

## ПРАВНИ ПРОБЛЕМИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ ПРИ АВТОМАТИЗИРАНО ПРОФИЛИРАНЕ

*Мартин Захариев\**

Автоматизираното профилиране е относително ново явление за информационното общество, намиращо все по-голямо приложение през последните две десетилетия. Допустимостта на профилирането и пределите, до които трябва да бъде позволено, поставят сериозни правни и нравствено-етични въпроси пред информационното общество и съвременната правова държава. То може да засегне правото на неприкосновеност на личния живот (на английски език – *privacy*<sup>1</sup>), да доведе до дискриминация, да накърни свободата<sup>2</sup> и принципа на зачитане на човешкото достойнство<sup>3</sup>, да наруши презумпцията за невинност и т.н. **Настоящият анализ обаче има за цел да изследва профилирането през призмата на защитата на личните данни.** Няколко са основните причини за това:

– профилирането за първи път се въвежда като понятие в регулаторните актове на ЕС в областта на защитата на личните данни, т.е. то е понятие на правото на защитата на личните данни;

– по своята същност профилирането иманентно е свързано с обработването на данни, идентифициращи физическите лица или разкриващи наличието на дадени характеристики у физическите лица, т.е. (поне на теория) на даден етап от реализацията си то трябва да се подчини на режима за обработка на личните данни;

– забраната за дискриминация или правото на неприкосновеност на личния живот може да се приложат едва на последния етап на профилирането – прилагане на профилите с цел вземане на решение спрямо профилираните лица (т.е. след като вече

---

\*Адвокат от София.

<sup>1</sup> В правната литература не съществува единно виждане какво представлява понятието *privacy*. За развитието на понятието *privacy* в правните системи на европейските държави и съотношението му със защитата на личните данни вж. **Fuster, G. G.** The Emergence of Personal Data. – Law, Governance and Technology Series 16. Switzerland: Springer International Publishing, 2014, 21–54.

<sup>2</sup> **Hildebrandt, M.** Profiling and the Identity of the European Citizen, Chapter 15. – In: **Hildebrandt, M., S. Gutwirth** (ed.). Profiling the European Citizen: Cross Disciplinary perspectives. Dordrecht: Springer, 2008, 303–326.

<sup>3</sup> **Bygrave, L. A.** Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling. – Computer Law & Security Report, 2001, volume 17, 17–24; also published in Privacy Law & Policy Reporter, 2000, volume 7, 67–76, available at [http://folk.uio.no/lee/oldpage/articles/Minding\\_machine.pdf](http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf), p. 4 (12.11.2016 г.).

данните са обработени), докато режимът на защитата на личните данни може да се приложи още на етапа на събиране на данни и тяхната обработка с автоматизирани средства с цел профилиране<sup>4</sup>;

– защитата на другите изброени по-горе права може да бъде затруднена поради по-трудни за доказване предпоставки на нарушението (при дискриминация) или поради приложимостта на тези права само срещу профилиране в специфични сфери (при презумпцията за невиновност), докато правилата за защита на личните данни винаги се прилагат само и единствено на основание наличието на обработка на такива данни<sup>5</sup>.

**Анализът на уредбата на профилирането във вторичното право на ЕС предполага последователно изследване на Директива 95/46<sup>6</sup> (Директивата) и на промените, които ще се въведат в режима на защита на личните данни в ЕС с Регламент 2016/679<sup>7</sup> (Регламента). Това са законодателните актове, които (ще) формират правната рамка на Съюза в областта на защитата на личните данни в следващите години. В настоящото изложение последователно ще бъдат анализирани дефиницията за „профилиране“; забраната за автоматизирано вземане на решения, основани на профилиране; правата, които субектите на данни имат при профилиране, и другите разпоредби в Регламента и Директивата, имащи отношение към профилирането.**

Понятието „профилиране“ не се използва в Директивата. Макар то да фигурира в първоначалното предложение на Европейската комисия за Директива за защита на личните данни<sup>8</sup> (чл. 14, § 2 от предложението урежда правото на всяко лице да не бъде обект на административно или частно (правно) решение, включващо оценка на

---

<sup>4</sup> За тази и за другите причини, обуславящи приложимостта на режима на защита на личните данни към профилирането, вж. **Schreurs, W. and others. *Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector*, Chapter 13.** – In: **Hildebrandt, M., S. Gutwirth** (ed.). *Op. cit.*, 242–246.

