https://doi.org/10.33919/ljnbu.20.2.2

ЗАЩИТАТА НА ЛИЧНАТА НЕПРИКОСНОВЕНОСТ В УСЛОВИЯТА НА ПАНДЕМИЯТА ОТ COVID-19

Деница Топчийска[1]

Резюме: В периода на пандемията от COVID-19 през април 2020 г. Министерството на здравеопазването започна администрирането на приложението за проследяване на контакти Virusafe, а със Закона за мерките и действията по време на извънредното положение, обявено с Решение на Народното събрание от 13 март 2020 г., бяха приети промени в Закона за електронните съобщения. Целта на законодателните изменения е да се осигури достъп на компетентните органи до данните за локализация от обществените електронни съобщителни мрежи на лицата, които са отказали или не изпълняват задължителната изолация или лечение по чл. 61 от Закона за здравето. Настоящата публикация има за цел да анализира основните характеристики на мобилните приложения за проследяване на контактни на заразените лица, както и приетите законодателни промени, като ги съпостави със стандартите за защита на личните данни, предвидени в Общия регламент на ЕС 2016/679 за защита на данните и Директива 2002/58/ЕО за правото на неприкосновеност на личния живот и електронни комуникации.

Ключови думи: COVID-19, данни за трафик и местоположение, технология за проследяване на контакти, лична неприкосновеност, защита на личните данни

През март 2020 г. в отговор на разрастващата се пандемия от COVID-19 много държави в света въведоха ограничения по отношение на свободното движение на своите граждани с цел да забавят и намалят разпространението на вируса. Мерките бяха предприети като част от препоръките на Световната здравна организация (СЗО) за действие в подобни ситуации, с които да се облекчат националните здравни системи и да се даде време за медицински проучвания. Негативният ефект върху икономиката поради ограничаването или спирането на работата в някои сектори, както и социалната изолация наложиха спешното разработване и въвеждане на други мерки, които да позволят възстановяването на свободното движение на лицата, като същевременно се запази ефективният контрол върху разпространението на заразата.

Според СЗО основната стратегия за справяне с епидемия от инфекциозно заболяване изисква бързото идентифициране и карантиниране на заразените лица, както и откриването на техните контактни лица от предходните дни и седмици[2]. В контекста на съвременното

[1] д-р Деница Топчийска, доцент по Теория на правото и Право на информационните технологии, департамент „Право“, Нов български университет, denitza.t@gmail.com.

[2] WTO, Contact Tracing. Достъпно: https://www.who.int/news-room/q-a-detail/contact-tracing. Посетено на: [2.06.2020].

информационно общество, в което почти половината от населението носи устройство, подлежащо на GPS локализиране, се постави въпросът за възможността да се използват новите технологии за подпомагане на този процес. В много държави започна разработването на технологични приложения, базирани на мобилните телефони, които да бъдат използвани за по-бързо и точно локализиране и проследяване на контактите на заразените с вируса лица. Тези приложения предизвикаха много въпроси както с оглед на достоверността и полезността на информацията, която могат да предоставят на обществените и здравните власти, така и по отношение на рисковете за личната неприкосновеност на лицата, с които те са свързани, и потенциалната възможност да доведат до масово наблюдение на населението.

В България Министерството на здравеопазването започна администрирането на приложението за проследяване на контакти *Virusafe* през април 2020 г., а със Закона за мерките и действията по време на извънредното положение, обявено с Решение на Народното събрание от 13 март 2020 г. (Закон за извънредното положение), бяха приети промени в Закона за електронните съобщения (ЗЕС). Целта на законодателните изменения е да се осигури достъп на компетентните органи до данните за локализация от обществените електронни съобщителни мрежи на лицата, които са отказали или не изпълняват задължителната изолация или лечение по чл. 61 от Закона за здравето[3]. Настоящата публикация има за цел да изследва и анализира основните характеристики на мобилните приложения за проследяване на контактни на заразените лица, както и приетите законодателни промени, като ги съпостави със стандартите за защита на личните данни, предвидени в Общия регламент на ЕС 2016/679 за защита на данните[4] и Директивата 2002/58/ЕО за правото на неприкосновеност на личния живот и електронните комуникации[5].

I. Мобилни приложения за проследяване на контактни на заразените лица

През май 2020 г. Масачузетският институт по технологии публикува информация относно 30 приложения за проследяване на COVID-19, разработени и достъпни в различни държави от Европа, Азия и Австралия[6]. Тези приложения са анализирани с оглед на технологията, която използват, и тяхното съответствие с принципите за справедливо обработване на лични данни, широко възприети в международните стандарти. Според представената информация основните технологии, които използват приложенията за проследяване на COVID-19, са геолокация и *Bluetooth*, като при използването на всяка от тях се проявяват рискове по отношение на личната неприкосновеност на лицата. Повече от 70 процента от

[3] Пар. 41 от Закона за мерките и действията по време на извънредното положение, обявено с Решение на Народното събрание от 13.03.2020 г. (обн., ДВ, бр. 28 от 24.03.2020 г.).

