РАБОТНА ГРУПА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПО ЧЛЕН 29

17/BG

WP 251 rev. 01

Насоки относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент (ЕС) 2016/679

Приети на 3 октомври 2017 г.

Последно преработени и приети на 6 февруари 2018 г.

РАБОТНАТА ГРУПА ЗА ЗАЩИТА НА ЛИЦАТА ПРИ

ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

създадена с Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г.,

като взе предвид членове 29 и 30 от нея,

като взе предвид Правилника за дейността си,

ПРИЕ НАСТОЯЩИТЕ НАСОКИ:

СЪДЪРЖАНИЕ

I. Въведение

В Общия регламент относно защитата на данните („ОРЗД“) конкретно се разглеждат профилирането и автоматизираното вземане на индивидуални решения, включващо профилиране[1].

Профилирането и автоматизираното вземане на решения се използват във все по-голям брой сектори — както частни, така и публични. Банковото дело и финансите, здравеопазването, данъчното облагане, застраховането, маркетингът и рекламите са само някои примери за областите, в които все по-редовно се извършва профилиране в подкрепа на вземането на решения.

Технологичният напредък и възможностите за анализи на големи информационни масиви, изкуственият интелект и машинното самообучение улесниха създаването на профили и вземането на автоматизирани решения, които имат потенциал да окажат значително въздействие върху правата и свободите на физическите лица.

Широкоразпространената достъпност на лични данни в интернет и от устройства с „интернет на нещата“ (IoT), както и възможността да се установяват корелации и да се създават връзки могат да позволят определяне, анализ и предвиждане на личностни или поведенчески аспекти на даден човек и на неговите интереси и навици.

Профилирането и автоматизираното вземане на решения могат да бъдат полезни за хората и за организациите, като осигуряват ползи, например:

- повишена ефикасност; както и
- икономии на ресурси.

Те имат множество търговски приложения, например могат да бъдат използвани за по-добро сегментиране на пазарите и за приспособяване на услугите и продуктите, така че да

[1] 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. Профилирането и автоматизираното вземане на индивидуални решения също така са обхванати от 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. Макар че настоящите насоки са насочени към профилирането и автоматизираното вземане на индивидуални решения съгласно ОРЗД, по отношение на тези две теми те са уместни и във връзка със сходните разпоредби в Директива (ЕС) 2016/680. Анализът на конкретни характеристики на профилирането и автоматизираното вземане на индивидуални решения съгласно Директива (ЕС) 2016/680 не е включен в настоящите насоки, тъй като в това отношение са предоставени насоки в Становище WP 258 — „Становище относно някои ключови въпроси във връзка с Директивата относно правоприлагането (Директива (ЕС) 2016/680)“, прието от Работната група по член 29 (наричана по-нататък „РГ29“) на 29 ноември 2017 г. Автоматизираното вземане на индивидуални решения и профилирането в контекста на обработването на данни за целите на правоприлагането са разгледани на стр. 11—14 от това становище, като то е достъпно на адрес: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178

съответстват на индивидуалните нужди. Тези процеси могат да бъдат от полза и в областите на медицината, образованието, здравеопазването и транспорта.

При все това профилирането и автоматизираното вземане на решения могат да породят значителни рискове за правата и свободите на физическите лица, което изисква да бъдат въведени подходящи гаранции.

Възможно е тези процеси да не са видими. Хората може да не знаят, че са подложени на профилиране, или да не разбират какво включва това.

Профилирането може да поддържа съществуващите стереотипи и социалната сегрегация. Освен това то може да „заключи“ дадено лице в конкретна категория и да го ограничи до прогнозираните му предпочитания. По този начин може да се подрони свободата му например да избере определени продукти или услуги като книги, музика или информационни канали. В някои случаи профилирането може да доведе до неточни предвиждания. В други случаи е възможно да доведе до отказ на услуги и стоки и до необоснована дискриминация.

С ОРЗД се въвеждат нови разпоредби за преодоляване на рисковете, произтичащи от профилирането и автоматизираното вземане на решения, по-специално по отношение на неприкосновеността на личния живот, но без да са ограничени само до тази област. Целта на настоящите насоки е да се пояснят тези разпоредби.

Документът обхваща:

- Определения на профилиране и на автоматизирано вземане на решения и принципният подход в ОРЗД към тях — глава II
- Общи разпоредби относно профилирането и автоматизираното вземане на решения — глава III
- Специфични разпоредби, насочени към изцяло автоматизираното вземане на решения, определено в член 22 — глава IV
- Профилирането и децата — глава V
- Оценки на въздействието върху защитата на данните и длъжностни лица по защита на данните — глава VI

В приложенията са посочени препоръки за най-добри практики, като се използва натрупаният опит на държавите — членки на ЕС.

Работната група за защита на личните данни по член 29 (РГ29) ще наблюдава прилагането на настоящите насоки и по целесъобразност може да ги допълва с допълнителни подробности.

