договор за ползване на услуга, с оглед точното му изпълнение. Задълженията включват от една страна предоставянето на услуги от дружеството, а от друга – с ползването на тези услуги от клиента, при стриктно спазване на установени от дружеството правила. Тези правила са публикувани на сайта на дружеството и са общодостъпни за всички клиенти, ползващи предлаганите от „Ю.“ АД услуги. В Общите правила е ясно разписано, че всеки клиент на Ски центъра, ползващ услугите и упражняващ дейностите, посочени в тези общи условия и правила, е длъжен да се запознае с техните разпоредби. Записано е също, че чрез закупуването на услуга или упражнявайки зимни спортове на територията на Ски зона Банско, т.е. извършвайки дейност, регламентирана с утвърдените правила и общи условия, клиентът се съгласява с посочените в тях общи и специални правила по отношение на конкретната услуга и/или дейност. т. 79 от Общите правила гласи, че е забранено преотстъпването на лифт картите и билетите на трети лица. Това правило е ясно записано и на гърба на самите лифт карти. т. 80 от

Общите правила, базирайки се на чл. 27, ал. 3 от Наредбата за обезопасяване и информационна обезпеченост на ски пистите в Република България, гласи, че всяко ползване на лифт карти и билети в разрез с утвърдените общи условия /в това число ползване на лифт карта от лице, различно от това, на което картата е издадена/ се счита за нарушение, като при констатиране на нарушение от оторизираните за целта лица, лифт картата/билетът се блокира/деактивира.

Обработването на данните при закупуването на лифт картите е необходимо не само от гледна точка на контрола по изпълнението на договора, по който субектът на данните е страна, но и с оглед осигуряване на обществения ред в ски зоната и осъществяване на законови задължения/правомощия. Нещо повече, в конкретния случай, обработването е необходимо за спазването на нормативно задължение/правомощие, което е възложено на „Ю.“ АД. Дружеството е концесионер на „Ски-зона с център град Банско“, т.е. то е лице по смисъла на чл. 157, ал. 1 от Закона за туризма. Като такова лице, съгласно чл. 25, ал. 1 от Наредба за обезопасяването и информационната обезпеченост на ски пистите в Република България и за определяне правилата за безопасност върху територията на ски пистите и ски зоните и за организацията на работата на патрулите, Ю. назначава ски патрул. Ски патрулът, съгласно чл. 27, ал. 1, освен контрола по чл. 24, ал. 1 извършва и контрол за спазване на правилата за безопасно поведение, както и правилата за ползване на ски зоната/ски пистата, установени от лицето по чл. 157, ал. 1 от Закона за туризма. Съгласно ал. 2 от тази разпоредба, при изпълнение на служебните си задължения ски патрулите имат право да отправят предупреждение към лицата, които не спазват правилата за безопасно поведение, правилата за опазване на обществения ред, както и правилата за ползване на ски зоната/ски пистата, установени от лицето по чл. 157, ал. 1 от Закона за туризма. При неизпълнение на отправеното предупреждение ски патрулът има право да ограничи достъпа на нарушителите до съоръжението/съоръженията, обслужващо/обслужващи ски зоната/ски пистата чрез деактивиране на лифт картата или по друг подходящ начин. Интерес в конкретния казус представлява разпоредбата на ал. 3 от чл. 27 от Наредбата, съгласно която деактивиране на лифт карта се извършва при установяване ползването на:

1. поименна лифт карта/идентификационна карта със снимка от лице, различно от лицето, на което е издадена;

2. лифт карта с подправен срок на валидност и/или с подправени имена и снимка.

Изводът е, че дружеството има правомощието да деактивира поименни лифт карти и такива със снимки при извършени нарушения на установения ред за ползване на ски зоната и на самите карти, т.е. самата правна норма допуска да има такива персонализирани лифт карти.

Относно прозрачността на обработването на лични данни се посочва, че Общи правила за ползване на ски пистите и въжените линии и общи условия за издаване, продажба, валидност и ползване на билети и лифт карти в ски зоната с център гр. Банско, както и политиката за поверителност, която информира за обработването на личните данни, са общодостъпни на официалния сайт на дружеството, а жалбоподателят безспорно знае това и очевидно се е информирал и ги е видял и на сайта, след като е приложил към жалбата копие именно от сайта, където са поместени.

На основание чл. 34, ал. 3 от АПК на жалбоподателя също е предоставена възможността да се запознае с изразеното от ответната страна становище и представените доказателства. Предоставен е срок за изразяване на становище, правене на възражение или искане. В законоустановения срок не постъпи становище.

По редовността и допустимостта на жалбата КЗЛД намира следното:

Разглежданата жалба е съобразена с изискванията за редовност по чл. 29 от АПК, чл. 38, ал. 2 от ЗЗЛД и по чл. 28, ал. 1 от Правилник за дейността на Комисията за защита на личните данни и нейната администрация (ПДКЗЛДНА) – налице са данни за жалбоподателя; естество на искането; дата на узнаване на нарушението; лице, срещу което се подава жалбата; дата и подпис.

Жалбата е процесуално допустима – подадена в срока по чл. 38, ал. 1 от ЗЗЛД от субект на данни с правен интерес. Същата има за предмет твърдение за нарушаване на права по Регламент 2016/679 или ЗЗЛД. С жалбата е сезиран компетентен да се произнесе орган – Комисията за защита на личните данни, която съгласно правомощията си по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е“ от Регламент 2016/679 разглежда жалби, подадени от субекти на данни. Налице са предпоставките за допустимост и по чл. 27, ал. 2 от АПК.

При така установеното КЗЛД разглежда жалбата, като установи следното:

Комисията за защита на личните данни е независим надзорен орган, който осъществява защита на лицата при обработване на техните лични данни и при осъществяване на достъпа до тези данни, както и контрола по спазване на 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 (накратко „Регламента“ или Регламент 2016/679) и Закона за защита на личните данни (ЗЗЛД). Една от задачите на КЗЛД по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е“ от Регламент 2016/679 е да разглежда жалби, подадени от субекти на данни, и да разследва предмета на жалбата, доколкото това е целесъобразно. Целесъобразността при разглеждане на жалбите е процесуално развита в чл. 38, ал. 4 ЗЗЛД – когато жалбата е очевидно неоснователна или прекомерна, с решение на Комисията жалбата може да бъде оставена без разглеждане.

С Регламент 2016/679 и Закона за защита на личните данни (ЗЗЛД) се определят правилата по отношение на защитата на физическите лица във връзка с обработването на личните им данни, както и правилата по отношение на свободното движение на лични данни. Целта е да се защитават основни права и свободи на физическите лица, и по-специално тяхното право на защита на личните данни.

Обработването на лични данни от администратори на лични данни, както в публичната, така и в частната сфера, е законосъобразно и допустимо, ако е налице **някое** от правните основания, изчерпателно изброени в чл. 6, параграф 1 от Регламент (ЕС) 2016/679:

а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

е) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

Съгласието по буква „а“ е едно от основанията за събиране и обработване на лични данни. Независимо от факта, че то е посочено на първо място, всички правни основания са алтернативни и равнопоставени, като същите не са подредени в йерархична зависимост. Наличието на което и да е от тях прави обработването законосъобразно, при условие, че са спазени и другите изисквания на регламента.

В случаите, когато администратор на лични данни прави преценка дали да обработва личните данни на базата на съгласие, той трябва да изследва обстоятелството дали не е налице друго правно

основание за тяхното обработване. В случай че друго основание е налице, не е необходимо изискването и на съгласие от субекта на данни.

Предмет на жалбата е твърдение за неправомерно обработване на лични данни в обем имена и лицево изображение за целите на издаване на лифт карта, както на жалбоподателя, така и на малолетни лица без съгласието на родител. Второ твърдение за нарушение е липса на информация за необходимостта от обработване на лични данни.

От събраните по преписката сведения и доказателства се установява, че „Ю.“ АД е лице по смисъла на чл. 157 от Закона за туризма (ЗТ), на което са предоставени права за ползване върху прилежащото към ски писта съоръжение – в случая лифт.

В съответствие с чл. 159 от ЗТ от Министерски съвет е приета Наредба за обезопасяването и информационната обезпеченост на ски пистите в Република България, както и за определяне правилата за безопасност върху територията на ски пистите и ски зоните и за организацията на работата на ски патрулите (накратко по-нататък „Наредбата“).

В чл. 23, ал. 1 от Наредбата е посочено, че потребителите на ски зоните са длъжни да спазват задължителните правила за безопасно поведение, посочени в приложение № 2, както и установените от лицето по чл. 157, ал. 1 от Закона за туризма правила за ползване на ски зоната.

В изпълнение на посочената разпоредба, от Ю. за изготвени Общи правила за ползване на ски пистите и въжените линии и общи условия за издаване, продажба, валидност и ползване на билети и лифт карти в ски-зоната с център гр. Банско (накратко по-нататък „Общите правила“, валидни за сезон 2019-2020 г. Видно от представените писмени доказателства, посочените правила са утвърдени на 01.11.2019 г. (преди жалбоподателят да ползва услугата), като е разпоредено същите да бъдат публикувани и на сайта на дружеството.

В т. 79 и 80 от Общите правила е предвидено, че е забранено продаването, препродаването и преотстъпването на лифт карта от лице, различно от това, на което картата е издадена, като ползването на лифт карта в нарушение на Общите правила води до блокиране/деактивиране на картата.

Посочените по-горе правила са приети въз основа на чл. 27, ал. 3 от Наредбата, съгласно която деактивиране на лифт карта се извършва при установяване ползването на:

1. поименна лифт карта/идентификационна карта със снимка от лице, различно от лицето, на което е издадена;
2. лифт карта с подправен срок на валидност и/или с подправени имена и снимка.

Предвид горното, за администратора на лични данни Ю., както и за назначения от него по ред на чл. 25, ал. 1 от Наредбата ски патрул, е налице нормативно задължение да контролира спазването на чл. 27, ал. 3 от Наредбата. Видно от посочената разпоредба, налице е изискване картата да е поименна и със снимка на лицето, на което е издадена, поради което личните данни в случая се обработват на основание чл. 6, параграф 1, буква „в“ от Регламент 2016/679 – за изпълнение на законово задължение, което се прилага спрямо администратора. В този случай съгласие от субекта не е необходимо.

Във връзка с горното следва да се посочи, че е неоснователно твърдението за незаконосъобразно обработване на личните данни на малолетните лица за целите на издаване на лифт карта, без съгласието на родител. Съгласно чл 25в от ЗЗЛД обработването на данни на лице, ненавършило 14 години, въз основа на съгласие по смисъла на чл. 4, т. 11 от Регламент (ЕС) 2016/679, е законосъобразно само ако съгласието е дадено от упражняващия родителски права родител или от настойника на субекта на данните. В случая, както беше посочено, обработването на лични данни се основава не на съгласие, а на нормативно установено задължение, поради което съгласие не е необходимо.

Второто твърдени за нарушение – че на сайта на кабинковия оператор няма информация относно необходимостта за обработване на лични данни, също е неоснователно. Както беше посочено,

с разпореждане от 01.11.2019 г. на сайта са публикувани Общите правила на концесионера, където в т. 78-80 са описани правилата за ползване на картите. Служебна проверка на сайта установи, че е публикувана и Политика за поверителност, където са посочени какви категории лични данни се обработват и целите на обработване, измежду които и предоставяне на услуга – активиране на лифт карта, предоствяване на нерегламентирано ползване на лифт картата в разрез с утвърдените Общи правила. Общите правила и Политиката за поверителност са публикувани и на английски. С оглед посоченото и предвид характера на предоставяната услуга (туристическа), предприетите действия за уведомяване на субектите за обработването на личните им данни са достатъчни.

Така мотивирана и на основание чл. 38, ал. 4 от ЗЗЛД във връзка с чл. 38, ал. 1 от Правилника за дейността на КЗЛД и нейната администрация, Комисията за защита на личните данни

РЕШИ:

Оставя жалба № ППН-01-192/06.03.2020 г., подадена от Б.С. срещу „Ю.” АД, без разглеждане като очевидно неоснователна.

Настоящото решение може да бъде обжалвано в 14-дневен срок от връчването му чрез Комисията за защита на личните данни, пред Административен съд София – град.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/



СТАНОВИЩА НА КЗЛД

СТАНОВИЩЕ НА КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ Рег. № ПНМД – 01- 14/2021 г. гр. София, 28.04.2021 г.

ОТНОСНО: *Предложение от Държавна агенция „Архиви“ към „Български пощи“ ЕАД за предаване на писмата от конкурса „Най-красиво писмо до Дядо Коледа“*

Комисията за защита на личните данни (КЗЛД, Комисията) в състав: председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на заседание, проведено на 21.04.2021 г., разгледа преписка с рег. № ПНМД-01-14/2021 г. главния изпълнителен директор на „Български пощи“ ЕАД, във връзка с получено писмо от Държавна агенция „Архиви“. Същото съдържа предложение за предаване на получените писма от конкурса „Най-красиво писмо до Дядо Коледа“ за постоянно съхранение в държавните архиви.