<sup>5</sup> **Schreurs, W. and others. *Op. cit.***

<sup>6</sup> Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, обн., „Официален вестник на ЕС“, L 281, бр. 38 от 23.11.1995 г.

<sup>7</sup> Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), обн., „Официален вестник на ЕС“, L 119, бр. 59 от 4.05.2016 г. По силата на чл. 99, § 2 регламентът ще започне да се прилага от 25.05.2018 г.

<sup>8</sup> Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, обн., „Официален вестник на ЕС“, C 277, бр. 33 от 5 ноември 1990 г.

неговото поведение, което се основава единствено на автоматизираната обработка на лични данни, определящи неговия *профил* или личност), впоследствие това понятие е премахнато от окончателния текст на Директивата. Тази промяна в хода на законодателната процедура на ЕС безспорно поражда проблеми при опитите да се регулира профилирането. За да бъде успешно регулирано дадено понятие, необходимо е правото най-напред да го дефинира. Единствената разпоредба в Директивата, свързана с някои аспекти на профилирането (по-точно с третия етап от профилирането – прилагането на профилите, респ. вземането на решения въз основа на резултатите от прилагането), е чл. 15, озаглавен *Индивидуални автоматизирани решения*. Той ще бъде анализиран по-долу.

Изключително важна стъпка в процеса на изграждането на правна уредба на профилирането е включването на легална дефиниция за него както в Регламента (чл. 4, т. 4), така и в Директива 2016/680<sup>9</sup> (чл. 3, т. 4). Следва да се отбележи, че в първоначалния проект за регламент за защита на личните данни липсваше легална дефиниция на понятието „профилиране“<sup>10</sup>. Затова следва да бъде оценен положително стремежът на европейския законодател да даде легална дефиниция, при това в два акта от вторичното право на ЕС. Дефинициите във въпросните актове са идентични (затова и анализът по-долу ще се основава само на Регламента): „*профилиране*“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение“<sup>11</sup>.

---

<sup>9</sup> Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни и за отмяна на Рамково решение 2008/977/ПВР на Съвета, обн., „Официален вестник на ЕС“, L 119, бр. 59 от 4.05.2016 г. По силата на чл. 63 директивата трябва да бъде транспонирана в правото на държавите членки до 6.05.2018 г., а за някои държави членки този срок може да бъде продължен до 6.05.2023 г., респ. до 6.05.2026 г.

<sup>10</sup> Вж. COM (2012) 11 Final Proposal for a regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), available at [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf) (12.11.2016 г.).

<sup>11</sup> Дефиницията е съобразена и с Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, приет от Работната група по чл. 29 от Директива 95/46 на 13.05.2013 г.

Недостатъците на тази дефиниция обаче могат да доведат до практически проблеми при прилагане на правилата за защита на данните в някои случаи на профилиране.

На първо място, според легалната дефиниция в Регламента профилиране ще е налице при всяка форма на автоматизирано обработване на *лични* данни. Подобен подход, свързващ профилирането само с обработката на лични данни, е необоснован, защото многообразието от профилиращи техники позволява обработката на всякакви данни. Възможно е с цел профилиране да се обработват и данни, които не притежават качеството „лични“; данни, които са били лични, но впоследствие са събрани и обработени като анонимизирани данни, и т.н., като в резултат на подобна обработка се генерира анализ или прогноза за чувствителни лични данни<sup>12</sup>. Според така формулираната дефиниция такава обработка няма да представлява профилиране по смисъла на Регламента. Наред с това при профилирането на групи от хора, а не на отделни индивиди<sup>13</sup> е възможно създадените „групови“ профили (разбирани като абстрактна информация, а не като лични данни) да се прилагат спрямо лицата, без възможност лицата да бъдат идентифицирани, но спрямо тях отново да се вземе дадено решение на база резултатите от прилагането на профила. Подобна хипотеза по-скоро не попада в легалната дефиниция за „профилиране“, доколкото последната изисква обработка на *лични* данни.