II. Определения

ОРЗД включва разпоредби за гарантиране, че профилирането и автоматизираното вземане на индивидуални решения (независимо дали включва профилиране или не) не се използват по начини, които оказват необосновано въздействие върху правата на физическите лица; например:

- специфични изисквания за прозрачност и добросъвестност;
- повишени задължения за отчетност;
- посочени правни основания за обработването;
- права на физическите лица да възразят срещу профилирането и по-конкретно срещу профилирането за маркетингови цели; както и

- ако са изпълнени определени условия, необходимостта от извършване на оценка на въздействието върху защитата на данните.

ОРЗД не е насочен само към решенията, които се вземат в резултат на автоматизирано обработване или профилиране. Той се прилага към събирането на данни за създаване на профили, както и към прилагането на тези профили към физически лица.

А. **Профилиране**

В член 4, параграф 4 от ОРЗД профилирането се определя като:

> 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;

Профилирането се състои от три елемента:

- то трябва да представлява *автоматизирана* форма на обработване;
- трябва да се извършва *с лични данни*; както и
- целта на профилирането трябва да бъде *оценяването на лични аспекти*, свързани с физическо лице.

В член 4, параграф 4 се посочва „всяка форма на автоматизирано обработване“ а не само „изцяло“ автоматизираното обработване (за което се говори в член 22). Профилирането трябва да включва някаква форма на автоматизирано обработване — макар че участието на човек не означава непременно, че съответната дейност вече не попада в приложното поле на определението.

Профилирането представлява процедура, която може да включва поредица от статистически изводи. То често се използва за изготвянето на прогнози относно хората, като се използват данни от различни източници с цел да се направи извод за дадено лице въз основа на качествата на други лица, които изглеждат статистически сходни.

Съгласно ОРЗД профилирането представлява автоматизирано обработване на лични данни за оценяване на лични аспекти, по-специално за анализ *или* за изготвяне на прогнози относно физически лица. Използването на думата „оценяване“ предполага, че профилирането включва някаква форма на оценка или преценка на дадено лице.

Просто класифициране на лицата въз основа на известни характеристики като възраст, пол и ръст не води непременно до профилиране. Това ще зависи от целта на класифицирането. Например дадено предприятие може да желае да класифицира своите клиенти по възраст или пол за статистически цели и за да добие обща представа за тях, без да прави прогнози или да достига до заключения относно конкретно лице. В този случай целта не е оценка на индивидуални характеристики и съответно не се извършва профилиране.

Определението в ОРЗД е вдъхновено от, но не е съвсем същото като определението за профилиране в Препоръка CM/Rec (2010)13 на Съвета на Европа[2] (наричана по-нататък „Препоръката“), тъй като Препоръката *изключва* обработването, което не включва извеждането на изводи. Независимо от това Препоръката включва полезното обяснение, че профилирането може да включва три отделни етапа:

- събиране на данни;
- автоматизиран анализ за установяване на корелации;
- прилагане на корелацията към конкретно лице, за да се определят характеристиките на неговото настоящо или бъдещо поведение.

Администраторите, които извършват профилиране, ще трябва да гарантират, че изпълняват изискванията на ОРЗД на всички горепосочени етапи.

Най-общо казано, профилирането означава събиране на информация относно дадено лице (или група лица) и оценяване на неговите характеристики или модели на поведение, за да бъде класифицирано в определена категория или група, по-специално с цел анализ и/или прогнозиране например на:

- способността му да изпълнява определена задача;
- интересите му; или
- вероятното му поведение.

Пример

Брокер на данни събира данни от различни публични и частни източници, било то от името на своите клиенти или за собствени цели. Брокерът на данни компилира данните, за да изготви профили на отделните лица и да ги постави в определени сегменти. Той продава тази информация на дружества, които желаят да подобрят целевото насочване на своите стоки и услуги. Брокерът на данни извършва профилиране, като поставя лице в дадена категория в зависимост от неговите интереси.

Въпросът дали е налице автоматизирано вземане на решения съгласно определението в член 22, параграф 1 ще зависи от конкретните обстоятелства.

Б. Автоматизирано вземане на решения

Приложното поле на автоматизираното вземане на решения е различно и може частично да се припокрива с профилирането или да произтича от него. Изцяло автоматизираното вземане на решения представлява способността за вземане на решения с технологични средства без човешка намеса. Автоматизираните решения могат да се основават на всякакви видове данни, например:

- данни, предоставени директно от съответните лица (например отговори на въпросник);

[2] Съвет на Европа. Защитата на лицата по отношение на автоматизираното обработване на лични данни в контекста на профилирането. Препоръка CM/Rec(2010)13 и обяснителен меморандум. Съвет на Европа, 23 ноември 2010 г. https://rm.coe.int/16807096c3 . Осъществен достъп на 24 април 2017 г.

- данни, които се установяват относно лицата (например данни за местонахождението, които се събират чрез приложение);
- извлечени или изведени по дедуктивен път данни, като например вече създаден профил на лицето (например кредитна оценка).