[4] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ОВ L 119, 4.05.2016 г., с. 1–88.

[5] Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12.07.2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации), ОВ L 201, 31.07.2002 г., с. 37–47.

[6] Лавчиев, Н. Приложенията за проследяване на COVID-19: къде се ползват и какви са резултатите. *Свободна Европа*, 21.05.2020. Достъпно: https://www.svobodnaevropa.bg/a/30621007.html. Посетено на: [2.06.2020]. Файлът на Масачузетския институт по технологии е достъпен тук: https://docs.google.com/spreadsheets/d/1ATalASO8KtZMx__zJREoOvFh0nmB-sAqJ1-CjVRSCOw/edit?fbclid=IwAR3yT3hUG3kLXHSuKyL3uQZ_uzePicyFnkuN4oQCMnba7BSdyHYgfaqXJK0#gid=0

анализираните приложения разчитат на доброволното участие на лицата, но няма пълна информация за степента на използването на тези технологии в различните държави, както и дали има възприети гаранции, че те ще бъдат използвани единствено докато приключи кризата с COVID-19.

В САЩ са предприети различни инициативи за разработване на технологии за проследяване на контакти на COVID-19 както от частни компании, така и от централната администрация в някои щати. Такова приложение например се подготвя от партньорство между *Apple* и *Google*, от Масачузетския институт по технологии, както и на щатско ниво в щатите Алабама, Северна Дакота и Южна Дакота[7]. В доклад на Масачузетския институт по технологии се анализират рисковете, които поставят технологиите за проследяване на зараза, за отделните лица и обществото[8]. Като основен риск е определено нарушаването на личната неприкосновеност на лицата, като същевременно се подчертава, че масовото обработване на данни относно тяхното местоположение и здравословното им състояние създава заплаха от налагането на тоталитарна държава, особено ако данните се обработват от държавен орган. Други рискове представляват опасността от стигматизиране на заразените лица, настъпване на вреди за бизнеса, където е била разпространена заразата, както и възможността за всяване на страх и дезинформация. В този смисъл в доклада се препоръчва данните в системите да бъдат администрирани от независим от държавата орган, както и да не бъдат използвани данни за геолокация. Посочва се, че геолокацията като метод за проследяване на заразата от COVID-19 се използва в Китай и е най-ефективен, когато държавните органи имат достъп до данните на всички лица. Този тип проследяване обаче крие сериозен риск за установяване на контрол върху данните на лицата и тотално наблюдение от страна на държавата.

В Европейския съюз (ЕС) още през април 2020 г. Европейската комисия[9] и Надзорният орган за защита на данните[10] приеха насоки относно стандартите, свързани със защитата на личната неприкосновеност на лицата, на които трябва да отговарят мобилните приложения за проследяване на контакти на COVID-19. Целта е да се възприеме общ европейски подход за разработването на тези мобилни приложения, за да се осигури ефективна система за предупреждаване, превенция и проследяване на контактите, която да помогне за ограничаване на разпространението на заболяването. Насоките нямат правнообвързващ характер и се отнасят единствено за доброволните мобилни приложения, които се възприемат като важен допълващ елемент от цялостната стратегия за борба с пандемията от COVID-19.

Общият подход на ЕС за мобилните приложения за проследяване на контакти предвижда те да се основават изцяло на доброволното участие на гражданите. С оглед на това

---

[7] Richtel, M. Contact Tracing with Your Phone: It's Easier but There are Tradeoffs. *New York Times*, 3 June 2020. Достъпно: https://www.nytimes.com/2020/06/03/health/coronavirus-contact-tracing-apps.html?fbclid=IwAR2rbLhEbBXY4b-ZMbXcCs6MuSirnjUuET38KbVFGTwpStyAgi0VLdFvGes. Посетено на: [3.06.2020].

[8] MIT Media Lab Report: Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic. Достъпно: https://arxiv.org/pdf/2003.08567.pdf. Посетено на: [3.06.2020].

[9] Съобщение на Комисията. Насоки за мобилните приложения, които подпомагат борбата с пандемията от COVID-19, във връзка със защитата на данните 2020/C 124 I/01, C/2020/2523, OJ C 124I, 17.04.2020, с. 1–9. Достъпно: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:52020XC0417(08). Посетено на: [3.06.2020].

[10] Европейски комитет по защита на данните, Насоки № 4/2020 относно използването на данни за местонахождение и инструменти за проследяване на контакти в контекста на пандемията от COVID-19, приети на 21.04.2020 г. Достъпно: https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_bg. Посетено на: [3.06.2020].