Нещо повече, ако не е налице обработка на лични данни, съответната обработка въобще няма да попада в приложното поле на Регламента (чл. 1 говори само за „лични данни“). В този смисъл е възможно не просто профилиране, а профилиране, способно да генерира анализ или прогноза за много чувствителни данни за дадено лице, а в същото време това лице да бъде лишено от защитата, която му предоставя Регламентът. Възможно е да се вземе решение на база прилагането на групов профил спрямо дадени лица, без да те бъдат идентифицирани, и отново да се избегне приложението на Регламента<sup>14</sup>. Неслучайно в литературата се посочва, че дефиницията за лични данни не трябва да бъде пречка пред прилагане на правилата за защита на личните данни спрямо профилирането, а тъкмо напротив – ако тази дефиниция е пречка, тя трябва да се преосмисли<sup>15</sup>.

В този смисъл *de lege ferenda* предлагам дефиницията на профилирането да бъде коригирана, като навсякъде в дефиницията прилагателното „лични“ пред думата „данни“ отпадне. Така приложното поле на понятието „профилиране“ ще се разшири

---

<sup>12</sup> **Custers, B.** The Power of Knowledge. Nijmegen: Wolf Legal Publishers, 2004, p. 19, 57.

<sup>13</sup> **Hildebrandt, M.** Defining Profiling: A New Type of Knowledge? Chapter 2. – In: **Hildebrandt, M., S. Gutwirth** (ed.). Op. cit., p. 20.

<sup>14</sup> **Schreurs, W. and others.** Op. cit., p. 254.

<sup>15</sup> **Gutwirth, S., P. De Hert.** Regulating Profiling in a Democratic Constitutional State. Chapter 14. – In: **Hildebrandt, M., S. Gutwirth** (ed.). Op. cit., p. 289.

и ще даде по-голяма защита на лицата, които са обект на профилиращи техники. Разбира се, в подобна хипотеза ще се постави въпросът дали е допустимо подобно разширяване на материалния обхват на Регламента. Доколкото обработката при профилирането ще е насочена към оценяване на „*определени лични аспекти, свързани с физическо лице*“, подобно разширяване на приложното поле на профилирането не е необосновано, а тъкмо напротив, по-ефективно ще защити лицата при обработка на данни, свързани с тяхната личност. Подобна теза би могло да се обоснове и с логиката на съображение 26 от Регламента, според което „*принципите за защита на данните следва да се прилагат по отношение на всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано*“. По този начин, дори първоначалната обработка да включва данни, които не са лични или са анонимизирани лични данни, ако впоследствие се генерират данни относно лични аспекти на физическото лице, тази обработка трябва да се квалифицира като профилиране и следва да се подчинява на правилата на Регламента.

В този смисъл е и препоръката на Съвета на Европа относно профилирането<sup>16</sup>. В нея се посочва, че профилирането представлява „продължителен процес“, в който, дори на етапа на събирането и обработването на данни да не се обработват лични данни, тези етапи са от съществено значение за определяне на законосъобразността и сигурността на обработването при третата фаза на профилирането (прилагането на профилите спрямо субектите на данни). Поради това тези етапи също следва да бъдат подчинени на правилата за защита на личните данни, дори в тях да не се обработват лични данни.

Освен това, формулирана по този начин, дефиницията на профилирането в Регламента оставя отворен въпроса изчерпателно или примерно е изброяването на личните аспекти, свързани с физическото лице. От една страна, използването на израза *по-конкретно* като че ли загатва, че изброяването е примерно. От друга страна, самият начин на изброяване, завършващ със съюза *или*, и липсата на традиционно използвани изрази при примерното изброяване, като *например, и т.н., и др.*, по-скоро сочат, че изброяването е изчерпателно. При тази постановка анализирането и прогнозирането на чувствителни лични аспекти като сексуална ориентация, политически и философски убеждения и др. (които са специална категория лични данни по смисъла на чл. 9, § 1 от Регламента), няма да попаднат в понятието за профилиране. Разбира се, възможно е по пътя на тълкуването посочените аспекти да бъдат „включени“ в обхвата на някои от изрично изброените – например сексуалната ориентация би могло да се подведе под категорията *лични предпочитания*, политическите и фило-

---

<sup>16</sup> The protection of individuals with regard to automatic processing of personal data in the context of profiling – Recommendation CM/Rec (2010) 13 adopted by the Committee of Ministers of the Council of Europe on 23 November 2010 and explanatory memorandum, Council of Europe Publishing, 2011, p. 39, Para. 99.