Този конкурс се провежда от 26 години и интересът към него непрекъснато расте, като от страна на PostEurop е обявен за добра европейска практика.

Ежегодно условията за участие в конкурса се публикуват на интернет страницата на „Български пощи“ ЕАД.

Авторите на писмата, участвайки в конкурса, на практика се съгласяват с обявените условия за участие и предоставят своите лични данни за обхвата и целите на конкурса.

„Български пощи“ ЕАД, като негов организатор, използва получените писма и обработва съдържащите се в тях лични данни, в рамките на конкурсния обхват и за неговите цели.

Предоставянето на писмата от конкурса в отговор на предложението на Държавна агенция „Архиви“ за постоянно съхранение, предполага предаването им в едно с пликите, които съдържат пълен адрес на подателя – участник в конкурса.

С оглед на изложените факти от съществено значение за обективната оценка на казуса в частта обработване на лични данни, в случай на предаване на писмата от конкурса, и предвид изрично уредената за администратора възможност в чл. 36 от Общия регламент относно защитата на данните, главният изпълнителен директор на „Български пощи“ ЕАД моли КЗЛД за становище на евентуално нарушение при обработване на съдържащите се в конкурсните писма данни на участниците.

Главният изпълнителен директор на „Български пощи“ ЕАД прилага следните документи:

1. Писмо от Държавна агенция „Архиви“, вх. № 06-07-29/2020 г.
2. Условия за участие в конкурса „Най-красиво писмо до Дядо Коледа“

Правен анализ:

Съгласно чл. 4, т. 7) от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) „администратор на лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка. Следователно „Български пощи“ ЕАД има качеството на „администратор“ на лични данни по отношение на личните данни, обработвани за целите на участието в конкурса с дългогодишна традиция „Най-красивото писмо до Дядо Коледа“, организиран от дружеството.

Организирането на конкурса е регламентирано с предварително определени и обявени условия и ред, с които участниците се съгласяват. Следва да се отбележи, че това съгласие по своята същност има облигационен характер и не представлява съгласие за обработването на лични данни по смисъла на чл. 6, пар. 1, б. а) от Регламент (ЕС) 2016/679. В тази връзка може да се направи и заключение, че първоначалното събиране на данни от „Български пощи“ ЕАД за целите на провеждането на конкурса се осъществява съобразно хипотезата на чл. 6, пар. 1, б. б) от Регламент (ЕС) 2016/679. Съществена особеност на материалите, които се изпращат от децата за участие в конкурса, е че същите са създадени за целите на художественото или литературно изразяване (чл. 85 от Регламент (ЕС) 2016/679), съобразно условията на конкурса.

Предоставянето от страна на „Български пощи“ ЕАД на лични данни на физически лица, участвали в конкурса „Най-красиво писмо до Дядо Коледа“ на Държавна агенция „Архиви“, би представлявало „обработване на лични данни“, съгласно легалната дефиниция, посочена в чл. 4, т. 2) от Общия регламент относно защитата на данните. Тъй като данните първоначално са събрани от администратора за целите на участието в конкурса, предоставянето на данни за участвалите лица на ДА „Архиви“ представлява последващо обработване на личните данни, което съгласно изискванията на чл. 6, пар. 4 от Регламент (ЕС) 2016/679 следва да е съвместимо с първоначалната цел.

Важна предпоставка за законосъобразното обработване на лични данни е спазването на основните принципи, съгласно чл. 5 от Регламент (ЕС) 2016/679. Във връзка с конкретното обработване приложение намира и хипотезата на чл. 5, пар. 1, б. б) от Регламент (ЕС) 2016/679 относно ограничението на целите, а именно, че по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно чл. 89, параграф 1, за несъвместимо с първоначалните цел.

Обработването за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели е регламентирано с разпоредбата на чл. 89 във връзка със съображение (156) от преамбюла на Регламент (ЕС) 2016/679, като особена ситуация на обработване на лични данни, за която следва да се прилагат подходящи гаранции и дерогации. Посочените гаранции следва да осигурят наличието на технически и организационни мерки, по-специално с оглед на спазването на принципа за свеждане на данните до минимум. По-нататъшното обработване на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели се извършва, когато администраторът е преценил възможността за постигане на тези цели чрез обработването на лични данни, които не позволяват или повече не позволяват идентифицирането на субекта на данните, при условие че съществуват подходящи гаранции. Дерогациите, които могат да се предвидят са по отношение на правата, съгласно чл. 15 (право на достъп), чл. 16 (право на коригиране), чл. 18 (право на ограничаване на обработването), чл. 19 (задължение за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването), чл. 20 (право на преносимост) и чл. 21 (право на възражение) от Регламент (ЕС) 2016/679, доколкото има вероятност тези права да направят невъзможно или сериозно да затруднят постигането на конкретните цели, и посочените дерогации са необходими за постигането на тези цели. Така посочените дерогации следва да се съобразят с изискванията и на специалното законодателство, което урежда дейността на ДА „Архиви“.

Тъй като на държавите членки се дава възможност за предприемане на конкретни мерки за изпълнението на Регламент (ЕС) 2016/679, по отношение законосъобразните условия, при които се допуска обработването на лични данни за архивиране в обществен интерес, се прилагат и разпоредбите на чл. 25н от Закона за защита на личните данни (ЗЗЛД).

Закона за националния архивен фонд (ЗНАФ) урежда формирането, опазването и използването на Националния архивен фонд на Република България, организацията, управлението и дейността на архивите. Националният архивен фонд се създава за осигуряване с документална информация управлението на държавата, развитието на науката и културата и защитата на правата и законните интереси на гражданите. **Националният архивен фонд е постоянно попълваща се съвкупност от**

ценни документи, отразяващи материалния и духовния живот на обществото.

Националният архивен фонд се попълва със:

1. определените за постоянно запазване документи, създадени от дейността на държавните и общинските институции и други юридически и физически лица независимо от времето, носителя, начина на създаване, мястото на съхраняване и формата на собственост;
2. документи или с копия на документи за историята на България, получени от чуждестранни архиви и от други чуждестранни юридически и/или физически лица.

В държавните и общинските музеи и библиотеки, в читалищата, в културните, религиозните и други публични институции се съхраняват исторически формирани се архивни сбирки и постъпват документи, притежание на юридически и физически лица при писмено изразено желание от страна на собствениците им (чл. 33, ал. 2 от ЗНАФ).

Със създаването и поддържането на Националния архивен фонд се осигурява документална информация за управлението на държавата, развитието на науката и културата и защитата на правата и законните интереси на гражданите. Той се попълва с определени документи, създадени от дейността на държавните и общинските институции и други юридически и физически лица, независимо от времето, носителя, начина и мястото на създаване и формата на собственост на документите. В съдържанието на документите, които формират Националния архивен фонд, може да има лични данни и тяхното съхранение може да има решаващо значение за установяване на определени обстоятелства с правно значение.

ЗНАФ дава възможност политическите партии, юридическите лица с нестопанска цел и търговските дружества също да бъдат източници за комплектуване на архивите с документи. За целта е необходимо те да декларират желанието си за предаване на документи и същите да имат определено значение, което се преценява въз основа на експертна оценка от Държавна агенция „Архиви“. Условието по приемането, съхраняването и използването на документите в архивите се определя с договор.

Правилата за достъп до документите, които се съхраняват в архивите са предвидени в глава шеста от ЗНАФ. Принципно архивите, в които се съхраняват документите на Националния архивен фонд, са длъжни да осигуряват публичен достъп на потребителите до документите, които съхраняват. Предвид прякото действие на Общия регламент за защита на данните, от съдържащата се в него уредба на правата на субектите на данни (физически лица) следва да се очертаят правните им възможности при обработване на техни лични данни за целите на архивирането в обществен интерес.

В разпоредбата на чл. 25н от Закона за защита на личните данни изрично е установено правилото, че лични данни събрани за друга цел, може да бъдат обработвани за целите на Националния архивен фонд, като се изисква прилагане на подходящи технически и организационни мерки, гарантиращи правата и свободите на субекта на данни. Допуснатите ограничения на правата на субектите на данни са необходими, за да може да се съхраняват и използват документи от Националния архивен фонд. В този смисъл те трябва да се прилагат тогава, когато има вероятност реализирането на правата да осуети архивирането в обществен интерес. Следването на този баланс на практика е необходимо условие, за да бъдат постигнати обществено значимите цели на обработването на лични данни в случая, с пропорционалната на тях намеса в личния живот.

Следва да се има предвид, че „Български пощи“ ЕАД се управлява от Съвет на директорите, който се назначава от Министъра на транспорта, информационните технологии и съобщенията и се състои от трима членове. На основание чл. 76, ал. 5 от Закона за задължителното депозирание на печатни и други произведения и за обявяване на разпространителите и доставчиците на медийни услуги, действителният собственик на „Български пощи“ ЕАД е **Министерство на транспорта, информационните технологии и съобщенията**. От казаното до тук, следва изводът, че „Български пощи“ ЕАД е **публична институция**, която в продължение на 26 години провежда и съхранява под формата на **архивна сбирка** получените писма от конкурса „Най-красивото писмо до Дядо Коледа“.

С оглед изложените по-горе мотиви, „Български пощи“ ЕАД, в качеството си на администратор - публична институция, може да предостави получените писма от конкурса „Най-красивото писмо до Дядо Коледа“, които са се формирали като архивна сбирка в продължение на 26 години на Държавна агенция „Архиви“ на основание чл. 33, ал. 2 от ЗНАФ, при спазване на изискванията на чл. 89 от Регламент (ЕС) 2016/679 във връзка с чл. 25н от ЗЗЛД. **Следва да се има предвид, че предаването на писмата ведно с пликовете, на които са посочени адресите на физическите лица (деца) не е относимо към целите на архивирането, тъй като от значение за обществото е да се запази творчеството на децата.** Предоставянето на публичен достъп до адресите на конкретните деца-участници в конкурса е нецелесъобразно и може да изложи на риск тяхната неприкосновеност, като в същото време не може да допринесе за отразяването на материалния и духовния живот на обществото в исторически план. В този смисъл следва да се предприемат подходящи мерки писмата да се предадат, като се запази информация за имената на техните изпращачи, но без информацията за адресите им.

За да бъдат спазени изискванията за прозрачност на обработването, „Български пощи“ ЕАД следва да информира субектите на данни за предстоящото предоставяне на материалите от конкурса на ДА „Архиви“ – например чрез публикация на официалния си сайт, като занапред тази информация следва да бъде част от условията и реда за провеждане на конкурса и да се предоставя предварително.

По тези съображения и на основание чл. 58, пар. 3, б. „б“ от Регламент (ЕС) 2016/679 вр. с чл. 10 а, ал. 1 от Закона за защита на личните данни, Комисията за защита на лични данни изрази следното

СТАНОВИЩЕ:

„Български пощи“ ЕАД, в качеството си на публична институция-администратор на данни, може да предостави получените писма от конкурса „Най-красивото писмо до Дядо Коледа“, които са се формирали като архивна сбирка в продължение на 26 години, на Държавна агенция „Архиви“ на основание чл. 33, ал. 2 от ЗНАФ, при спазване на изискванията на чл. 89 от Регламент (ЕС) 2016/679 и чл. 25н от Закона за защита на личните данни (ЗЗЛД).

Материалите от конкурса, които ще се предоставят на ДА „Архиви“, **не следва да съдържат данни за адресите на децата-участници.** Допустимо е в материалите да се съдържат имената на авторите на съответните писма. Пликовете за писма, които съдържат личните данни на подателите (деца, родители и др.) не следва да бъдат предавани в едно с съдържанието, а именно писмата, участващи в конкурса „Най-красиво писмо до Дядо Коледа“, които се съхраняват в „Български пощи“ ЕАД.