се подчертава, че за да се създаде доверие у населението и да се мотивира да използва приложенията, е от изключително значение обработването на личните данни да бъде в съответствие с Общия регламент на ЕС за защита на данните и Директива 2002/58/ЕО. Насоките съдържат следните основни препоръки:

1. Препоръчва се администратор на личните данни да бъде национален здравен орган за разлика от предложението на Масачузетския институт по технологии.
2. Приложения не бива да проследяват конкретните движения на физическите лица, а да разчитат по-скоро на информация за хора и обекти в непосредствена близост до ползвателите. С оглед на това се препоръчва приложенията да бъдат базирани на технологията *Bluetooth Low Energy* (BLE), която избягва възможността за проследяване за разлика от данните за географското позициониране.
3. Данните в приложенията трябва да бъдат децентрализирани. Това означава, че те трябва да се пазят на устройството на потребителя и само с неговото съгласие и с оглед постигане на целите, за които той се е съгласил, да бъдат качени на сървъра на разположение на здравните органи (например ако лицето се зарази и е съгласно да сподели тази информация).
4. Основание за обработването на данните може да бъде съгласието на лицата, което трябва да бъде свободно изразено, конкретно, изрично и информирано в съответствие с Общия регламент на ЕС за защита на данните. Възможно е да се използва и основанието, което предвижда възможност за обработване на данни, когато това е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора[11]. В тези случаи основанието за обработването трябва да бъде установено в правото на ЕС или в националното законодателство, което прилага администраторът на данните. Използването на второто основание се препоръчва, тъй като в този случай е възможно законодателят да предвиди допълнителни изисквания с оглед законосъобразното и добросъвестно обработване.
5. Мобилните приложения могат да съдържат различни функции, като за всяка от тях целите на обработване на данните трябва да бъдат ясно и конкретно формулирани. По отношение на всяка една от функциите и в съответствие с дефинираните цели трябва да бъде и обемът на събираните данни, които трябва да бъдат подходящи, свързани с целите и ограничени до минимално необходимите за постигане на целите.
6. Потребителите трябва да имат възможност да избират коя от функционалностите на приложението да използват, като в съответствие с това трябва да бъдат и събираните от тях данни. Приложенията трябва да разполагат с една или повече от следните функционалности:
    - предоставяне на точна информация за пандемията от COVID-19;
    - функция за проверка на симптомите;
    - функция за проследяване на контактите и за предупреждение;
    - осигуряване на форум за използване на телемедицина.
7. Срокът за съхраняване на данните трябва да бъде до приключване на кризата с COVID-19, след което те трябва да бъда заличени или анонимизирани.

[11] Член 6, параграф 1, буква д) от Общия регламент на ЕС за защита на данните.

8. Препоръчва се предварително да бъде извършена оценка на въздействието на приложението за проследяване на контакти, която да бъде публикувана.
9. Също така приложенията трябва да бъдат обект на непрекъснат независим одит, чрез който да се гарантира, че обработването на данните се осъществява в съответствие с правото на ЕС и приложимото национално законодателство.

В България през април 2020 г. стана достъпно мобилното приложение за проследяване на контакти *Virusafe*, одобрено и администрирано от Министерството на здравеопазването[12]. Приложението е безплатно, некомерсиално и е насочено към всички лица над 14-годишна възраст, които пребивават на територията на България. Функционалностите, които приложението предлага, включват функция за проверка на симптомите (личен статус), споделяне на локация на устройството, получаване на съобщения и достъп до информационен екран. Обработването на данни във *Virusafe* се извършва на основание съгласието на потребителя, който може да избере дали да сподели информацията за своята локация, или да използва единствено останалите услуги, за които тя не е необходима. Използването на приложението изисква крайно мобилно устройство, което поддържа наличието на определен клас софтуер и интернет връзка.

В общите условия за ползване на мобилно приложение не е публикувана информация относно използваната технология, както и къде се съхраняват данните. Не е посочено при използването на различните функционалности какви данни се събират и за какъв срок ще бъдат обработвани. Няма информация относно извършена предварителна оценка на въздействието по смисъла на Общия регламент на ЕС за защита на данните, както и дали системата ще подлежи на независим одит. Няма ясно и достъпно описание на начина, по който ще бъда споделяна информация за заразени лица. В общите условия за ползване на мобилното приложение е посочено, че то ще функционира да отмяната на извънредното положение, което беше отменено на 13 май 2020 година. Към настоящия момент няма яснота относно начина, по който ще продължи да функционира.

Очевидните несъответствия на Приложението *Virusafe* с Общия регламент на ЕС за защита на данните и с препоръките на Европейската комисия и Европейския комитет по защита на данните не станаха предмет на обществена дискусия, най-вероятно тъй като то предизвика много слаб интерес сред населението в България. Реалните потребители на приложението бяха под 1 процент от населението, а според изследванията, за да бъде то ефективно, потребителите трябва да бъдат над 70 процента от населението[13]. Друг проблем, който се прояви, беше, че социално слабите и маргинализирани групи не разполагат с техническите възможности за използване на приложението, а те се оказаха до голяма степен засегнати от вируса COVID-19. В ЕС и САЩ все още предстои да се прецени до каква степен тези приложения за проследяване на COVID-19 ще бъдат използвани и доколко биха били реално ефективни за гражданите и здравните власти.

II. Измененията в Закона за електронните съобщения във връзка с пандемията от COVID-19

В Съобщението на Европейската комисия относно Насоките за мобилните приложения, които подпомагат борбата с пандемията от COVID-19, във връзка със защитата на да-

[12] Министерство на здравеопазването, *Virusafe*. Достъпно: www.virusafe.info. Посетено на: [3.06.2020].