софските убеждения – под *интереси*, и т.н. Въпреки това подобен подход крие рискове, тъй като човешката личност е изключително сложно и многоаспектно явление и едва ли може да се формулира легална дефиниция, която да е в състояние да изброи всички аспекти, имащи отношение към личността на отделния човек.

Аргумент, че изброяването е примерно, може да се извлече и от анализа на чл. 15, § 1 от Директивата, въвеждащ забраната за вземането на индивидуални автоматизирани решения спрямо физическите лица (както беше посочено по-горе, това е най-важната разпоредба в Директивата, която има отношение към профилирането, макар в нея да не се споменава думата „профилиране“<sup>17</sup>): в нея се говори за оценяване по автоматизиран път на лични аспекти на дадено физическо лице, „*като резултатите от работата му, кредитоспособност, надеждност, поведение, и т.н.*“. Анализът на разпоредбата води до извод, който се възприема и в теорията<sup>18</sup> – че изброяването в Директивата е *примерно*<sup>19</sup>.

Анализът на правните проблеми, които поставя профилирането, предполага изследване и на останалите релевантни разпоредби в Директивата и Регламента – **най-напред на чл. 15 от Директивата, озаглавен *Индивидуални автоматизирани решения***. Параграф 1 от посочената разпоредба задължава държавите членки да предоставят на всяко лице правото да не бъде обект на решение, което има правни последици за него или го засяга съществено и което се основава единствено на автоматизираната обработка на данни, имаща за цел да се оценяват някои лични аспекти, свързани с него, като резултатите от работата му, кредитоспособност, надеждност, поведение и т.н. Логиката зад създаването на подобна разпоредба е, че Комисията е виждала като една от най-големите опасности на бъдещето злоупотребата с информацията при вземането на решения<sup>20</sup>. Комисията посочва също, че използването на профили при вземането на решения лишава индивида от възможността да влияе на процеса по вземане на решения и води до все по-честото автоматично възприемане на валидността (разбирана като правилност) на автоматизираното решение от хората, като отговорността на човека да изследва съответната фактическа обстановка и да вземе решение (в резултат на съзнателни волеви процеси, а не вследствие на резулта-

---

<sup>17</sup> **Bygrave, L. A.** Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling. – Computer Law & Security Report, 2001, volume 17, 17–24, available at [http://folk.uio.no/lee/oldpage/articles/Minding\\_machine.pdf](http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf), p. 2 (12.11.2016).

<sup>18</sup> **Ehman, E., M. Helfrich.** EG Datenschutzrichtlinie Kurzkommentar. Köln: Verlag Dr. Otto Schmidt, 1999, S. 230.

<sup>19</sup> Трябва също така да се отбележи, че при имплементирането на Директивата в някои държави членки въобще няма изброяване на личните аспекти – така например чл. 34б от българския Закон за защита на личните данни предвижда, че „...*решението на администратора е недопустимо, когато: (...) 2. е основано единствено на автоматизирано обработване на лични данни, предназначено да оценява лични характеристики на физическото лице*“.

<sup>20</sup> **Ehman, E., M. Helfrich.** Op. cit., S. 227.

та от автоматизираната обработка) все повече намалява<sup>21</sup>. Следва да се отбележи, че чл. 22, § 1 от Регламента като цяло повтаря разрешението, залегнало в чл. 15, § 1 от Директивата, поради което анализът по-долу се отнася и за двете разпоредби.