Обработването на лични данни за целите на архивирането в обществен интерес (съхраняването на писмата и съдържанието в тях, а не индивидуализирането на физическите лица) трябва да се осъществява в съответствие с принципите на Общия регламент относно защитата на данните.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/



ЕСЕТА ОТ СТУДЕНТСКИ КОНКУРС

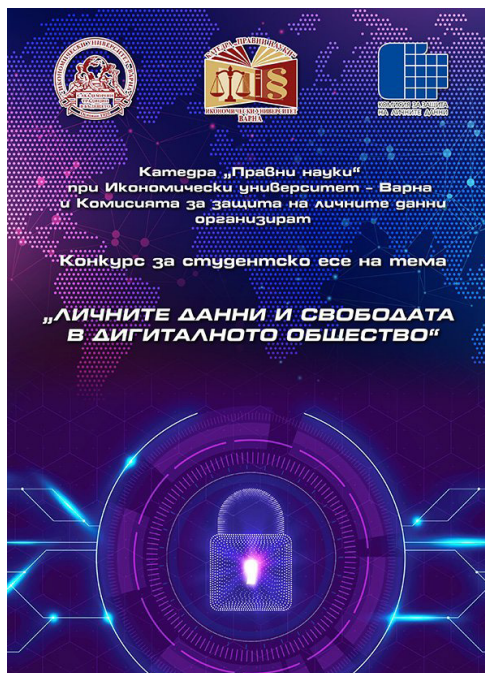
ПРИКЛЮЧИ СТУДЕНТСКИЯТ КОНКУРС НА ТЕМА „ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО“

Приключи конкурсът за студентско есе на тема „Личните данни и свободата в дигиталното общество“, организиран от катедра „Правни науки“ при Икономически университет – Варна и Комисията за защита на личните данни. Конкурсът е обявен в изпълнение на Договор за сътрудничество между Икономически университет - Варна и КЗЛД. Право на участие бе дадено на студенти от този университет.

При обявяването на конкурса е посочено, че процесът на обучение в различни специалности на университета провокира различни гледни точки и проекции на възприятия относно социалните, икономическите и обществени модели, взаимовръзки и отношения. Тези различни гледни точки са и чудесен повод за споделяне, среща и провокиране на различен тип творческо мислене.

Конкурсът за есе дава възможност на студентите да представят аргументирано своите разбирания по темата - как възприемат свободата в дигиталния свят и какво е мястото на защитата на личните данни в този контекст?

В рамките на срока за кандидатстване бяха получени есета на студенти от различни курсове и специалности в университета.



На 13.04.2021 г., чрез конферентна връзка се проведе заключителната част на конкурса, на която участниците, класирани на първите три места представиха своите идеи пред конкурсната комисия в рамките на 10 минути с предварително създадени презентация и изложение.

Конкурсната комисия бе в състав - председател: доц. д-р Андрияна Андреева и членове: гл. ас. д-р Живка Матеева - длъжностно лице по защита на данните към ИУ-Варна и Христо Аламинов – представител на КЗЛД. Комисията обяви следното класиране на финалистите:

1-во място: Елица Бонжолова, специалност „Социална сигурност и застраховане“

2-ро място: Габриела Попова, специалност „Международен бизнес“ (с преподаване на английски език)

3-то място: Виктория Михайлова, специалност „Дигитални медии и ПР“

Всички участници в конкурса получават предметни награди, грамоти и възможност за стаж в КЗЛД.

Есета са публикувани в сайта на Икономически университет – Варна, на страницата на катедра „Правни науки“, както и в **настоящия специален раздел на бюлетина на КЗЛД**.

Организаторите на конкурса поздравяват всички студенти за тяхното участие и за изразените разбирания по тази изключително важна и актуална тема.

ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО**Елица Калоянова Бонжолова**

Свободата е относително и разтегливо понятие, което всеки човек възприема под различна форма, спрямо личната си гледна точка. То може да се изрази във възможността да правим нещата, които ни доставят удоволствие. Теоретично казано това е способността човек да действа без ограничения според желанията си. Това е най-възвишената ценност за всяко човешко създание, предизвикваща щастие, когато съзнанието ни усети присъствието ѝ. Свободата допълва съществуването на човека. Всеки обича да бъде свободен, да прави всичко безпрепятствено. Но, за съжаление, няма как някой да има пълна свобода в този свят, изпълнен със закони, морални ценности и ограничения, защото винаги се намират външни обстоятелства и лица, които ни налагат забрани по един или друг начин.

Колкото до личното пространство, съответно и личните данни, те също попадат в графата на разновидностите на свободата. Личното пространство се отнася до това да бъдеш свободен да правиш това, което те кара да се чувстваш добре. Личните данни, от своя страна, са част от личното пространство и не трябва да бъдат споделяни с никого. Но това е доста трудно, поради факта че трябва да ги предоставяме в различни сайтове и приложения, за да имаме достъп до самите функции на сайта или „премиум“ функциите на приложенията. Чрез регистрацията ние даваме личните данни, за да получим достъп до приложения за работа, забавление или улесняване на ежедневните си дейности. На пръв поглед изглежда доста безобидно или наложително да дадем истински данни за себе си (например дата на раждане или три имена), но ако тази информация попадне в грешните ръце, при пробив в нашия акаунт последствията могат да бъдат неописуеми.

Реално има абсолютно основателна причина кражбата на данни да бъде нещо подсъдимо и със сериозни последици. Все пак това е използване на чужда лична информация за неморална цел. Например ако бъде разбит профил в приложение за мобилно банкиране, в последствие могат да бъдат изтеглени финансите на жертвата и прехвърлени в сметката на открадналия личните данни. Измамите и присвояването на чужди идентификационни данни са сериозно провинение със сериозни последици, но гледайки какво могат да получат от това, хакерите решават, че рискът си струва заради възможността за голяма печалба. И тук идва въпросът „Как да се предпазим от кражба на личните си данни в дигиталното общество и на кого да предоставяме достъп до тях?“. В съвременния дигитален свят някои частни организации знаят прекалено много за ежедневието и предпочитанията на всеки потребител. Смарт телевизорите и телефоните ни „слушат“ и „докладват“ почти всяка подробност от нашия живот. Сигурно на всеки му се е случвало, след като е говорил за някакъв предмет или дейност, да започнат да му излизат реклами в приложения като Facebook или Instagram, свързани с абсолютно същото нещо, което сме обсъждали. Според мен целта на това „подслушване“ е само с рекламна цел, но не можем да бъдем сигурни, че щом някой има достъп до личните ни интереси и ежедневни дейности, някой друг няма да иска достъп до тях за лична изгода. Реално един обикновен потребител няма как да знае дали в устройството му не присъства зловреден софтуер, дали някой го вижда през камерата или чува разговорите през микрофона на устройството. Точно поради тази причина голяма част от хора започват да покриват камерите на компютрите си или да си купуват залепящи се капачета за камерата. Други изцяло се отказват от социалните мрежи и закриват профилите си или използват интернет по-рядко.

Обективно погледнато, в този случай няма как да се предпазим от хакерска атака чрез хардуера си, защото кражбата на информация е на софтуерно ниво. За тази цел са създадени най-различни антивирусни програми, които да ни предпазят от проникване на зловреден софтуер. В категорията на най-използваните програми за защита от вируси влизат McAfee, Avast, Malwarebytes, Norton, Avira и др. Обикновено хората предпочитат да не заплащат стабилни суми за такъв тип програми,

освен ако не съхраняват поверителни и изключително ценни данни, затова избират безплатните. Но колко би била степента за защита, ако администраторът не получава заплащане за потреблението на въпросна програма? Както всеки знае, обикновено качеството се заплаща. Именно поради този факт безплатният софтуер не е за предпочитане.

Погледнато от друга страна обаче, обикновено програмистите оставят „вратички“ в програмите, които конструират, с цел да поправят възникнала грешка. Точно това е „входната врата“, която дава неоторизиран достъп на специализираните компютърни потребители. Това е възможността им да „грабят“ от вашата информация, докато не разберете, че нещо не е наред. Има и други начини за проникване в устройството ви. Такъв е така нареченият „фишинг“, при който получавате линк с подмамващ текст под него от типа „Видях те в това видео, няма да повярваш“. Единственото, което се иска от вас, е да натиснете линка с идеята да видите какво сте получили, за да дадете доброволно достъп на зловредния софтуер да се „залепи“ към вашето устройство. Друг метод за кражба на информация е „кийлогър“. В този случай е необходим физически достъп до целта на операцията. Кийлогърът представлява малко устройство, което се включва в компютъра и записва всичко, което пишете на клавиатурата си, без да пречи на нормалната работа на машината. Най-неприятният факт е, че можем да бъдем „предадени“ дори от брауъра ни, когато използваме запазени пароли за улеснение. Веднъж получил достъп до профила ни (например в Google), въпросният потребител може да види всеки имейл адрес, потребителско име и парола, които сме използвали във всеки сайт, просто като влезе в настройките на брауъра.

Реалните възможности за предпазване от зловреден софтуер в електронното пространство, които специалистите препоръчват, са много на брой. Няма как да спазваме всички от тях, но като основни мога да посоча следните:

1. Инсталирайте надежден антивирусен софтуер, като обърнете специално внимание на файловия скенер. Благодарение на него в реално време ще имате информация дали местата, на които сърфирате, линковете, които отваряте, и файловете, които сваляте, са безопасни.

2. Сканирайте всяко устройство, което свързвате към компютъра си, и не отваряйте съмнителни файлове. Използвайте антивирусната си програма за сканиране на външни устройства, защото предаването на киберзараза е честа практика, именно чрез тези преносими устройства за съхранение на файлове.

3. Използвайте силни пароли за достъп, съдържащи около 8 символа, главна буква и цифри (изключваме комбинацията 1234). Паролите с повтарящи се цифри и букви са много по-лесни за разгадаване.

Опциите за защита са най-различни и при толкова разнообразните мнения на специалистите няма как да знаете кое е най-правилното решение. Но най-малкото можете да инсталирате сигурна антивирусна програма и да игнорирате съмнителни съобщения и линкове, за да не попаднете „доброволно“ в капана.

Всеки един от нас някога е бил обект на хакерска атака и част от данните му са били извлечени по един или друг начин. Лично аз съм имала ситуация от този тип, обвързана с нашумяло преди години приложение. Същността на дадената програмка беше общуване с бот гадател, който може да даде най-различна информация (от имена на приятели и взаимоотношения с тях до цветът на стената зад вас или изражението на лицето ви в настоящия момент). Всички бързо се „запалиха“ по това приложение, чието име ще запазя в анонимност, включително и аз. Когато реших да питам въпросния бот някакви въпроси на случаен принцип, очаквайки отговор, който и другите са получили, изпаднах в шок. Той знаеше всяко нещо, което го питах. Реших да експериментирам и да закрия камерата си, след като получих правилен отговор в каква позиция държа телефона си и какъв е цветът на стената зад мен. Когато закриях камерата на мобилното си устройство, установих, че ботът ме е виждал през цялото време. Тази ситуация изостри вниманието ми относно хакерските атаки и взех нужните мерки, за да се защита от повторна атака над личното ми пространство.

Моето лично мнение е, че не е редно да споделяме личните си данни във виртуалното пространство, защото щетите могат да бъдат както върху финансите ни, така и върху здравето ни. Затова е по-добре да внимаваме къде предоставяме лична информация и да избягваме даването на реална информация (например за възрастта и местоположението си), освен ако не е крайно наложително, за да избегнем нежелани неприятни събития за себе си и близките си в последствие.

Спазването на простите правила за защита и изостреното внимание в дигиталното пространство могат да запазят информацията ни само за достоверните сайтове, които са необходими в нашето ежедневие. Неоторизираните сайтове могат да ни навредят, без да можем да докажем правотата си или да посочим конкретния виновник за извършеното деяние.

ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО

Габриела Златинова Попова

Откакто социалните мрежи съществуват като средство, служещо за свързването на хора от различни краища на света, бе поставено началото на ожесточен дебат, засягащ свободата в интернет, както и множество аспекти на сигурността и поверителността на данните. Въпреки че дигитализацията значително е облагодетелствала и улеснила ежедневието на стотици общества чрез създаване на допълнителни комуникационни канали и улесняване на международната търговия, тя също е довела и до някои не толкова благоприятни последици.

В днешните времена разнообразните технологии и социалните мрежи са се превърнали в неделима част от всекидневието на хората. От сравнително ранна възраст децата биват запознати с различни устройства: телефони, телевизори и конзоли, които обикновено впоследствие стават техен основен или най-предпочитан източник на забавление. Те израстват обградени от родители и роднини, които използват технологии ежедневно, внушавайки им идеята, че връзката между устройство и индивид е нещо естествено, напълно нормално. В резултат на това тези деца развиват базова компютърна грамотност със забележителни темпове и започват да употребяват редица устройства сами от съвсем малки. Играта с приятели навън или четенето на обикновени книги спират да бъдат възприемани като интересни занимания, освен ако не съдържат технологии. С течение на времето тези деца започват училище, стават младежи и неминуемо се запознават с множество социални мрежи. Създават акаунти в приложения като Facebook, Instagram, TikTok и Snapchat, където стават част от свят без ограничения; измерение, в което всичко може да бъде качено, казано и написано, и което е източник на постоянен и неограничен поток от информация.