[13] Кръстев, Б. Колко хора наистина ползват приложение срещу COVID-19?. *Клуб Z*, 21.05.2020. Достъпно: https://clubz.bg/98914-kolko_hora_naistina_polzvat_prilojenie_sreshtu_covid_19. Посетено на: [22.05.2020].

нните изрично се посочва, че те не се отнасят до мобилните приложения, имащи за цел изпълнение на изискванията за карантина (включително задължителните)[14]. В България с приемането на Закона за извънредното положение бяха приети промени в Закона за електронните съобщения (ЗЕС)[15], в съответствие с които на компетентните органи се предоставя достъп до данните за локализация от обществените електронни съобщителни мрежи на лицата, които са отказали или не изпълняват задължителната изолация или лечение по чл. 61 от Закона за здравето[16]. Изменението на Закона за електронните съобщения влезе в сила от 24 март 2020 г. и е предвидено да се прилага до отпадане на необходимостта от принудителното изпълнение на задължителната изолация и болничното лечение на лица по чл. 61 от Закона за здравето.

На 22 април 2020 г. разпоредбата на параграф 41 от Закона за извънредното положение, с която се приеха измененията на ЗЕС, беше оспорена пред Конституционния съд като противоконституционна на две основания. От една страна, се твърди, че поради неспазване на процедурата за приемане на законодателни актове при приемането на параграф 41 от Закона за извънредното положение се нарушава принципът на публичност в парламентарното управление, изведен от чл. 1, ал. 1 от Конституцията и утвърден в конституционноправната доктрина. От друга страна, изменението в ЗЕС е оспорено на материално основание, като се посочва, че мярката представлява непропорционална намеса в правото на личен живот на гражданите[17] и тайната на кореспонденцията им, гарантирани в чл. 32 и 34 от Конституцията. За целите на настоящото изложение ще насочим вниманието си единствено по отношение на втория аргумент за противоконституционност.

С параграф 41 от Закона за извънредното положение се допълва съществуващият режим в ЗЕС за достъп до трафични данни и данни за местонахождение на лицата. В посочените изменения се предвижда, че данните, които се създават и съхраняват в процеса на дейността на предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги и са необходими за установяване на идентификатор за ползваните клетки, ще бъдат съхранявани за целите и за нуждите на принудителното изпълнение на задължителната изолация и болничното лечение на лица по чл. 61 от Закона за здравето, които са отказали или не изпълняват задължителна изолация и лечение. Данните, необходими за установяване на идентификатор за ползваните клетки, представляват административни адреси на клетки на мобилна наземна електронна съобщителна мрежа, от които е генерирано или в които е терминирано повикване (чл. 251и, ал. 6 от ЗЕС). Те представляват един от шестте вида трафични данни и данни за местонахождение, които се генерират в процеса на дейността на предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, и трябва да се съхраняват за период от 6 месеца за целите, предвидени в чл. 251б, ал. 2 от ЗЕС. Право да искат извършване на справка за тези данни, когато е необходимо за изпълнение на техните правомощия, имат Главна дирекция „Национална полиция“,

[14] Съобщение на Комисията. Насоки за мобилните приложения, които подпомагат борбата с пандемията от COVID-19, във връзка със защитата на данните (2020/C 124 I/01), ОВ C 124I, 17.04.2020 г., с. 1–9.

[15] Обн., ДВ. бр. 41 от 22.05.2007 г., посл. изм. и доп., ДВ, бр. 51 от 5.06.2020 г. В статията е взета предвид редакцията на Закона за електронните съобщения (ЗЕС) към 15.06.2020 г.

[16] Пар. 41 от Закона за мерките и действията по време на извънредното положение, обявено с Решение на Народното събрание от 13.03.2020 г. (обн., ДВ, бр. 28 от 24.03.2020 г.).

[17] Относно правните и етични проблеми на личната сигурност вж. Николова, Р. (2012). Защита на личния живот, безопасност и сигурност. В: *Дигиталните медии – речник на основните понятия*. Велико Търново: Фабер, с. 260–264.

Столичната дирекция на вътрешните работи и областните дирекции на Министерството на вътрешните работи[18]. След направено искане от страна на ръководителя на съответните структури предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, са задължени да предоставят незабавен достъп до данните. Искането трябва да съдържа правното основание за предоставяне на достъпа, както и информация за данните и периода, които следва да се отразят в справката, и определеното длъжностно лице, на което да се предоставят данните[19]. Трябва да се отбележи, че ЗЕС не се прилага по отношение на съдържанието на съобщенията, чиято конфиденциалност се гарантира в чл. 32 от Конституцията и достъпът до което се осъществява по реда, предвиден в Закона за специалните разузнавателни средства[20].