В литературата съществува противоречие дали с посочената разпоредба на Директивата се въвежда абсолютна забрана за автоматизирано вземане на решения<sup>22</sup>, или единствено се регламентира допустимостта на автоматизираните решения<sup>23</sup>. Езиковият анализ на разпоредбата и обстоятелството, че чл. 15 от Директивата урежда предоставянето на субективно право на едно лице да не бъде обект на автоматизирани решения (т.е. от засегнатото лице зависи дали да го упражни, или не), са предпоставка някои автори да считат, че чл. 15 регламентира единствено допустимостта на автоматизираните решения<sup>24</sup>. Това разбиране следва да бъде споделено. Въвеждането на правото на лицето да изрази своето мнение (а с Регламента – и да оспори взетото решение) подсказва, че според логиката на европейския законодател вземането на такива решения по принцип не е абсолютно забранено, но засегнатото лице следва да има набор от права, с които да се защити (например право да изрази своето мнение, да оспори резултата и т.н.).

За да се приложи чл. 15, § 1 от Директивата, респ. чл. 22, § 1 от Регламента, трябва кумулативно да са налице четири елемента:

1. Вземане на решение;
2. Решението трябва да има правни или други съществени последици за физическото лице;
3. Решението трябва да се основава единствено на автоматизираната обработка на данни;
4. Обработката трябва да има за цел да се оценяват някои лични аспекти, свързани със засегнатото физическо лице.

По отношение на първия елемент в литературата се посочва, че трябва да е налице някакво отношение, мнение или позиция спрямо физическото лице. Сочи се още, че понятието „решение“ трябва да се тълкува широко и свободно в светлината на логиката на разпоредбата и макар това понятие да се свързва по правило с определена психическа активност у субекта, който го взема, разпоредбата трябва да обхваща и ситуации, в които софтуер взема решения на база въведени данни без каквато и да е човешка намеса<sup>25</sup>.

<sup>21</sup> Bygrave, L. A. Op. cit.

<sup>22</sup> Brühann, U., T. Zerdick. Umsetzung der EG-Datenschutzrichtlinie. – CR 7/1996, 429–436.

<sup>23</sup> Dammann, U., S. Simitis. Datenschutzrichtlinie, Kommentar. Baden-Baden: Nomos, 1997.

<sup>24</sup> Ehman, E., M. Helfrich. Op. cit., S. 228.

<sup>25</sup> Bygrave, L. A. Op. cit.

По отношение на втория елемент понятието *правни последици* е относително ясно и се свързва с такива последици, които са в състояние да променят или предопределят правата и задълженията на дадено лице<sup>26</sup>. Известна неяснота обаче поражда изразът *по подобен начин го засяга съществено* (в Регламента *по подобен начин го засяга в значителна степен*). Той трябва да се разбира в обективен смисъл (т.е. не бива да е предопределящо дали отделният човек оценява съответното засягане като „съществено“, а по-скоро от значение е дали то би се възприело като такова от други хора в подобна ситуация). Спорен е въпросът дали „същественото засягане“ предполага само неблагоприятни последици за лицето, или не, още повече че в проекта за директива изрично е било включено прилагателното „неблагоприятни“, а във финалния текст то е отпаднало. В теорията основателно се посочва, че е много дискуссионна възможността да се приложи чл. 15, § 1 от Директивата спрямо решение, което е изцяло положително за субекта<sup>27</sup>.

Неясно е също така дали персонализираните чрез алгоритми реклами може да се приемат за правни последици или за последици, засягащи по друг начин съществено съответния субект на данни. Рекламите не засягат в такава съществена степен субектите както например автоматичният отказ на онлайн искания за кредит или електронните практики за набиране на персонал без човешка намеса<sup>28</sup>. Някои автори обаче посочват, че след като чл. 22 от Регламента цели да регулира „възможно най-всеобхватно“ профилирането, то следва да се отнася и за „широко разпространената практика“ на създаването на профили при използване на информационни и комуникационни услуги<sup>29</sup> (т.е. правилата на Регламента за профилирането следва да се отнасят и за персонализирани реклами).

По отношение на третия елемент следва да се има предвид, че понятието *единствено* може да породи известна несигурност, доколкото почти всички програми на даден етап са включвали човешка намеса. Всъщност въпросното изискване предполага такава липса на човешка намеса, при която човек не е участвал активно и не е оказал реално въздействие върху процеса по вземане на решението<sup>30</sup>.

По отношение на четвъртия елемент, наред с изложеното по-горе относно личностните аспекти на съответното физическо лице, следва да се имат предвид още няколко особености: за да се приложи чл. 15, § 1 от Директивата, респ. чл. 22, § 1 от Регламента, необходимо е автоматизираното решение да се основава на анализ на *ня-*

<sup>26</sup> Bygrave, L. A. Op. cit., p. 7.