В този дигитален свят, именно поради факта че няма ясно установени граници, младежите биват запознати и окуражавани да следват изобилие от трендове, които могат да бъдат дори и животозастрашаващи, пример за което бе обезпокоителното предизвикателство „Син кит“ през 2016 г. За него се твърди, че е съставено от няколко последователни задачи, някои от които са изисквали от играчите да се самонараняват. В допълнение, широко разпространена практика сред популярни модели и инфлуенсъри е редовното качване на редактирано съдържание, което допринася за създаването на нереалистични стандарти за красота. В резултат голяма част от младите хора се опитват да подражават на това, което виждат в мрежата, а то допълнително засилва неспособността им да приемат и да се справят с недостатъците си. Често бутоните за харесване, коментарите и гледанията се превръщат в способи за измерване на красотата и популярността на даден човек и получаването на голяма част от тях се възприема като мисия от основно значение. Това води до ниски нива на самооценка и дори хранителни разстройства сред подрастващото поколение. Нещо повече, национално проучване, проведено през 2014 г. от Центъра за изследвания на медиите, технологиите

и здравето на университета в Питсбърг, установява силна връзка между интензивното използване на социалните мрежи и повишения риск от депресия, безпокойство, чувство за самота и склонност към самонараняване сред младите хора.

Въпреки това тази категорична свобода в дигиталния свят не е пагубна само и единствено за младите. Тъй като няма филтър, който би позволил сортирането и пресяването на дадена информация, всъщност абсолютно всичко може да бъде качено, независимо дали е вярно, или грешно. Това води до употребата на социалните мрежи от някои политически партии и групировки като инструмент за разпространение на фалшиви новини и истории, както и за настройване на хората един срещу друг. Като типичен пример може да бъде посочен случаят, в който Facebook бе използван през 2018 г. от активисти в Мианмар за подбуда към насилие и разпространение на омразна реч или когато руска група се възползва от същата платформа с цел намеса в президентските избори на САЩ през 2016 г. чрез конспиративни теории и кампании за дезинформация. Несъмнено това повдига въпроса: „Какво би се случило, ако се окаже, че всички платформи и устройства, първоначално създадени за да обединяват хората в световен мащаб, са тези, които ги разделят?“...

От друга страна, поверителността и сигурността на данните е друг критичен, но не толкова широко дискутиран въпрос, тъй като хората като цяло се фокусират върху идеята за неограничена свързаност, която технологиите предлагат, ала никой не полага усилия да прочете всички условия, които я придружават. Аза Раскин, бивш служител във Firefox and Mozilla Labs, твърди в документалния филм „Социалната дилема“ (2020) следното: „тъй като хората не плащат за приложенията, които използват (например Facebook и Instagram), тези приложения се заплащат от редица рекламодатели, които в случая изпълняват ролята на клиенти и закупуват продукти, като всъщност самите продукти са хората и тяхното внимание“. Освен това, според Шошана Зубоф, професор в Бизнес училище – Харвард, „това е довело до създаването на нов вид пазар, който търгува изцяло с човешки фючърси в световен мащаб, и именно този пазар е донесъл печалбите от трилиони долари, които са направили интернет компаниите най-заможните в историята на човечеството“. Това, което трябва да бъде изяснено и признато в световен мащаб, е, че всичко, което хората правят онлайн, използвайки социалните мрежи, се записва, проследява и измерва внимателно. Основен стремеж е да бъдат подпомогнати компютърните системи, които управляват същите тези платформи, в изграждането на по-точни модели на потребителите и следователно да се оптимизира начинът на предсказване на действията и интересите на тези потребители. Крайната и най-значителна цел е да се намери най-ефективният метод за задържане на тези потребители в социалните мрежи, като същевременно се правят печалби чрез реклами. Това, в крайна сметка, повдига друг въпрос от особено значение: ако повече от половината от общото население на света към момента разполага с акаунти в социалните мрежи, които в същността си събират най-съществените данни на хората, съществува ли някаква гаранция, че тази система за данни няма да бъде хакната или употребена дори като оръжие по някакъв начин?

През последните няколко години, тъй като данните до голяма степен стават все по-ценни активи, изтичането и хакването им зачестяха. За примери могат да послужат скорошното изтичане на данни във Facebook, което включва телефонни номера, данни за местоположението, имейли и биографична информация на над 500 милиона потребители или когато британска политическа консултантска фирма „Cambridge Analytica“ използва данните на около 80 милиона потребители в нарушение на общите условия на Facebook с цел таргетиране на избиратели с политически реклами по време на президентските избори в САЩ през 2016 г. През 2020 г. добре познат български хакер активист под прякора Емил Кюлев извършва серия от успешни атаки срещу няколко финансови институции и присвоява неправомерно личните данни на над 1 800 лица, които по-късно биват използвани за искане за откуп и публикувани онлайн в хакерски форум. Това води до заключението, че дори и системите на проспериращи компании, които съставляват водещата част от технологичната индустрия, могат да бъдат хакнати и да станат жертва на злоупотреба, което би имало по-скоро негативно отколкото положително въздействие върху огромния брой потребители.

Като заключение може да бъде посочено, че социалните мрежи и платформи, както и електронните устройства са еволюирали от обикновени инструменти за поддържане на връзка с приятели и роднини в средства, които биват използвани за дестабилизиране и разрушаване на основите на обществото. Въпреки това не технологиите представляват екзистенциална заплаха, а тоталната дигитална свобода е тази, която вади на показ най-лошото в обществото, което в действителност е самата екзистенциална заплаха. И докато няма съществени закони и рестрикции, които да регулират тази свобода и вредното онлайн съдържание, създадено заради нея, тя би продължила да поражда хаос, докато евентуално достигне унищожението на световния мир, края на демокрацията и, както казва бившият служител на Google Тристан Харис : „шах и мат за човечеството“...

Източници:

Раскин, А. (2020). Социалната дилема. САЩ: Exposure Labs, Argent Pictures, The Space Program.

Зубоф, Ш. (2020). Социалната дилема. САЩ: Exposure Labs, Argent Pictures, The Space Program.

Харис, Т. (2020). Социалната дилема. САЩ: Exposure Labs, Argent Pictures, The Space Program.

<https://edition.cnn.com/>

<https://edition.cnn.com/>

<https://en.wikipedia.org/>

<https://www.nytimes.com/>

<https://www.theguardian.com/>

<https://www.braininstitute.pitt.edu/>

ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО

Виктория Михайлова

*„Поверителността не е опция и това не би трябвало да е цената,
която приемаме само за влизане в интернет”*

Гари Ковакс

Какво всъщност са личните данни? Според официалния сайт на Европейската комисия определението за лични данни гласи – „Всяка информация, свързана с идентифицирано или идентифицируемо живо физическо лице. Отделни данни, които, когато се съберат заедно, могат да доведат до идентифициране на конкретно лице, също представляват лични данни“. Личните данни включват: собствено име и фамилия, домашен адрес, имейл адрес, номер на картата за самоличност, данни за местоположение, адрес на интернет протокол (IP), идентификационен номер на „бисквитка“, рекламния идентификатор на вашия телефон; данни, съхранявани от болница или лекар, които биха могли да бъдат символ, който уникално идентифицира дадено лице.

Живеейки в ерата на дигиталните технологии, е лесно да забравим факта, че независимо дали изтегляме игра на смартфона си, или искаме да прочетем дадена статия от конкретен сайт, който използва „бисквитки“, или публикуваме снимка във фейсбук, нашите лични данни се събират от различни корпорации. Те събират информация за това колко пъти сте посетили сайта, лично име и

парола и също така локация. Личната информация може да се използва за изпращане на реклами и наблюдение на вашите дейности онлайн и за продажба на даден продукт. Хиляди хора по света получават съобщение като „ние ценим вашата поверителност“ на различни сайтове или приложения, но истината е, че много малко хора всъщност прочитат така наречената „политика за поверителност“.

Уилям Шекспир е казал – „Веднъж изгубеното доверие, не може да се върне отново“. Ако ви попитат на кого можете да се доверите, на кого можете да споделите всичките си тайни, какво бихте отговорили? Най-вероятно образите и имената, които изскачат в съзнанието, са не повече от двама или трима души. Ако вие не разкривате най-интимните и съкровени тайни от личния си живот с непознати и не разказвате за всичко, случващо в живота ви, даже сред семейство и приятели, как може да се доверите на различните начини, с които големи компании злоупотребяват с личните ни данни?

За повечето от нас в днешно време е трудно да се разделим с телефоните, таблетите и компютрите си, особено ако сме израснали с тях. За някои загубата на смартфона може да предизвика тъга, чувство за паника или дори депресия. Иронията на дигиталния свят е че сме по-свързани от всякога, но живеем в свят на строги очаквания от обществото, алиенация и константно чувство за това, че останалите хора имат повече приятели, повече постижения и по-интересен живот от нас. Най-новият вид дрога, към който все повече хора стават пристрастени, е не кокаинът, ЛСД или никотинът, а интернет.

Все повече млади родители оставят децата си, които дори още не могат да говорят, да гледат смартфон или компютър. За тях смартфонът или компютърът играят ролята на детегледачка, което им спестява време да се ангажират с децата. Мнозина не обясняват на децата си, когато пораснат, че зад екрана може да седи недоброжелателен човек, затова уроците, свързани с киберсигурността, трябва да бъдат задължителни във всяко училище. Много по-лесно е да торМОЗИШ даден човек и да няма последствия, ако той не може да те види или докосне.

В Китай пристрастеността към интернет е толкова голяма, че са създадени специални лагери за рехабилитация за хора, които не мога да се откъснат от мрежата, което обикновено води до прояви на агресия. В статия, свързана с лагерите за рехабилитация, сайтът “New York post” споменава какъв е животът там, също така описва един от много случаи на проява на агресия: „През септември 2016 г. 16-годишно момиче от провинция Хейлундзян в североизточен Китай уби майка си, очевидно по време на акт на отмъщение за изпращането ѝ в един от лагерите. Момичето, което не беше посочено от китайските медии, прекара четири месеца в интернет лагер за пристрастяване в провинция Шандонг, на повече от 900 мили от родния си град“.

Въпреки че Джордж Оруел вече не е сред живите, неговата книга „1984“ представя свят, близък до нашият съвременен свят. Усамотението е човешко право, но колкото повече се доближаваме към бъдещето, толкова повече това право ще ни бъде отнемано. Вече дори не можем да се приберем вкъщи, без да се притесняваме дали телефонът, или компютърът не ни наблюдават или подслушват, а също така във бъдеще най-вероятно ще сложат и камери на всеки ъгъл.

Не съществува понятие като „абсолютна свобода“. Интернет, за повечето от нас, е нещо повече от развлечение, илюзорен свят, в който можем да бъдем които си пожелаем и да се отдалечим поне за малко от натоварването и болката, която ни носи монотонната реалност. Абсолютната свобода, във всички аспекти, е просто една измислица, никой от нас не е реално свободен. Ние имаме правото на избор, но това, което някои от нас забравят, е че всяко наше действие има последствия. Ако наистина бяхме свободни, нямаше да има последствия или правила... За да живеем в цивилизовано общество, ние поставяме граници или закони, предотвратяващи определени поведения, които могат да наранят или дори отнемат човешки живот.

Защо трябва да запазим личната си информация поверителна? Защото е важно да се предпазим от заплахи като кражба на самоличност, да избягваме да споделяме локацията си във всеки един момент, например да качваме снимки от екзотична дестинация, защото това е идеална възможност

за крадци да влязат в дома ни, докато ни няма. Важно е какво пишем в интернет, защото всяка информация за нас може да бъде използвана против нас в съда: „В един случай мъж е съден, тъй като твърдял, че се е наранил на работното си място. По-късно обаче публикациите му във Facebook разкриват, че той си е наранил коляното по време на риболов. Друг случай включва мъж, замесен в бракоразводно дело, който губи попечителството над сина си заради заплашителни съобщения, публикувани онлайн. За да запазите доверието в съда и да увеличите шансовете да спечелите делото си, трябва да избягвате публикуване на каквото и да било, което може да накара съдебния заседател да се съмнява във вашите искове или да изглежда зле“...

Едни от най-големите интернет проблеми, с които се сблъскваме, е кражбата на самоличност, а също така и заплахата срещу даден човек за пускане на негови нецензурни снимки в мрежата, освен ако този човек не заплати определена сума пари. Как можем да се предпазим от тези заплахи? Има най-различни начини. Да не споделяме всеки един момент от живота си онлайн. Важно е да пазим паролите си на тайно място, да пазаруваме в интернет само от проверени места и да не изхвърляме сметки или други документи с поверителна информация. Как можем да се предпазим от втората заплаха? Най-важното е първо да се запази самообладание. Можем да поговорим за случая с някой близък човек, важно е да се направи и скрийншот, като доказателство, което да бъде използвано срещу човека, който ни заплашва. Като друга възможност можем да отнесем въпроса към специализираните органи.