Според предвидената в ЗЕС процедура ръководителят на съответната структура, след изпращане на искането за достъп до данни, трябва да уведоми незабавно компетентния съдебен орган, като приложи искането и изложи своите мотиви. Систематичното тълкуване на правните разпоредби води до извода, че в мотивите трябва да се посочат пълно и изчерпателно фактите и обстоятелствата, обуславящи целта по чл. 251б, ал. 2 от ЗЕС[21]. Ако в срок от 24 часа компетентният съд постанови отказ, предоставените данни трябва да бъдат унищожени незабавно от структурите, които са получили достъп до тях. В случаите на злоупотреба с данни за трафик или местонахождение в ЗЕС е предвидена административна отговорност за длъжностното лице от съответния държавен орган или предприятие, предоставящо обществени електронни съобщителни мрежи и/или услуги[22].

Правната уредба в ЗЕС, свързана с обработването и достъпа до трафични данни и данни за местонахождение, генерирани от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, е въведена в съответствие с Директива 2002/58/ЕО за правото на неприкосновеност на личния живот и електронни комуникации[23]. Директивата установява задължение за държавите членки на ЕС да гарантират в националното си законодателство поверителността на данните за трафик и за местонахождение, пренасяни и обработвани чрез обществените комуникационни мрежи и услуги. Тези данни трябва да бъдат изтрити или анонимизирани, когато вече не са необходими за предаване на дадено съобщение, с изключение на данните, свързани с изготвянето на абонатни сметки и плащания за взаимно свързване. Данните могат да се предават на държавни органи или на други трети страни само ако са анонимизирани от доставчика или когато става въпрос за данни, указващи географското положение на крайното оборудване на ползвателя, които не представляват данни за трафик, само с предварителното съгласие на ползвателите[24].

---

[18] Член 251в, ал. 2, изр. 2 от ЗЕС.

[19] Член 251г[1], ал. 1, изр. 2 и ал. 2 от ЗЕС.

[20] Закон за специалните разузнавателни средства (обн., ДВ, бр. 95 от 21.10.1997 г., посл. доп., ДВ, бр. 37 от 7.05.2019 г.)

[21] Член 251в, ал. 3 във връзка с чл. 251г[1], ал. 2 и ал. 3 от ЗЕС.

[22] Член 332 от ЗЕС.

[23] Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12.07.2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронните комуникации), ОВ L 201, 31.07.2002 г., с. 37–47.

[24] Член 5, 6 и 9 от Директива 2002/58/ЕО.

В съответствие с чл. 15 от Директива 2002/58/ЕО са допустими изключения от правата и задълженията, предвидени в директивата, включително и по отношение на достъпа до данни за трафик и за местонахождение. Според Насоките за мобилните приложения за проследяване, които приема Европейският комитет по защита на данните, такива дерогации биха могли да бъдат въведени и приложени в условията на пандемията от COVID-19[25]. В съответствие с чл. 15 от Директива 2002/58/ЕО ограниченията трябва да се приемат със закон и са допустими само ако представляват необходима, подходяща и пропорционална мярка в рамките на демократичното общество, за да се гарантира обществената безопасност и превенцията. Всяко ограничение трябва да бъде съобразено с принципите на правото на ЕС и защитата на основните права и свободи на лицата.

Още през 2008 г. Съдът на ЕС в свое решение във връзка с преюдициално запитване[26] дава насоки за прилагането на чл. 15 от Директива 2002/58/ЕО. В тълкуването си съдът посочва, че предвидените възможности за изключения, от една страна, се отнасят до националната сигурност, отбраната и обществената безопасност, като свързаните с тях дейности са присъщи на държавите или на държавните органи, и от друга страна, засягат разкриването и преследването на престъпления. Съдът посочва, че чл. 15 от Директива 2002/58/ЕО изрично препраща към чл. 13, параграф 1 от Директива 95/46/ЕО[27], която позволява на държавите членки да приемат мерки, с които да ограничат задължението за поверителност на личните данни във всички случаи, в които такова ограничение е необходимо за защита на правата и свободите на трети лица. С оглед на това според Съда на ЕС няма пречки държавите членки да предвидят ограничения от правата и задълженията, свързани с конфиденциалността на данните, предвидени в Директива 2002/58/ЕО, като предоставят възможност тези данни да бъдат разкривани не само в наказателни, но и в рамките на граждански производства. Широкото тълкуване, което възприема Съдът, е основание да се направи извод, че няма правна пречка да бъде предвидена законовата възможност на национално ниво за разкриване на лични данни при всички производства, в които се засягат основни права и свободи на лицата. Във всички случаи обаче трябва да бъде предвидена съдебна защита за лицата, когато техните права са нарушени от незаконосъобразното обработване на лични данни.

Директива 95/46/ЕО е отменена с Общия регламент на ЕС за защита на данните, който се прилага от 25 май 2018 година. Регламентът предвижда актуализирана и адаптирана към съвременната технологична среда правна рамка за защита на данните. В него се предвижда като специално основание възможността за приемане на ограничителни мерки на национално ниво по отношение на правата и задълженията, предвидени в регламента, когато това е необходимо с оглед постигането на важни цели от обществен интерес, включително свързани с общественото здраве. Такова ограничение е допустимо и за защитата на субекта на данните или на правата и свободите на други лица. Всяко ограничение обаче трябва да съответства на критериите за необходимост и пропорционалност в рамките на демократичното общество, а Регламент (ЕС) 2016/679 въвежда и допълнителни изисквания по от-

[25] Съобщение на Комисията. Насоки за мобилните приложения, които подпомагат борбата с пандемията от COVID-19, във връзка със защитата на данните 2020/C 124 I/01, C/2020/2523, OJ C 124I, 17.04.2020 г., с. 1–9.