<sup>27</sup> Ibid, p. 8.

<sup>28</sup> Същите са посочени изрично в Регламента като примери за решения, които пораждат правни последици за субекта или го засягат също толкова значително (съображение 71, изр. 1).

<sup>29</sup> Härting, H. Datenschutz-Grundverordnung. Köln: Dr. Otto Schmidt, 2016, S. 151, Para. 618.

<sup>30</sup> Bygrave, L. A. Op. cit.

кои, но не и на всички личностни аспекти на физическото лице. Релевантни са тези личностни аспекти, които описват неговия характер – способности, поведение, предпочитания, потребности и т.н., а не тези, които имат чисто физиологичен характер, без да разкриват характера на лицето – скорост на реакция, кръвна група и т.н. (освен ако не се комбинират с други данни, разкриващи аспекти от характера на лицето – степен на положено старание, респ. нестарание, в дадена ситуация и т.н.)<sup>31</sup>.

Важно е да се отбележи, че както разпоредбата на чл. 15 от Директивата, така и нейният аналог – чл. 22 от Регламента, предвиждат определени **основания, при които забраната за автоматизирано вземане на решения (в това число и за профилиране) не се прилага**, т.е. автоматизираното вземане на решения е позволено. Според Директивата такова решение е допустимо, ако:

1. е взето по време на сключването/изпълнението на договор, при условие че молбата за сключване/изпълнение на договора, подадена от съответното физическо лице, е била удовлетворена или че съществуват подходящи мерки за гарантиране на неговите законни интереси като възможности, които му позволяват да изложи своето мнение (чл. 15, § 2, б. „а“);

2. е разрешено от закона, който също постановява мерки за гарантиране на законните интереси на съответното физическо лице (чл. 15, § 2, б. „б“).

Към посочените в Директивата условия Регламентът добавя още една нова хипотеза – забраната не се прилага, ако решението:

3. се основава на изричното съгласие на субекта на данни (чл. 22, § 2, б. „в“).

В Регламента първото основание търпи известни промени, доколкото се изисква решението да е **необходимо** за сключването или изпълнението на договор. Теоретици посочват, че преценката за необходимостта от такова решение следва да се основава на обективни критерии<sup>32</sup>, т.е. естеството на услугите по договора да предполага извършването на профилиране – например анализ на енергийното потребление в едно домакинство при предоставяне на услугата Smart Home (на български език – „Умен дом“)<sup>33</sup>. Субективната преценка на доставчика на съответните услуги по договора няма да е достатъчна, за да се приложи въпросното основание. Така например, дори от гледна точка на една кредитна институция да изглежда смислено, полезно и дори задължително да създаде профил на свой потенциален кредитополучател, обективно профилиране в такъв случай няма да е необходимо<sup>34</sup> – в такава хипотеза чл. 22, § 2, б. „а“ от Регламента няма да се приложи.

Директивата и Регламентът изискват като условие за допустимостта на такова решение да се осигурят подходящи мерки за защита на правата, свободите и легитим-

<sup>31</sup> Bygrave, L. A. Op. cit., p. 11.

<sup>32</sup> Härting, H. Op. cit., S. 151, Rz. 620–621.

<sup>33</sup> Ibid, S. 147, Rz. 599.

<sup>34</sup> Ibid, S. 152, Rz. 620.

ните интереси на субекта на данните. Като пример двата акта посочват правото на лицето да изрази гледната си точка, а Регламентът добавя и още две права – **правото на човешка намеса** от страна на администратора и **правото на субекта да оспори решението**. Правото на човешка намеса се посочва в теорията като необходимо условие за упражняване на правото да се изрази мнение още в Директивата, макар и да не е изрично записано в нея<sup>35</sup>. Закрепването му в изрична разпоредба в Регламента безспорно ще подобри регламентацията. Съществен е въпросът в кой момент лицето може да изрази мнението си, респ. да оспори решението. В теорията се приема за безспорно, че правото да се изрази мнение трябва да се упражни от засегнатото лице, **преди** да бъде взето окончателно решение спрямо него, в противен случай това право би се обезсмислило<sup>36</sup>. По-различна обаче е ситуацията с правото да се оспори решението – самата конструкция на това право иманентно предполага наличието на *вече* взето решение (или поне наличието на проект за такова решение). Логиката на цитираните разпоредби несъмнено изисква лицето да бъде уведомено, че за него е формирано решение на база профилиране (или друго автоматизирано обработване на данни), да бъде запознато с решението или с проекта за решение и да му се даде възможност да го оспори, преди решението да бъде приложено на практика.