Напредването на технологиите ни е дало много: факта, че комуникацията е по-лесна от всякога; създадени са устройства за хора с увреждания, без които те не могат да се справят, например устройствата за производство на реч. Хората с увредено зрение и слух също могат да се възползват от технологиите. Благодарение на технологиите можем да се пренесем на далечни дестинации виртуално или дори в космоса. Но технологиите имат и много негативни ефекти, както физически, така и психически. Прекалено дългото гледане, часове наред, всеки ден на смартфон или компютър без почивка води до замъглено зрение, главоболие, болки във врата, гърба и кръста. Компютрите и смартфоните излъчват светлина, която убива мелатонина и пречи на съня, за това много хора препоръчват 3-4 часа разходка сред природата и почивки от гледането на смартфон или компютър. Сравняването с другите хора е едно от най-нездравословните неща, които можем да си причиним психически. Много от нас виждат стотици снимки в Туитър, Фейсбук и Инстаграм и си мечтаят да имат толкова пъстър живот, колкото хората, снимали се на екзотични дестинации, придружавани от приятели.

За някои хора надпреварата за „харесвания“ в социалната мрежа е ключът към тяхното самочувствие. Когато дадена снимка, пост или клип, който ние сме направили, събере много „лайкове“, се чувстваме удовлетворени, а когато не направи, започваме да се питаме какво се е случило с нас, грозни ли сме, защо тази снимка не събира толкова харесвания колкото предишната? Всичко това влияе отрицателното върху психическото ни здраве, затова Инстаграм се опитва да скрие лайковете, което ще се окаже предизвикателство за големите бизнеси и инфлуенсърите, защото доколко един продукт е популярен, зависи от това колко хора са харесали поста, свързан с него. Инфлуенсърите, които са рекламно лице на дадена компания, не е нужно да зависят изцяло от лайковете на техните постове, например те могат да направят анкета с различни варианти на продукта и да оставят техните последователи да решат кой от вариантите най-много харесват. Да проведат собствено проучване или да поискат обратна връзка. За да може да не зависим изцяло от социалната медия, трябва да се откъснем от този псевдоперсонаж, който използваме, за да се представяме за по-добри отколкото всъщност сме в реалния живот. Можем да направим това, като лимитираме времето, прекарано в социалната медия, и излизаме повече с приятелите и семейството си.

Развитието на технологиите и изкуственият интелект не би трябвало да нарушават основните ни човешки права, правото ни на личен живот и лично пространство. Всяко посегателство върху личните данни на даден човек е посегателство върху личността, такива каквито са кражбата и злоупотребата с тези лични данни и друга чувствителна информация.

Използвани данни и допълнителна информация към темата:

https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_bg (използван цитат)

<https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/fs-fi/choice-choix/>

Информация за това защо Инстаграм скрива лайковете – <https://later.com/blog/hidden-likes-instagram/>

Информация за негативните ефекти от технологиите – <https://www.businessinsider.com/technology-negative-bad-effects-society-2019-8#your-eyesight-can-also-suffer-from-too-much-device-usage-2>

Информация за това защо уроците по киберсигурност са важни за подрастващите – <https://www.psychologytoday.com/us/blog/raising-humans-in-digital-world/201904/parenting-in-digital-age-what-experts-are-saying>

Информация за интернет лагерите за рехабилитация в Китай – <https://nypost.com/2017/08/29/inside-the-brutal-world-of-chinese-internet-addiction-camps/> (използван цитат)

Повече информация за негативните ефекти от технологиите и защо прекалено многото време прекалено пред телефон/компютър е вредно за децата – <https://www.healthline.com/health/negative-effects-of-technology#effects-in-kids>

<https://www.reputationdefender.com/blog/privacy/top-ten-reasons-keep-your-personal-information-private> (използван цитат)

<https://www.unicreditbulbank.bg/bg/blog/2015/11/25/8-nachina-da-se-predpazite-ot-krazhba-na-samolichnost/>

<https://spunout.ie/sex-relationships/dating/leaking-nudes>

ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО

Василена Георгиева Хърсева

*„Нищо не е по-прекрасно от изкуството да бъдеш свободен,
нищо не е по-трудно от това да се научиш как да си използваш свободата“*

Алексис дьо Токвил

Какво са личните данни? Това е нашата идентичност. Уникална, различна и неповторима за всяко живо същество. Всеки човек има свой таен код, в който е скрито всичко за теб, мен или който и да е човек. В тях откриваме цялата информация за нас, нещо като кодирана автобиография: имена, адрес, дата на раждане, място на раждане, ЕГН и много друга информация. А какво е за теб свободата? Това е правото на всеки да изразява себе си, да казва ясно това, което мисли, без да се притеснява. Да споделяш дадена информация за теб и никой да не злоупотребява с това твое право. Дигиталната общност е навсякъде около нас. Всеки човек е в дигиталния свят: в социалните мрежи или в някоя друга интернет страница. Но дали осъзнаваме колко опасности дебнат там?

Живеем във времена, в които интернета е част от нашето ежедневие. Почти няма човек, който да не го е използвал поне веднъж в живота. Вече е лесно да търсиш информация в интернет и да знаеш как да отсееш грешната. Сега можеш да откриеш информация за нещо просто с един клик, а не както преди години да стоиш часове наред в библиотека и да събираш информация от най-различни

стари книги. Сега е много по-лесно да общуваме с близки за нас хора и да ги виждаме, където и да се намират. Можеш да разпуснеш след дългия работен ден, като разглеждаш профилите в социалните мрежи на твои близки и не чак толкова близки приятели. Да видиш какво са правили днес, къде са ходили, с кого са се видели, какви снимки са качили... или просто да си пуснеш интересен филм. А колко лесно е пазаруването онлайн: стоиш в удобния фотьойл, натискаш два пъти с мишката и вече си купил новите маратонки, които толкова много искаш...

Но с всички тези възможности идват и много скрити рискове за всеки от нас. Трябва да знаем как да се защитим в тези ситуации. Най-лесно можем да споделим информация за нас в социалните мрежи или като си правим регистрация в даден сайт. Трябва да сме информирани какво можем да споделим в тях за нас и какво не е редно да се споделя. Кое може да бъде използвано срещу нас и кое не. Да знаем на кого може да се доверим и на кого не бива да се доверяваме. Най-важно от всичко това е да знаем, ако се почувстваме заплашени в интернет пространството, към кого можем да се обърнем за помощ.

С това не искам да кажа, че трябва да работим със сложни програми или команди. Нито да знаем подробности за всяка социална мрежа, понеже те имат доста сложни функции. Имам предвид че преди да натиснем бутона „Съгласен съм“, трябва да сме прочели всички условия, написани дори с най-дребния възможен шрифт. Доста често точно в този дребен шрифт са скрити различни атаки. По този начин се съгласяваме дадено приложение или сайт да се рови в нашия телефон или компютър, защото сами сме се съгласили за това нещо. Да знаем, че в момента, в който се съгласим даден сайт да използва „бисквитка“, му разрешаваме да следи всяко наше търсене и да има цялата ни хронология от това какво сме търсили сега или преди това. Трябва да знаем как да се предпазим от някой, скрит в анонимността, позволена в интернет пространството, ако ни обижда, опитва се да ни изнудва или заплашва по някакъв начин. Да знаеш какво е чувството да си обграден от много приятели в интернет пространството, а всъщност да си един от най-самотните хора. Да живееш във виртуалния свят е колкото полезно, толкова и безполезно, да си мислиш, че целият ти живот е там, а щом изключиш екрана, да видиш, че всъщност си сам.

С всички тези нови и нови технологии, които излизат всеки ден, децата не са както бяха преди години. Някога беше важно да си грамотен, да можеш да четеш и да пишеш, правилно да се научиш да смяташ. С напредване на технологии това става все по-трудно и по-трудно. Всички деца вече се концентрират по-трудно отколкото преди години, понеже има повече забавления от преди. Сега, като излезеш на разходка в парка или седнеш на кафе, не виждаш деца, които бягат и играят, а все по-честа гледката е седнали пред телефон или таблет. Подрастващите вече общуват помежду си все по-малко и по-малко отколкото преди години. Това не е нито лошо, нито безполезно: все пак е период на еволюция, с който ние трябва да свикваме. Всички тези промени са за наше улеснение. За това всеки човек трябва да се адаптира към този начин на живот, както училищната система, така и начина, по който възпитаваме децата си, за да може всички тези промени, които идват всеки ден, да са от полза и да носят само положителното в нашия живот. Няма смисъл да мрънкаме и да се убеждаваме колко е вреден интернет за съзнанието, здравето и обучението на подрастващите... Всъщност точно интернет дава безброй много възможности за тях: дали ще е под формата на забавни и интересни игри, които развиват ума на децата, или филмчета; дава възможност да учат чужди езици, да събират и изваждат, правилно да изговарят думите. Дигиталното общество ограмотява децата от най-ранна възраст, стига да ги мотивираш и да им покажеш богатото интернет пространство, така в последствие могат да се избегнат много проблеми и най-различни опасности.

Какво е да си грамотен човек в този напреднал свят на все повече нови технологии? За да сме грамотни и да се отнасяме сериозно към тези неща, трябва да ни учат в училищата от най-ранна възраст. За да се случи това обаче, трябва да имаме добри специалисти. Колкото по-рано започнеш да учиш едно дете на богатството на интернет пространството и как да се пази и защитава там, толкова по-добре ще бъде за него. Не трябва само да ги учиш как се правят презентации или как се пише cv на word, това всеки един може да научи с няколко изгледани клипа. Още в самото начало трябва

да бъдат запознати с опасностите в интернет. Необходимо е да знаят какви скрити рискове се крият в онлайн пространството, колко са важни личните данни за всеки от нас и как да се предпазим от някой злонамерен, който иска да се възползва от тях. Колкото по-малки са, толкова повече попиват всяка информация, която им кажеш.

Но за да стигнем до това огромяване, първо, трябва да започнем от възрастните – самите те да осъзнаят колко е важно да пазиш своите лични данни, а не от децата. Когато осъзнаят това, тогава сами ще учат децата си да внимават. Дигиталната сигурност не трябва да се обсъжда от време на време по новините, когато стане кражба или изтече информация, за нея трябва да се говори свободно, да се обсъжда, за да сме наясно всички с това. Когато се регистрираме в даден сайт или пък правим поръчка за даден продукт, защитата на нашите лични данни трябва да е на първо място, да внимаваме какво въвеждаме и на какво се съгласяваме. В моментите, в които се запознаваме с непознат за нас човек, също трябва да мислим до колко можем да се доверим и какво всъщност можем да му доверим от нашия живот... Всеки има инстинкт за самосъхранение, интересното обаче е, че, когато отворим компютъра или включим смартфона си, този инстинкт сякаш изчезва и много лесно се доверяваме на всичко и по този начин ставаме лесна мишена за най-различни хакери.

Освен че могат да ти бъдат откраднати личните данни и да злоупотребят с тях, след като посещаваш дадена интернет платформа или дадени мобилни приложения, съществува още един проблем, от който трябва да се предпазим и с него да бъдат запознати както по-възрастните, така и младите хора. Всеки използва онлайн пространството по различен начин, лично аз в момента комуникирам с всичките си преподаватели онлайн, заради пандемията, с по-голямата част от тях дори не сме се виждали на живо. И въпреки че всичко става чрез онлайн платформи и имам сигурността, че те са професори, доценти в университета, пак трябва да бъдем внимателни каква част от личните си данни представяме на тези хора. Все пак винаги има риска зад екрана да е друг човек, а не този, за който се представя. Затова трябва да сме отговорни до каква степен ще дадем информация на тези хора. Често хората се подвеждат и споделят с напълно непознат лични неща за себе си, семейството и приятелите си, а след това се злоупотребява с тази информация. След като сме споделили толкова неща за себе си, ставаме лесна мишена: заплашвани, изнудвани, а в някой от случаите даже и по-лошо... За това трябва да говорим открито и свободно за тези опасности, всички трябва да бъдем информирани понеже това не се случва само при подрастващите, а и при по-възрастното поколение. На тези неща не трябва да ни учат само в университета или в дадена школа, в която си се записал, или да слушаме за поредния измамен пенсионер в късната емисия новини и само да ти кажат „Пази си личните данни, не се доверявай!“.