[26] Решение на Съда на ЕС от 29.01.2008 г. по дело C-275/06, Productores de Música de España (Promusicae)/ Telefónica de España SAU, пар. 49–54.

[27] Директива 95/46/ЕО на Европейския парламент и на Съвета от 24.10.1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни OB L 281, 23.11.1995 г., с. 31–50 (отм.).

ношение на съдържанието на законодателните разпоредби, с които се въвеждат ограничителните мерки[28].

Въпросът, в кои случаи е допустимо запазване на трафични данни, включително и данни за местонахождение, е широко дискутиран в ЕС във връзка с обявяването за невалидна от Съда на ЕС на Директива 2006/24/ЕО за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи[29]. Директива 2006/24/ЕО се приема като отговор на терористичните атаки в Мадрид и Лондон през 2004 и 2005 г. и има за цел да хармонизира националните законодателства в държавите членки във връзка със запазването на данни за трафик и данни за местоположение за целите на разследването, разкриването и преследването на сериозни престъпления. Трябва да се отбележи, че Директива 2006/24/ЕО не отменя правото на държавите членки да въвеждат и други ограничения по отношение на правата и задълженията, свързани със защитата на конфиденциалността на данните, за целите и при условията, предвидени в чл. 15 от Директива 2002/58/ЕО.

За да прецени съответствието на Директива 2006/24/ЕО с правото на ЕС, съдът прилага следния тест. Първо, съдът установява дали чрез директивата се ограничават основни права и свободи, предвидени в Хартата на основните права на Европейския съюз. В конкретния случай с Директива 2006/24/ЕО се ограничава правото на зачитане на личния и семейния живот, правото на защита на личните данни и свободата на изразяване. Второ, установява дали ограничението е наложено с оглед на значим общ за Съюза интерес, който в конкретния случай е правото на сигурност. Трето, проверява дали е спазен принципът за пропорционалност на констатираната намеса, който изисква постигане на легитимните цели, без да се надхвърля подходящото и необходимото за постигането им.

В своето решение Съдът на ЕС приема, че независимо че запазването на трафични данни и данни за местоположение е мярка, която има основно значение за борбата с организираната престъпност и тероризма, тя не може да се приеме като необходима и пропорционална за постигането на тази цел по начина, по който е регламентирана в Директива 2006/24/ЕО. Съгласно установената практика на Съда на ЕС намесата в правото на лична неприкосновеност трябва да се ограничи до строго необходимото[30]. Директива 2006/24/ЕО се прилага общо за всички лица, за всички електронни съобщителни средства, както и за всички данни за трафик, без да въвежда никакво разграничаване, ограничаване или изключение с оглед на целта за борба с тежките престъпления. Същевременно достъпът на компетентните национални органи до запазените данни не се предоставя след предварителен контрол, осъществяван от съдебен орган или от независима административна структура, чието решение да има за цел да ограничи достъпа до данните и тяхното използване само до строго необходимото за постигането на преследваната цел и което да се постановява след мотивирана молба на тези органи, подадена в рамките на наказателни производства за предотвратяване, разкриване и наказателно преследване на престъпления. Периодът на запазване на данните не е разграничен с оглед вида на данните, както и не са предвидени доста-

[28] Вж. чл. 23, пар. 1 (д), (и) и пар. 2 от Регламент (ЕС) 2016/679.

[29] Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15.03.2006 г. за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО, ОВ L 105, 13.04.2006 г., с. 54–63 (отм.).

[30] Пар. 51 и 52 от Решение на Съда на ЕС от 8 април 2014 г. по съединени дела C-293/12 и C-594/12. Достъпно: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=bg&mode=lst&dir=&occ=first&part=1&cid=5589916. Посетено на: [5.06.2020].

тъчно ясни гаранции за защита на правата на субектите на данните от злоупотреби. С оглед на представените аргументи през 2014 г. Съдът на ЕС отменя Директива 2006/24/ЕО като невалидна.

След отмяната на Директива 2006/24/ЕО държавите членки самостоятелно трябваше да преценят съответствието на националното си законодателство, въведено в изпълнение на тази директива, с националните си конституции и изискванията на член 15 от Директива 2002/58/ЕО. В България Конституционният съд обяви за противоконституционни разпоредбите на ЗЕС, с които се транспонираше Директива 2006/24/ЕО, като уредба, която не отговаря на изискванията да бъде необходима, подходяща и съразмерна в условията на едно демократично общество[31]. В съответствие с решението на Съда на ЕС и практиката на ЕСПЧ, Конституционният съд в решението си подчерта, че въвеждането на мерки за запазване на трафични данни и данни за местоположение, тъй като ограничават основни права трябва, да стане с точни, ясни и предвидими правила, създаващи сигурни гаранции за защита и сигурност. През 2015 г. бяха приети нови разпоредби в ЗЕС относно запазването и достъпа до трафични данни и данни за местонахождение, към които се интегрират разпоредбите на параграф 41 от Закона за извънредното положение, обявено с Решение на Народното събрание от 13 март 2020 година.