Във връзка с правото на човешка намеса следва да се направи допълнително уточнение – възможна е хипотеза, в която човек механично (рутинно) следва решението, генерирано по автоматизиран път, без да анализира в дълбочина съответния проблем. Ето защо правото да се осигури човешка намеса следва да се тълкува в смисъл, че администраторът трябва да осигури в разумна степен ангажираността на човек, който въз основа на собствена мисловна активност и задълбочена проверка на данните, които са основа за вземане на решение, да провери правилността на съответното решение<sup>37</sup>.

Третото основание за дерогиране на забраната за автоматизирано вземане на решения – съгласието на субекта на данни, е новост в Регламента в сравнение с Директивата. То заслужава специално внимание, защото при профилиращите техники е възможно генерирането на хипотези и постигането на резултати, които са непредвидими както за субекта на данните, така и за лицето, обработващо данните (администратор или обработващ). В същото време по смисъла на Регламента „*съгласие на субекта на данните*“ означава всяко **свободно изразено, конкретно, информирано и недвусмислено указание** за волята на субекта на данните, изразено чрез изявление или ясно потвърждаващо действие, което **изразява съгласието му свър-**

<sup>35</sup> Bygrave, L. A. Op. cit.

<sup>36</sup> Ehman, E., M. Helfrich. Op. cit., S. 233.

<sup>37</sup> Koops, B.-J. Some Reflections on Profiling, Power Shifts and Protection Paradigms – Reply to Hildebrandt, M. Profiling and the Identity of the European, Citizen, Chapter 15. – In: Hildebrandt, M., S. Gutwirth (ed.). Op. cit., p. 336.

заните с него лични данни да бъдат обработени“ (чл. 4, т. 11). В този смисъл е изключително дискуссионна възможността да се допусне профилиране въз основа на съгласието на лицето. Нещо повече, събирането и обработката на данни с профилиращи техники, при които е възможно и генерирането на никому неизвестни резултати, противоречи на принципа на събиране на данни за конкретни, изрично указани и легитимни цели (чл. 5, § 1, б. „б“ от Регламента). В същото време както в Препоръката на Съвета на Европа, така и в актовете на работната група по чл. 29 от Директивата<sup>38</sup> се посочва, че съгласието следва да бъде предвидено като основание за допустимостта на профилирането. В този смисъл съгласие от субекта на данните за профилиране следва да се търси и получи на две плоскости:

– съгласие за категориите данни, които може да се обработват (например само данни, свързани с интернет активност, посещения на интернет сайтове, търсене в търсачки и т.н.);

– съгласие за категориите резултати, които може да се получат (например резултати, свързани с потребителските предпочитания и интереси на лицето – предпочитани филми, книги и т.н.) – по аналогия с разрешението в съображение 33 от Регламента, при което поради невъзможността да се определи целта на обработването на лични данни за научноизследователски цели субектите на данни дават съгласие само за определени области на научни изследвания или части от научноизследователски проекти.

Съществена новост в Регламента в сравнение с Директивата е забраната по чл. 22, § 4 профилирането, респ. вземането на автоматизирани решения, да се основава на обработката на специални категории данни по чл. 9. В литературата с основание се посочва, че профилиране въз основа на тези данни би породило твърде голям риск от дискриминация въз основа на защитен признак<sup>39</sup>. Регламентът все пак допуска derogирането на това правило (при съгласие на лицето – чл. 9, б. „а“, или при необходимост от обработването в обществен интерес – чл. 9, б. „ж“).