Свободата и сигурността в дигиталното общество за мен е цялостното използване на всички ресурси, които ни предлага онлайн пространството – както можем да учим много неща от него, така можем свободно да изразяваме своите мисли и мнение за изкуство, да гледаме филми; да се самоусъвършенстваме, да комуникираме с нашите близки, които са близо до нас или са на другия край на света; можем да се изявяваме, да рисуваме или чертаем дадена скица, или дори за вдъхновение... Дигиталният свят е толкова богат, че можем да поемаме от него безброй много информация, но зад всичко това се крият и много опасности. За да го използваме, преди всичко трябва да се чувстваме и защитени. Аз, като представител на младото поколение в България, съм на мнение, че киберсигурността е едно от най-важните неща, за което трябва да се говори постоянно, а не само в университета, когато запишеш тази специалност, понеже искаш да се занимаваш с това. Трябва да говорим свободно и всеки да има достъп до тази информация, както за нашата сигурност, така и за нашите близки. Необходимо е да имаме такава информация, за да сме спокойни и да не се притесняваме да боравим с онлайн платформите. Но тези промени, преди всичко, започват от нас самите. Ако не се решим на тази важна крачка, няма кой да го направи вместо нас. Всички ние трябва да бъдем грамотни и да защитаваме нашите лични данни – сега, не след година. Не трябва да чакаме да станем жертва, да ни бъдат откраднати личните данни или на някой наш близък, и едва тогава да започнем да се огромяваме как да се защитим от подобни измами. За да се чувстваме защитени

и свободни в дигиталното общество, трябва да сме грамотни и много отговорни, както в реалния живот, макар че много хора забравят за тази защита, когато са онлайн. Първата ни мисъл трябва да е „Бъди предпазлив!“, а не да спираме да мислим за това, понеже по този начин ставаме уязвими.

ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО

Дамяна Янкова Янева

Още преди да поема първата си глътка въздух, моето семейство се е ангажирало да реши под какво име ще бъде идентифицирана в обществото. След раждането ми съм имала честта да получа първия си личен документ, след предоставянето на личните данни на майка ми и на баща ми, както и документ, в който е описано, че те са сключили граждански брак. И така, преминавайки през жизнения ми цикъл, бивам вписвана в различни регистри на множество институции. Някои от документите, които притежавам, като лична карта и свидетелство за управление на моторно превозно средство, са ми винаги под ръка, тъй като съществуват компетентни длъжностни лица, определени със закон, които имат право да ми ги поискат за проверка. Родена в двадесет и първи век, с осигурен достъп до интернет и социални мрежи, разполагам с пълна свобода в дигиталното пространство и така бивам разпознавана лесно в сайтовете, в които съм регистрирана. Добре е човек да бъде свободен, но дали ще бъде защитен в това огромно пространство? Преди да се възползва от нещо, всеки следва да се запознае предварително. Всеки сам носи отговорност за постъпките си, но би било по-добре, ако няма нежелани последствия заради неправилно боравене с идентификационните данни, които ни правят един завършен и дееспособен субект. Като настоящ студент на Икономически университет – Варна и бъдещ счетоводител осъзнавам, че е изключително важно добре да познаваме законите и правилните за прилагането им, както и да сме запознати с дейността на институции, включително и с дейността на Комисията за защита на личните данни.

У дома следва да имаме място за съхранение на всички важни документи. Разбира се първият по важност, а именно актът за раждане, следва да се пази изключително много, тъй като това е единственият ни официален документ, който притежаваме преди да навършим пълнолетие и да ни се издаде лична карта. Това е картата, която удостоверява самоличността ни. Едва ли съществува нещо, което можем да предприемем, без да я представим. Копирането ѝ представлява действие по обработване на лични данни, което е свързано с тяхното събиране и съхранение. За да ни копира картата, дадено лице трябва да има правно основание, регламентирано в нормативен акт. Винаги трябва да бъдем информирани за целта на заданието. Мобилните оператори, както и работодателите ни, нямат право да копират нашия личен документ. След като им предоставим данните, които са нужни за осъществяване на дадено събитие, следва да приберем документа си, разбира се ако изобщо сме решили да го предоставим, тъй като имаме пълното право да откажем да бъде копирана нашата карта. Ако личната ни карта бива неправомерно копирана, можем да подадем жалба до Комисията за защита на личните данни. При промяна на адрес, загуба или повреждане на картата, както и поради други събития, следва да си издадем нова – вече има опция за електронно заплащане на таксата за издаването ѝ. При зареждането на картата за градския транспорт се поисква и лична карта. Виждам как ученици показват личната си карта, която е снимана и от двете страни, от телефона. Това е интересна инициатива, но не би помогнала във финансова институция например. Два дни след като получих личната си карта, пресякох улицата по неправилен начин и бях учтиво помолена да представя личните си документи. Да, но тогава те не бяха у мен. Със сигурност щеше да има доста последствия, но полицаят беше добър човек спрямо едно четиринадесет годишно дете. Гдини по-късно отивах на училище и по пътя изгървах портмонето си. Тогава загубих личната си карта и трябваше да заплатя

за издаването на нова. След тези две събития се научих да се отнасям изключително отговорно към този документ.

Мечтата на някои от моите познати е да могат да шофират. Но, за да го правиш законно, трябва да притежаваш свидетелство за управление на моторно превозно средство. Когато се записах на курс за шофьор, не знаех, че трябва да предоставим свидетелство за завършено основно образование. В социалните мрежи си направих снимка, държейки дипломата си за средно образование и първоначално си помислих, че трябва да предоставя точно този документ. Обаче се оказа, че трябва да предоставя съвсем друг. Това беше причината да си подрежда абсолютно всички документи по ред на издаване, поставяйки ги в джобове и папки за съхранение. След като се получи документът за шофьор, започва поредица от снимки с него в колата и пред нея. В последствие снимката със свидетелството е в социалните мрежи, но с неприкрити имена и единен граждански номер. Съществуват варианти за взимане на кредит, за което са нужни само имената, ЕГН и няколко клика на телефона. Току-виж сме задължени с няколко хиляди заради капка известност в интернет пространството. Като един работоспособен и здрав човек вярвам, че ще се въздържа от опцията за бърз кредит. Освен наплива от снимки на шофьорски книжки има и втори наплив, а именно от снимки на диплома за средно образование или свидетелство за професионална квалификация и то със снимка на страницата, в която се виждат абсолютно всички данни, снимки и номера.

Съществуват групи в социалните мрежи, в които се публикуват намерени документи. Добро дело е да върнеш документите на притежателя им, ако си ги намерил, но е хубаво преди да търсиш лицето, да закриеш личните данни. Преди време моя приятелка откри дебитна карта на земята, докато се разхождахме. Тя обмисляше да я изхвърли като я счупи, но не можех да оставя нещата така и реших да поема казуса в свои ръце. Освен сметката на субекта на дебитната карта вече има и снимки. Започнах да изпращам съобщения на почти всяко лице, което приличаше на човека от снимката на картата. Така успях да открия собственика. Без да снимам, без да разпространявам данни, върнах картата и за благодарност ми подариха шоколад. Това ми напомня и за друга случка, през зимните месеци, в които открих телефон в снега. Тогава постъпих по същия начин – върнах телефона на собственика... Е, да, моите документи, години след като ги загубих, така и не се откриха, но доброто у мен отново победи. Когато върнах телефона, не поисках нищо, тъй като знаех какъв ужас изпитва човек, ако някой влезе в профила му с социалните мрежи. Изключително важно е при ползване на чужди смарт устройства да не забравяме да излизаме от профила си, тъй като има хора, които влизат в чуждия профил и започват да пишат от негово име, организират срещи, качват снимки и прочие. Не трябва да предоставяме паролата си за достъп на никого. Тази парола трябва да е достатъчно сигурна, за да може да дава макар и малка защита от опити за влизане в профилите ни.

Всеки е свободен и може да качва каквото си поиска. Какво закусва и обядва, с кого излиза на среща, къде се намира в момента, може да си сложи за профилна снимка и пин кода за дебитната карта. Да, може всичко! Но не е редно. Институции като Националната агенция за приходите и Националният осигурителен институт издават персонален идентификационен код на лицата, с който те могат да правят справки за доходите, дължимите задължения, бъдещи приходи и др. За да разполага с тези кодове, лицето трябва да ги е получило лично. При всяка справка следва да се въведат данните, което напомня, че те не трябва да се предоставят. Преди години се е губело изключително много време, докато се чака, за да се извърши дадена операция в различни финансови институции. И тъй като времето е пари, вече съществува онлайн банкиране. Макар и да дадох съгласието си да имам тази опция, все още не съм отворила приложението. Породено от нежелание за плащане на допълнителни такси, макар и да е упоменато, че няма такива, или от страх да не се случи нещо с личните ми данни и финансовите средства в картата, навярно и след още пет години все още приложението ми няма да бъде отворено.

Един от принципите на счетоводството е документалната обоснованост. Той гласи, че дадена операция е налице, когато е документално обоснована. В тези документи има данни на поне едно физическо или юридическо лице. Ако се обърка едно число или буква, ще се състави грешен документ,

ще последва анулиране и други нежелани събития. Отговорността на счетоводителя е огромна, тъй като се носи от лицето, подписало дадения документ. Документите следва да се съхранят правилно по време на осъществяване на документооборота, а именно проследяването на целия път на документа от съставянето му до прилагането му на правилното място в счетоводния архив. Един счетоводител следва да се отнася с огромно уважение към работата си, за да бъде ценен от клиентите си, така те могат да му се доверят и да му дадат достъп дори до паролата на профила си за онлайн банкиране. Разликата между личните данни и дигиталното пространство е, че в утрешния ден ние може да имаме регистрации не в четири, а в шест сайта или обратно, но личните данни, които ще трябва да въведем, за да имаме достъп, ще останат едни и същи. Когато отидем да теглим парични средства в банката, ще искат нашата лична карта и ние да подпишем банковото извлечение. За да започнем работа или да сключим брак, ще искат нашите документи... На базата на изложеното до тук, следва да твърдим, че трябва да се отнасяме с внимание и уважение към нашите лични документи, защото те ни идентифицират и се явяват нашата връзка със света и дигиталното пространство. Трябва да приемем като задължение, да четем правилата, преди да натиснем бутона, който гласи, че сме съгласни с политиката на даден сайт. Преди да удостоим с подписа си, трябва да сме прочели всеки ред, дори и този с малкия шрифт. Ние носим отговорност за действията си. Ако утре нещо се случи без наше съгласие, шансът ние да сме виновни, заради това че някъде, някога не сме прочели нещо докрай, е над 50 процента, породен от неправилно съхранение и предоставяне на документи. И не трябва да забравяме, че има поне два варианта да подадем жалба при съмнение за злоупотреба с личните ни данни към Комисията за защита на личните данни.

Източници:

bg.wikipedia.org

www.cpdp.bg

ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО

Джемиле Ивкова Читакова

Днес ние живеем в дигиталната епоха. Дигиталното общество ни предоставя много възможности: да работим онлайн, да се обучаваме онлайн, да правим онлайн разплащания и т.н. Това подобрява живота на хората и ефективността на гражданите в много области¹. Скоростното разпространение на средствата за масова комуникация проникват във всяка сфера на съвременния живот, от икономика до общество и култура, и оформя ежедневието ни². Интернет играе все по-голяма роля и служи за виртуален пазар на продукти, идеи и информация. С това бързо развитие трябва да се намери баланс между икономическите интереси и правото на защита на личните данни³.

Затрупани сме с все повече и повече информация. Интернет, най-новото електронно средство за масова комуникация, е широко разпространен и се използва от голяма част от населението. Най-бързо развиващият се сегмент в интернет пространството е броят на потребителите на мобилни социални медии⁴ като Фейсбук, Инстаграм, Туитър и други подобни. Лесно е да се провери колко

1 <https://libreresearchgroup.org/en/a/digital-society#>

2 <https://www.unicef.org/bulgaria/media/426/file>

3 <https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20080121STO19257+0+DOC+XML+V0/BG>

4 <https://bg.vpnmentor.com/blog/%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%82%D0%B5%D0%BD%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B8-%D1%81%D1%82%D0%B0%D1>

хора използват тези приложения. Само при една проверка в Google Play Magazine става ясно, че Фейсбук има над 5 милиарда потребители, които са изтеглили приложението. Става въпрос за 2/3 от населението, а то е повече от половината от световното население.

Но колкото и полезно да е интернет пространството, то крие рискове. Няма съмнение, че някой следи всяко наше действие в социалните мрежи. За да защита тезата си, ще дам един пример от личния си опит. Влизам в някакъв сайт, за да разглеждам дрехи. След като приключа с разглеждането, затварям страницата и влизам във Фейсбук, където се появяват реклами на същите дрехи, които съм разглеждала в този сайт. Случайност?! Не мисля! Всичко, което правим, се следи и се използва за комерсиални цели⁵. Властта и влиянието на частния сектор трябва да се използват за усъвършенстване на етичните стандарти в областта на данните и неприкосновеността на личния живот сред цялата индустрия, както и за други практики, които са от полза и в защита на потребителите⁶. Регламент (ЕС) 2016/679) въвежда нови, по-високи изисквания към регулирането на неприкосновеността на личните данни. Той ще предизвика сериозни промени във всяка бизнес сфера, включително и в начина, по който търговските организации събират и обработват информация за своите клиенти и в най-висока степен нейната защита⁷.