За да се прецени дали разглежданото законодателно изменение отговаря на стандартите, установени в Конституцията на РБ, член 15 от Директива 2002/58/ЕО и практиката на Конституционния съд, трябва да се приложи тестът, възприет от Съда на ЕС при преценката на валидността на обявената за невалидна Директива 2006/24/ЕО за запазване на трафичните данни. С приемането на параграф 41 от Закона за извънредното положение се засягат и ограничават основно правото на лична неприкосновеност на лицата и правото на защита на личните данни на лицата. Тези права не са абсолютни и могат да бъдат ограничени, за да се съвместят и да се постигне баланс с други основни права. Докато традиционно правото на защита на личната неприкосновеност и в частност правото на защита на личните данни се разглежда в конкуренция с интереса за гарантиране на сигурност в обществото, **в условията на пандемията от COVID-19 в академичната дискусия беше поставен въпросът за намирането на справедлив баланс между правото на лична неприкосновеност и правото на живот като особено по значимост право**. В този контекст се подчерта, че не само ограничението на правото на лична неприкосновеност трябва да бъде обосновано като съразмерна, пропорционална и необходима мярка, но и отказът от предприемането на мерки за защита на живота в условията на пандемия също трябва да бъде обоснован с оглед на тези стандарти[32].

Въведеното изменение на ЗЕС е направено с оглед да се осигури обществената безопасност, която представлява легитимно призната цел в съответствие с Конституцията на РБ, правото на ЕС и по-конкретно Общия регламент на ЕС за защита на данните и Директива 2002/58/ЕО. С изменението на ЗЕС се дава достъп на определените държавни органи, а именно Главна дирекция „Национална полиция“, Столичната дирекция на вътрешните работи и областните дирекции на Министерството на вътрешните работи, единствено и само до данните, които са необходими за установяване на идентификатор за ползваните клетки. Достъпът се предоставя във връзка и за целите на изпълнението на задълженията по осигуряване на принудителното изпълнение на **задължителната изолация и болничното** лече-

[31] Конституционен съд на РБ, Решение № 2 от 12.03.2015 г. по к. д. № 8/2014 г.2, обн., ДВ, бр. 23 от 27.03.2015 г.

[32] Размяна на мисли между философа Юрген Хабермас и теоретика на правото Клаус Гюнтер. *Пирон*, бр. 19, 2020 /извънредно положение/. Достъпно: www.piron.culturecenter-su.org/. Посетено на: [5.06.2020].

ние единствено на лица по чл. 61 от Закона за здравето, които са отказали или не изпълняват задължителна изолация и лечение.

За тълкуването на разглежданите изменения в ЗЕС и преценката на пропорционалността на въведените мерки има значение Законът за изменение и допълнение на Закона за здравето, приет във връзка с изтичането на срока на извънредното положение, и по-специално разпоредбите относно процедурата за налагане на задължително лечение и изолация и дефинициите относно правната употреба на понятията „изолация“ и „карантина“[33]. Трябва да се отбележи, че измененията на Закона за здравето в тази част не са оспорени пред Конституционния съд. На изолация подлежат **само лица, болни от заразна болест и заразоносители**, с цел предотвратяване на разпространението на съответната заразна болест. В тази група не се включват лицата, които подлежат на карантина, а именно контактни лица на лица, болни от заразна болест, и на лица, които са влезли на територията на страната от други държави, с цел предотвратяване разпространението на съответната заразна болест[34]. В съответствие с разпоредбите на ЗЕС оправомощените лица могат да имат достъп само до данните на тези лица, които са отказали или не изпълняват **задължителна изолация и лечение**, и данните са им необходими за осъществяването на принудителното изпълнение.

Достъпът до данни на лица, болни от заразна болест и заразоносители, може да бъде осъществен единствено с оглед на болестите и след като състоянието на лицето е констатирано по реда, определен в Закона за здравето. Обхватът на заразните болести е определен в чл. 61, ал. 1 от Закона за здравето, а именно: холера, чума, вариола, жълта треска, вирусни хеморагични трески, дифтерия, коремен тиф, полиомиелит, бруцелоза, антракс, малария, тежък остър респираторен синдром, COVID-19 и туберкулоза с бацилоотделяне. В съответствие с чл. 61, ал. 3 от Закона за здравето министърът на здравеопазването по предложение на главния държавен здравен инспектор може да разпореди задължителна изолация на лица, болни или заразоносители на заразни болести, извън посочените по ал. 1. Задължителната изолация и болничното лечение по чл. 61 от Закон за здравето се извършва с предписание на директора на съответната регионална здравна инспекция по предложение на лекаря, насочил лицето за хоспитализация. Предвидената процедура създава голяма степен на сигурност относно необходимите елементи на фактическия състав, за да се поиска незабавен достъп да данните на лицата от доставчиците на електронни съобщителни услуги, който в рамките на 24 трябва да бъде потвърден от съдебен орган. За да получи достъп до данните, компетентният държавен орган по чл. 251в, ал. 2, изр. 2 от ЗЕС трябва да се позове на предписание на директора на съответната регионална здравна инспекция. Опасността от заразяване на други лица в случаите, когато болни или заразоносители на заразни болести откажат или не изпълняват предписаната изолация или болнично лечение, представлява спешна ситуация, която обосновава необходимостта от директен достъп до данните.