Директивата (чл. 12, б. „а“, предложение 3) и Регламентът уреждат правото на лицето, което е обект на автоматизирано вземане на решения, да бъде запознато с логиката, на която е основано автоматизираното вземане на решения (Регламентът говори за *съществена информация относно използваната логика* – чл. 13, § 2, б. „е“; чл. 14, § 2, б. „е“; чл. 15, § 1, б. „з“). Новост в Регламента е изискването да се предостави на лицето в момента на получаване на личните му данни информация за съ-

---

<sup>38</sup> Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, p. 3.

<sup>39</sup> **Bosco, F. and others.** Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities – Chapter 1. – In: **Gutwirth, S. and others** (ed.). Reforming European Data Protection Law, Law, Governance and Technology Series 20. Dordrecht, Springer Science + Business Media, 2015, p. 21.

ществуването на автоматизирано вземане на решения, включително профилирането, посочено в чл. 22, § 1 и 4. Това е положителна стъпка от страна на европейския законодател, защото един от често изтъкваните проблеми при профилирането е асиметричната информираност в отношенията профилиран – профилиращ, доколкото хората често не знаят, че са обект на профилиране, нито знаят относно какви личностни аспекти и при какви критерии за оценка се извършва профилирането<sup>40</sup>.

Регламентът въвежда и няколко **нови правила относно профилирането**, които не се съдържат в Директивата. На първо място, по силата на чл. 21, § 1 субектът на данните има право по всяко време и на основания, свързани с неговата конкретна ситуация, **да възрази** срещу обработване на лични данни, отнасящи се до него, което се основава на чл. 6, § 1, б. „д“<sup>41</sup> или б. „е“<sup>42</sup>, включително профилиране, основаващо се на посочените разпоредби. В такъв случай администраторът е длъжен да прекрати обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции. Аналогично право на възражение срещу профилирането е предвидено, ако то се използва **за целите на директния маркетинг** (чл. 21, § 2) – в този случай обработването се прекратява (чл. 21, § 3). Регламентът изисква субектът на данните изрично да се уведомява за съществуването на правото по § 1 и 2 по ясен начин и отделно от всяка друга информация. Това трябва да стане най-късно в момента на първото осъществяване на контакт със субекта на данните (чл. 21, § 4).

Регламентът въвежда и т.нар. **оценка на въздействието** (на английски език – *impact assessment*). Според чл. 35, § 1 от Регламента администраторът е длъжен да извърши оценка на въздействието на предвидените операции по обработването на личните данни, когато е налице вероятност определен вид обработване, при което се използват нови технологии, да породи висок риск за правата и свободите на физическите лица. Тази оценка се извършва **преди** обработването. Допуска се в една оценка да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове.

С Регламента се реформира и работната група по чл. 29 от Директивата – тя става Европейски комитет по защита на данните (Комитета), който става орган на

---

<sup>40</sup> **Hildebrandt, M.** Profiling and the Identity of the European Citizen Chapter 15. – In: **Hildebrandt, M., S. Gutwirth** (ed.). Op. cit., p. 308; Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation.

<sup>41</sup> Изпълнението на задача от обществен интерес или при упражняването на официални правомощия.

<sup>42</sup> Наличие на легитимни интереси на администратора/трета страна, освен когато пред тях преимущество имат интересите/основните права и свободи на субекта на данните (когато субектът на данните е дете).

Съюза и ще притежава своя правосубектност (чл. 68, § 1 от Регламента). Комитетът има правомощия да издава насоки, препоръки и най-добри практики за допълнително уточняване на критериите и условията във връзка с решенията, основани на профилиране на данни съгласно чл. 22, § 2 от Регламента (чл. 70, § 1, б. „е“).

Развитието на информационните и комуникационните технологии (ИКТ) е от естество да катализира важни промени в обществото и икономиката, но в правовата държава тяхното функциониране трябва да се подчинява на ясни правила. В този смисъл реформата в сферата на защитата на личните данни е много важна стъпка в правилната посока. Тепърва ще стане ясно дали Регламентът ще издържи проверката на времето. Във всички случаи обаче положителен е стремежът на европейския законодател да постави автоматизираното профилиране в определени правни рамки, които да регламентират неговата прозрачност и законосъобразност и да гарантират правата на лицата, чиито данни се обработват с цел профилиране.