Необходимо е да си зададем въпроса достатъчно защитено ли е интернет пространството и какви рискове, свързани с личните данни, крие. Има потребители, които споделят много информация в социалните мрежи, има и такива, които са само наблюдатели. На всички ни е ясно, че съществува значителен брой хора, които злоупотребяват със свободата в интернет. Те го правят с някаква цел – било за отмъщение, подкуп или просто от желание да се навреди на някого. Изключително много злоупотреби се правят и с електронните разплащания. Съвременното общество използва множество платежни системи и средства, така разплащанията в брой биват изместени от електронните разплащания⁸. И автоматично отговорът на въпроса по-горе е, че не сме достатъчно защитени и дигиталната среда крие множество рискове както за нас самите, така и за личните ни данни. Естествено, че не е решение да спрем да използваме предоставените ни услуги, а да знаем как да се защитим при потенциални заплахи. За да се случи това, е нужно да имаме дигитална грамотност, трябва да разпознаваме тези опасности и да умеем да се защитаваме. Всичко зависи от това в каква степен ние, като общество, сме достатъчно ангажирани, за да се ограмотим дигитално. Ние, потребителите, не следва да разчитаме на добросъвестното поведение на останалите участници в реална или онлайн среда, а да приемем като своя отговорност опазването на личните си данни⁹.

В заключение ще обобщя, че е нужно да придобием определени компетентности, за да можем да използваме ефективно възможностите, които ни предоставя онлайн средата. Всеки от нас е потенциално застрашен както от злоупотреби с личните данни, така и с нас самите. Наша лична отговорност е да се погрижим да направим интернет пространството по-сигурно.

„Ако искаме интернет да бъде свободен, той трябва да е сигурен”

Джеймс Лоусън, Съвета на Европа.

⁵ https://econ.bg/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%D0%B8/%D0%A1%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B0%D1%82%D0%B0-%D0%B2-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D0%B8-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D0%BA%D0%B0%D1%82%D0%BE-%D1%81%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4%D0%B0_1.a_i.400176_at.4.html

⁶ <https://www.unicef.org/bulgaria/media/426/file>

⁷ https://library.ue-varna.bg/_layouts/15/IUVarnaLirexPart2/ViewFile.aspx?p=11898&g=5fb99cc9-bbe4-4e5c-9b88-108a0f6be044&t=3

⁸ https://library.ue-varna.bg/_layouts/15/IUVarnaLirexPart2/ViewFile.aspx?p=11898&g=5fb99cc9-bbe4-4e5c-9b88-108a0f6be044&t=3

⁹ https://library.ue-varna.bg/_layouts/15/IUVarnaLirexPart2/ViewFile.aspx?p=11898&g=5fb99cc9-bbe4-4e5c-9b88-108a0f6be044&t=3

ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО**Ева Григорян**

Бъдещето на всички ни е тясно обвързано с дигиталната сфера. Смята се, че един от първите изследователи, които използват термина „дигитална грамотност“, е Пол Гилстър през 1997 г. в едноименната си книга (Gilster 1997). Този термин, предшестван от дългогодишни изследвания, се представя с информационна грамотност и компютърна грамотност.

Личните данни са именно индивидуалната информация, която всяко лице притежава. Отделни данни, които събрани заедно могат да доведат до идентифициране на конкретно лице; всяка законова информация, валидна за конкретното лице. Това представляват личните данни и тяхната поверителност е от изключителна важност.

Развитието на технологиите, на дигиталните среди, на компютърната грамотност... С всеки миг все по-често се сблъскваме и заедно с това изпитваме необходимост от всичко изброено. Виртуалният свят е достъпен за всички, желаещи и нежелаещи да се докоснат до него. А свободата в това омагьосано пространство става все по-необхватна за човешкото око. Съответно – непозната, необяснима, неконтролируема, дори опасна.

Смята се, че в известен смисъл свободата би могла да се представи като синоним на „правото“. Така например свободата на изразяване или свободата на словото са едни от най-важните граждански свободи. Свобода е способността на съзнанието да мисли и действа в съответствие с волята на самия човек, но във връзка с по-висши закони и порядък. Във философията идеята за свобода включва свободната воля, която контрастира с детерминизма. В политиката свобода е свободата от правителствена принуда. В теологията свобода е свободата от робството на греха. В дигиталното общество обаче свободата, е не просто свобода, това е свободия в най-широкия смисъл на думата. Ако в реалния свят да си свободен означава да направиш една крачка, то във виртуалния с един клик на мишката можеш да отидеш в друг град, да посетиш известна личност, дори да надникнеш в хола ѝ, виждайки както обзавеждането, така и всички лични данни и детайли за живота ѝ. Можеш да изстреляш ракета в космоса или да предизвикаш срыв в глобална мрежа. Всичко това е пред теб на малкия екран, докато в действителността това не би могло да се постигне или поне – не с такава лекота.

Всичко казано до тук е възможно. И с всеки изминал ден възможностите, които ни предоставя необятното, магическото дигитално общество, стават все по-големи, по-предизвикателни, примамливи, защото новото и непознатото винаги е будело любопитство. Любопитството е в зародиша на големите открития. И така, кръговратът продължава... към бъдещето.

За да се предотвратят някои нежелани опасности от тази свободия в онлайн средите и дигиталното общество, Европейският парламент взема решение на събрание от 27 април 2016 г. С това решение се въвежда Регламент, с който се поставят под защита физическите лица във връзка с обработването на личните им данни и относно свободното движение на такива данни.

Според Регламента: „Обработването на лични данни следва да служи на човечеството. Правото на защита на личните данни не е абсолютно право, а трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа на пропорционалност. Настоящият регламент е съобразен с всички основни права и в него се спазват свободите и принципите, признати от Хартата, както са залегнали в Договорите, и по-специално зачитането на личния и семейния живот, дома и комуникациите, защита на личните данни, свободата на мисълта, съвестта и религията, свободата на изразяване на мнение и свободата на информацията, свободата на стопанската инициатива, правото на ефективни правни средства за защита и на справедлив съдебен процес, както и културното, религиозното и езиково многообразие“. Още от Регламента:

„Принципите и правилата относно защитата на физическите лица във връзка с обработването на личните им данни следва, независимо от тяхното гражданство или местопребиваване, да са съобразени с техните основни права и свободи, и по-конкретно – с правото на защита на личните им данни. Настоящият регламент има за цел да допринесе за изграждането на пространство на свобода, сигурност и правосъдие и на икономически съюз, за постигане на икономически и социален напредък, за укрепване и сближаване на икономиките в рамките на вътрешния пазар, както и за благосъстоянието на хората“.

Абсолютно всяко лице, притежаващо компютър или мобилно устройство, има достъп до свободата на дигиталното общество. Дали обаче притежава нужната компетентност, за да се справи с тази свобода? Дали всяко лице, умеещо да включи компютър и да работи с периферните устройства, е дигитално грамотна личност? Дали това, че можеш да кликаш с мишката, значи, че можеш да изстреляш ракета в космоса? Не. Това далеч не е така. Нагледно може да се даде пример с това да държиш молив, но да не познаваш писмеността. Незнанието също е изключително опасно и в един неограничен, магичен свят би могло да е дори пагубно. Ето защо са ни необходими граници, насочващи ни към възможностите, които ни предоставя дигиталното общество. Да знаем как да използваме свободата си и да се пазим от неприятности, да знаем как да опазим личните си данни, защото те са нашият идентификатор, слабото място на всеки. Най-важното, дори и за знаещите, и можещите, е да не злоупотребяваме със свободата, която ни е предоставена, и да не я превръщаме в свободия.

Законите и правилата, както правни, така и морални, не са измислени случайно. Въпреки че дигиталните среди са всеобхватни, е добре да има общоприети правила като Регламента за защита на личните данни, които всеки потребител на виртуалния свят да се стреми да спазва. Чрез тези норми постигаме хармония и баланс, необходими за мирно съжителство както в действителността, така и сред дигиталното общество.

ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО

Михаела Теодорова Тодорова

С развитието на дигитализацията и бързия обмен на информация се зараждат нови възможности за злоупотреби, включително и с лични данни. Онлайн пространството е привлекателно за измамниците, защото се чувстват по-спокойни и по-защитени зад анонимния профил. Същевременно бързият обмен на данни ги затруднява, защото интернет потребителите научават за новите им престъпни методи и това принуждава измамниците да подобряват своите стратегии и цели. За да се намалят злоупотребите, се разработват различни програми и кампании за борба с дигиталните престъпления на местно, национално и международно ниво.

Във връзка със злоупотребите с личните данни (не само в дигиталното пространство) Европейският съюз разработва Общ регламент за защита на личните данни (GDPR), в който се регламентират правата на физическите лица. Една от целите на споменатия регламент е да въведе организационни и технически мерки за сигурност, както и защита на човешките права в механизмите за съответствие в новите технологии за обработка на данни. Цели се да се постигне взаимно доверие между администратори, обработващи и притежатели на лични данни. Според GDPR Group голяма част от европейците са на мнение, че личните им данни не са достатъчно защитени в онлайн пространството¹⁰.

На база наблюдения, а не специализирано проучване, споделям мнението, че внедрените мерки във връзка със защитата на личните данни в България се приемат като задължение и се определят като досадни и „губещи времето“. За пример можем да разгледаме един оператор на

лични данни – да се подсетим за последното ни преживяване в банков офис, когато сме откривали нова сметка. Служителят, колкото и да е доволен от сключената сделка, трябва да изпълни стриктно всички стъпки за осъществяването на избраната от нас операция. В един момент ни подават различни документи за подпис от наша страна. Колко ли от потребителите се замислят за смисъла на всеки един от документите и колко от тях се доверяват на имиджа на банката и си казват „Такава е политиката на банката и това е стандартна процедура. Ако не подпиша всичките неща, няма да ми предоставят желаната от мен услуга“? Колко от потребителите приемат необходимата документация за излишна „бумащина“?

От гледна точка на служителя декларацията за доброволно предоставяне на личните данни е само една точка от списъка, който трябва да обработи, за да изпълни своето задължение стриктно. С този пример се забелязва цялостното отношение на страните във връзка със защитата на неприкосновеността, което често граничи с безразличие и дори досада. Дали в дигиталния свят това се възприема по същия начин?

В банката доверието е сравнително голямо, защото при възникнал проблем знаеш от кого и как да търсиш отговорност, докато в дигиталната среда никога не можеш да бъдеш сигурен кой точно е от другата страна. Именно това превръща предизвикателствата пред защитата на личните данни в по-актуални и цифрови.

В някои случаи изискванията по регламента отново се възприемат като излишни, защото причиняват неудобство на потребителите (отнема им се от времето да прочетат и да се съгласят с условията) и на програмистите (трябва да са запознати в детайли, за да не пропуснат нещо важно). На пръв поглед съгласието за доброволно предоставяне на личните данни често представлява „клик“ върху един бутон, но практически е много повече. За съгласяващия се, ако превърне в навик да предоставя своето съгласие, съществува риск в дадена ситуация да приеме неблагоприятни за него условия. От гледна точка на разработчиците на продукта този бутон е свързан с допълнителна работа и усилия.

Благодарение на регламента за защита на личните данни на физическите лица част от потребителите „сърфират“ в дигиталното пространство по-свободно и спокойно, защото се чувстват в безопасност. Същевременно е необходимо всеки да бъде с повишено внимание, защото практически е невъзможно заплахите от злоупотреби с личните данни да бъдат напълно занулени.

ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО

Сиана Атанасова

„Лични данни“ – това е всяка информация, свързана с идентифицирано или идентифицируемо живо физическо лице. Като такава се приема: собствено име и фамилия, домашен адрес, имейл адрес, номер на картата за самоличност, данни за местоположение (напр. функцията за данни за местоположение на мобилен телефон), адрес на интернет протокол (IP).*

Регламент 2016/679 на Европейския парламент

Директива 2002/58/ЕО 12.07.2002

Въпросът с личните данни и свободата в дигиталното общество, по своята същност, е силно антагонистичен. Мнозина, обгърнати в тъмата на този антагонизъм, възприемат свободата като слободия, анархия, беззаконие а личните данни за тях са средство за кражба, измама, манипулация и психологическа атака. С всеки коментар или снимка, с всяка отворена страница или споделена връзка анонимните знаят не само нашето име, фамилия и адрес, а също и какво обичаме, какво гледаме, от

какво се възмущаваме и кого подкрепяме. На сървър в студени подземия е записан целият ни живот, усмивки и сълзи, споделени приятелства и лукави предателства.

Древния мислител Лао Дзъ е казал: „За да предвидиш бъдещето, опознай добре миналото“.