Предвид гореизложеното може да се направи изводът, че изменението на ЗЕС, направено с пар. 41 от Закона за извънредното положение, представлява законосъобразна и необходима мярка в съответствие с правото на ЕС и националното ни законодателство. Въведените правила са точни, ясни и предвидими, което е предпоставка да се гарантира защитата и сигурността на лицата. За да се прецени обаче дали мярката е пропорционална, е необходимо да се обсъди дали заложената цел не би могла да се постигне с по-малко ограничителни мерки по отношение на личната неприкосновеност на лицата. За съжаление, тази преценка не може да бъде направена поради липсата на мотиви към законодателните изме-

[33] Цитираното изменение на Закона за здравето е в сила от 13.05.2020 г.

[34] Пар. 46 и 47 от ДР на Закон за здравето.

нения. Трябва да се отбележи също така, че неспазването на предвидената в Конституцията и закона процедура за приемане на нормативни актове е достатъчно основание, за да бъде отменена разглежданата разпоредба. С оглед на многобройните критики към законодателния процес през последните години конкретното конституционно дело представлява подходящ повод Конституционният съд да се произнесе по този проблем, което ще има сериозен ефект върху законодателната практика на НС.

Заключение

Използването на модерните технологии за проследяване на заразените и контактните лица в условията на пандемията от COVID-19 постави много въпроси, свързани с постигането на справедлив баланс между основните права и запазването на демократичните ценности. В тази безпрецедентна извънредна ситуация правото на лична неприкосновеност беше поставено в конкуренция с правото на живот, което стана предпоставка за по-широко навлизане на държавата в личната сфера на лицата. Разработването на технологичните приложения за проследяване към този момент се оказва слабо ефективна мярка с оглед справянето с пандемията не само в България, но и в другите държави от ЕС поради ограничения интерес на гражданите към тях и невъзможността за включване на всички групи от населението, особено социално слабите и маргинализираните. Съобразяването на мобилните приложения за проследяване с Общия регламент на ЕС за защита на данните до голяма степен би повишило доверието на лицата и би ги мотивирало да се включат в общата система на ЕС за ограничаване на разпространението на заразата.

Пандемията от COVID-19 постави отново и въпроса за възможността за достъп на компетентните органи до данните за местонахождение на лицата, генерирани в процеса на дейност на доставчиците на електронни съобщителни мрежи и/или услуги. Създадената вече практика както от Съда на ЕС, така и от Конституционния съд в България дава достатъчна основа, за да се прецени конституционосъобразността на въведените мерки и ограничения. Независимо че на основата на направения анализ може да се заключи, че разглежданите изменения на ЗЕС са законосъобразни и необходими, тяхното съответствие с изискването за пропорционалност не може да бъде преценено поради нарушенията в законодателния процес и липсата на мотиви. От ключово значение за справяне с кризата остава необходимостта от въвеждане на законосъобразни и пропорционални мерки, които да гарантират правото на живот при минимално навлизане в личната сфера на лицата.

Цитирана литература

Николова, Р. (2012). Защита на личния живот, безопасност и сигурност. В: *Дигиталните медии – речник на основните понятия*. Велико Търново: Фабер, с. 260–264.

PROTECTION OF PRIVACY IN THE PERIOD OF COVID-19 PANDEMIC

Denitza Toptchiyska[35]

Abstract: During the pandemic of COVID-19 in April 2020 the Ministry of Health in Bulgaria began the administration of the Virusafe contact tracking application. With the Law on Emergency Measures and Actions, declared by a decision of the National Assembly of 13th March 2020 amendments to the Electronic Communications Act were adopted. The purpose of the legislative amendments was to provide access of the competent authorities to the localization data from the public electronic communication networks of the individuals, who have refused or do not fulfill the obligatory isolation or treatment under art. 61 of the Health Act. This publication aims to analyze the main features of mobile applications for tracking the contacts of infected persons, as well as the adopted legislative changes, comparing them with the standards of personal data protection provided in the EU General Data Protection Regulation 2016/679 and Directive 2002/58/EC on the right to privacy and electronic communications.

Keywords: COVID-19, Traffic and Location Data, Contact Tracing Technology, Privacy, Data Protection

[35] Denitza Toptchiyska, PhD, Associate Professor of Theory of Law and Information Technology Law, Department of Law, New Bulgarian University, denitza.t@gmail.com.