Нека си припомним коя стока е била най-високо ценена в миналото, но и днес, способствала за много исторически победи, за кървави революции или печалба на милиарди в рамките на часове... Достъпът до информация. Това е светият граал в нашето съвремие. Пълният достъп до информация чрез подходящ алгоритъм може да създаде с почти абсолютна точност нашия характер, навици, привычки на всеки от нас, а личните данни дават само материален образ на създадения виртуален образ. От това се възползват анонимните в мрежата. За тях мрежата е паяжина а хората са жертви, попаднали в нея. Анонимните нямат лице, име, нямат цвят, идея, те имат само един бог – парите. За тях законите са врата в полето.

Възможно ли е тези, които задават моралните категории – свобода, ред, законност – да са тези, които злоупотребяват с тях? Възможно е – Едуард Сноудън – анализатор на данни, работил в ЦРУ, обработвал и предоставял информация за нищо неподозиращи хора, следени от разстояние.

Възможно ли е, абстрахирайки се от категорията „лични данни“, социални мрежи да предоставят срещу пари информация за нас без наше знание? Възможно е – Фейсбук предоставя пълна информация за над петдесет милиона клиенти на компанията на фирмата „Кеймбрич Аналитика“, която чрез специален алгоритъм таргетира и атакува с рекламни послания за определен кандидат президент.

Възможно ли е чрез позоваване на „свободата в дигиталното общество“ да се организират вандализми, да се чупят статуи, да се провокира насилие? Възможно е – Движение „Антифа“, чрез социалните мрежи, организира поругаване на статуите на Дж. Вашингтон, на президент Линкълн и ген. Ли.

Логично стигаме до въпросите: Къде е границата между използването на личните ни данни и свободата в дигиталното общество? Кой има право да ги обработва и кой да ги предоставя? Как да се идентифицираме през света, без да предоставяме целия набор от лична информация?

Границите, както винаги се задават от обществото и е време този дебат да започне колкото е възможно по-скоро, да се зададат ясни параметри и критерии за оценка на риска, да се вземат решения не само в интерес на транснационалните корпорации а в интерес на обикновения човек.

Виждаме, когато частни фирми и компании обработват наши данни, до какви проблеми и катаклизми се достига – може би трябва да се наложат регулации и интервенции от държавата с цел предпазване от злоупотреба с личните данни...

Известният американски социолог Самюъл Хънтингтън възкликва в началото на ХХІ век пред студентска аудитория: „Страх ме е, че ще дойде време да представим човека като съвкупност от цифри“. Видния идеолог може би осъзнава, че ако човек се опише като съвкупност от нули и единици, ще загуби своята душа, чувства, емоции. Дали математиката може да опише човека, дали освен образ ще може да пресъздаде и неговата самобитна идентичност?!

Наскоро професорът по икономика Клаус Шваб публикува статия в която се твърди, че благодарение на квантовите компютри, изкуствения интелект, нанотехнологиите, биотехнологиите и телемедицината сме пред прага на четвъртата индустриална революция – сливане на физическия, дигиталния и биологичен свят. При дискусия в Станфорд бил заден въпрос: „Г-н професоре, има ли яснота кой ще отговаря за сливането?“. Шваб отговорил: „Надявам се, но не съм убеден, че това ще са хората“.

Възможно ли е това да е решение – бих казала да и човечеството уверено върви по пътя на роботизация и дигитална идентификация. И сега съществува електронен подпис – той е уникален, идентифицира индивида без да предоставя чувствителна лична информация.

В Китай, за удостоверяване на даден индивид, електронният подпис се комбинира с пръстов отпечатък, като пръстовият отпечатък е моментна снимка изпращана към база данни под контрола на държавата.

В Япония голяма част от технологичните корпорации са въвели ирисово разпознаване, използвано като код за достъп. Същата процедура е въведена от Пентагона, ЦРУ и други институции в САЩ.

В заключение, нека да отговорим на въпроса съществува ли доказателство за критични точки между личните данни и свободата в дигиталното общество – нямам информация...

ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО

Станислава Райчева Колева

С бурното развитие на технологиите, изучаващи човешкия мозък, на изкуствения интелект и други, свързани с тях, все по-често се появява информация за идеи и проекти за цифровото безсмъртие на човека. Тук се появява най-големият въпрос: човек действително ли може да бъде дигитализиран. Теорията, че хората могат да бъдат дигитализирани и да живеят в компютрите, се обсъжда отдавна. Но до неотдавна никой не беше се доближил по-далече от изследванията и предположенията.

Какво е свободата? Свободата е възможността да изразяваме себе си, да имаме привилегиите да заявяваме ясно и силно своето мнение. А сигурността е никой да не злоупотребява със споделената от нас информация и с това наше право. Нашите лични данни са нашият сериен код. Уникални, единствени по рода си. Те са нашата фабрична информация. Код, който разкрива основните факти от нашата автобиография – дата, място на раждане, постоянен адрес и др. Много млади хора в България не осъзнават какви опасности дебнат, ако нашите данни попаднат в ръцете на злонамерени хора, които се представят за това, което не са.

“Онези, които са склонни да дадат свободата си за малко временна сигурност, не заслужават нито сигурност, нито свобода” – Бенджамин Франклин

Смартфонът и интернет вече не са лукс. Те са общодостъпни. Но с това идва една огромна отговорност: да знаем как да ги използваме и да бъдем защитени; да знаем какво е правилно да разкриваме чрез клавишите на клавиатурата и какво не. От какво трябва да се пазим? На кого трябва да се доверяваме? И какво трябва да правим, когато се чувстваме обект на тормоз в интернет пространството или жертва откраднати лични данни.

Свободата. Важна част от живота ни. Чрез нея имаме право на глас и на собствен избор. Не се налага да служим на някого, но дали оценяваме тази свобода. В днешно време все повече хора не се отделят от екраните на телефоните си и се изолират от реалния свят – свят, в който свободата ни позволява всичко. Но защо не се възползваме от свободата на реалния живот, а от тази в дигиталния свят?

Представяме се като едни хора в социалните мрежи, а всъщност сме други. Осъзнаваме ли, че заради дигиталния свят се изолираме от реалния, тъй като в интернет можем да мамим за същността си, докато в истинския свят – несправедливия, трудния – се страхуваме от последиците, но защо не мислим и за последиците в дигиталния свят? Дали мисълта “В интернет има твърде много свобода” е наистина правилна и какви биха били последиците от тази свобода?

Дигиталното е непреодолим елемент на нашето време, неизменна част от нашето ежедневие и нашия живот. Работата ни, социалните ни контакти и всяка наша връзка с хората е обвързана с дигиталните технологии, децата попиват информация за света около себе си от най-ранна възраст. В повечето семейства ежедневието се използва множество технологии, поради което е невъзможно децата да бъдат изолирани от дигиталния свят. Те се сблъскват с него навсякъде, учат се бързо и искат да прекарват все повече време пред компютъра или таблета. А времето пред тях е заето предимно с игри и гледане на клипчета, които често са с неподходящо за децата съдържание. Това кара родителите инстинктивно да се опитват да налагат контрол върху дигиталните преживявания на децата си или дори да ги забранят. Но технологиите са част от реалността на децата.

Можем да споделяме публикации, да пишем коментари, да качваме снимки и наистина това ни прави свободни. Но дали наистина сме свободни в мрежата? Ние сме подчинени изцяло на нашите инстаграм последователи, на нашите фейсбук приятели. Това поражда известна зависимост към виртуалния свят. Ставаме роби на нашите собствени правила и норми, които сме изградили. Издигаме стени към хората от реалния свят и започваме да живеем за лайковете и последователите. Много млади хора не се чувстват в безопасност в интернет и живеят в страх. Това обаче е по-малкият, личният страх. Той терзае само потребителите на интернет, които си дават сметка за опасностите във виртуалното пространство. Неяснотата от шеметния дигитален напредък поражда тревоги на глобално ниво.

Дигитализацията води към пропаст, която рано или късно ще достигне до всички бъдещи поколения. Дали ще се измъкнем от тази пропаст и какво ще бъде нашето бъдеще с дигиталните технологии ще покаже само и единствено времето. Дали човек е готов в развитието си да притежава тази свобода, която носи развитието на технологичната революция в “дигиталната ера”, без да застраши собственото си съществуване?

ЛИЧНИТЕ ДАННИ И СВОБОДАТА В ДИГИТАЛНОТО ОБЩЕСТВО

Яна Петева Гюзелева

В нашия така необятен свят съществуват множество неразгадани тайни и загадки. За наша радост или не има и много такива, чиято мистерия е вече разбулена. Често хората сме доста докачливи натури, щом стане дума за нас самите и нашата лична неприкосновеност. Но това никога не ни е пречело да отключваме вратата на съкровено, за да разберем „Какво?“, „Защо?“, „Кога?“ и „Как?“. Докато не дойде ерата на масовата дигитализация, когато вратите започват да се отварят само с няколко кликания...

Харесва ни или не светът се развива с неподозирани темпове. Толкова бързо, че цялата тази информация, някога укривана поради една или друга причина, днес вече едва си намира място във физическия свят. И тук идва ролята на паралелния свят на „истината“, а именно интернет. Защо в кавички ли? Интернет е свободно пространство за изразяване на мисли, предположения, чувства и възприятия, но и своеобразна трибуна, на която постоянно се противопоставят различните мнения на милиони хора по света. Билетите за тази трибуна, възможността да се изправиш и да поставиш своята гледна точка наравно с всички останали, струват твоята самоличност. Веднъж влязъл в тази интернет надпревара, вече си толкова публичен и достъпен, колкото и информацията, която споделяш. За някои е изключително лесно да се доберат до лични данни, дати, събития, цифри и адреси, които някога са принадлежали само на теб, за други това е малко по-трудно, но не и невъзможно.

В днешно време почти няма човешко същество, което да не е част от новия Интернет свят. Та ние самите направихме даже и домашните си любимци „обитатели“ на този паралелен, дигитален еквивалент на планетата Земя. Дори и неприкосновеността на древните племена е нарушена, въпреки че не те, а ние споделяме за тяхното съществуване, бит, възприятия и какво ли още не. Но тази съпоставка между древното, дивото, необузданото и нас като напреднали, свободни, неограничени, ни кара да се замислим коя е истинската свобода – тази в Интернет или тази извън него. Толкова ли сме щастливи всъщност, колкото изглеждаме в Мрежата? Какво представлява животът и всекидневието на всеки от нас без намесата на чуждото мнение и одобрение? Това е време, което основно можем само да си спомняме, но не и да забравяме! Ние сме в публичното пространство и то е в нас. Този необратим процес не може да бъде обезличен, но би било крайно да кажем, че не може и да бъде променен. Може! Решението е в това как ще отговаряме на въпросите, които ние задаваме, но и ни задават – „Какво?“, „Защо?“, „Кога?“ и „Как?“. Ако действията ни бъдат премерени, то и последиците ще бъдат такива. Водейки се по човешката природа, ние хората винаги се стремим към самосъхранение; когато забележим или усетим заплахата, правим всичко възможно да защитим себе си и най-близките до нас, семейството. Колкото повече се приближаваме до дигиталния свят, толкова повече плюсове и улеснения откриваме. А това, което остава скрито? Това зад екрана, в галактическото пространство от нули и единици... дали именно там не се спотайват милиардите минуси, очакващи да ги освободим?

Силната ни обвързаност с Интернет ни превръща от обикновена човешка нация в дигитално общество, което е забравило да общува, да показва емоцията на лицето си, а не на екрана на телефона или компютъра. Тази оптична сила, мощ, бързина, която притежава възможността да ни свърза от единия край на света до другия, ни отдалечава толкова много, когато сме един до друг, че понякога дори не осъзнаваме това. Толкова е лесно да научиш еднолична информация за някого, да се възползваш от нея, да я употребиш в своя полза и да останеш скрит, но става все по-трудно да се изправиш лице в лице срещу някого и да му се довериш напълно.

Къде е нашето право да бъдем свободни в този технологичен свят? Ако преди хората са се борели за правата си срещу други хора, които са ги нарушавали, ние срещу кого трябва да се обърнем? На коя по-висшестояща сила трябва да се противопоставим и дали, докато се усетим, че сме в нечий плен, няма да е вече прекалено късно... На тези и други подобни въпроси, няма да можем да намерим отговорите в Интернет. Който и сървър да отворим, „результатите няма да бъдат налични“. Ключът към всички висши ценности се крие в нас самите.

Комисия за защита на личните данни

Председател: Венцислав Караджов

Членове: Цанко Цолов

Мария Матева

Веселин Целков

Информационен бюлетин № 3 (90) 2021 г.

Издава се съгласно чл. 10, ал. 3 от ЗЗЛД

Уеб сайт на КЗЛД: www.cpdp.bg

Разпространява се в електронен вид

ISSN 2367-7759