Автоматизирани решения могат да се вземат със или без профилиране; профилирането може да се извършва без вземането на автоматизирани решения. При все това профилирането и автоматизираното вземане на решения не представляват непременно отделни дейности. Действие, което започва като обикновен процес на автоматизирано вземане на решения, би могло да се превърне в основан на профилиране процес в зависимост от начина, по който се използват данните.

Пример

Налагането на глоби за превишена скорост единствено въз основа на доказателства от камери за контрол на скоростта представлява процес на автоматизирано вземане на решения, който не включва непременно профилиране.

Вземаните решения обаче ще се превърнат в решения на основата на профилиране, ако се следят навиците за шофиране на конкретно лице във времето и ако например размерът на наложената глоба бъде определен в резултат на оценка, която включва и други фактори, например дали превишената скорост представлява повторно нарушение или дали водачът наскоро е извършил и други нарушения на правилата за движение.

Решения, които не са само автоматизирани, също могат да включват профилиране. Например преди да предостави ипотека дадена банка може да проучи кредитната оценка на заемополучателя, като хора осъществяват съдържателна допълнителна намеса преди решението да бъде приложено към конкретно лице.

B. <u>Как са разгледани понятията в ОРЗД</u>

Профилирането потенциално може да бъде използвано по три начина:

i) общо профилиране;
ii) вземане на решения на основата на профилиране; както и
iii) *изцяло* автоматизирано вземане на решения, включващо профилиране, което поражда правни последици за субекта на данните или по подобен начин го засяга в значителна степен (член 22, параграф 1).

Разликата между точки ii) и iii) може да се демонстрира най-добре чрез следните два примера, в които дадено лице кандидатства за заем онлайн:

- решението относно одобрението на заема се взема от човек въз основа на профил, изготвен изцяло чрез автоматизирани средства (точка ii);
- решението относно одобрението на заема се взема чрез алгоритъм и лицето се известява по автоматизиран начин за решението, без преди това да е извършена съдържателна оценка от човек (точка iii).

Администраторите могат да извършват профилиране и автоматизирано вземане на решения, при условие че спазват всички принципи и че разполагат със законосъобразно основание за обработването. Прилагат се допълнителни гаранции и ограничения, в случай че се извършва изцяло автоматизирано вземане на решения, включващо профилиране, съгласно определението в член 22, параграф 1.

В глава III от настоящите насоки се обясняват разпоредбите на ОРЗД за *всички* случаи на профилиране и автоматизирано вземане на индивидуални решения. Това включва процеси на вземане на решения, които *не* са изцяло автоматизирани.

В глава IV от настоящите насоки се обясняват конкретните разпоредби, които се отнасят *само* до изцяло автоматизираното вземане на индивидуални решения, включващо профилиране[3]. Съществува обща забрана на този вид обработване, която отразява потенциалните рискове за правата и свободите на физическите лица.

III. Общи разпоредби относно профилирането и автоматизираното вземане на решения

Настоящият преглед на разпоредбите се прилага към всички случаи на профилиране и автоматизирано вземане на решения. Посочените в глава IV допълнителни специфични разпоредби се прилагат, ако обработването отговаря на определението в член 22, параграф 1.

A. Принципи за защита на данните

Принципите важат за всички случаи на профилиране и автоматизирано вземане на решения, при които се използват лични данни[4]. За да се улесни спазването, администраторите следва да отчетат следните области от ключово значение:

1. Член 5, параграф 1, буква а) — законосъобразно, добросъвестно и по прозрачен начин

Прозрачността на обработването[5] е основно изискване на ОРЗД.

Процесът на профилиране често е невидим за субекта на данни. Той функционира чрез създаване на извлечени или изведени по дедуктивен път данни относно физически лица — „нови“ лични данни, които не са предоставени директно от самите субекти на данни. Степента на разбиране е различна при всяко лице и на някои хора може да им бъде трудно да разберат сложните техники, които се използват при процесите на профилиране и автоматизирано вземане на решения.

Съгласно член 12, параграф 1 администраторът трябва да предостави на субектите на данни информация относно обработването на техните лични данни в кратка, прозрачна, разбираема и лесно достъпна форма[6].

---

[3] Съгласно определението в член 22, параграф 1 от ОРЗД.

[4] Съображение 72 от ОРЗД — „Профилирането се подчинява на правилата на настоящия регламент относно обработването на лични данни, например правните основания за обработването или принципите за защитата на данни“.

[5] Насоките на Работната група за защита на личните данни по член 29 относно прозрачността разглеждат прозрачността по-подробно; вж. „Guidelines on Transparency under Regulation 2016/679“ (Насоки относно прозрачността в съответствие с Регламент 2016/679), (WP260rev.01), 11 април 2018 г., http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[6] Служба на комисаря по информацията на Австралия. В „Consultation draft: Guide to big data and the Australian Privacy Principles“ (Проект за консултация: ръководство за големите информационни масиви и

По отношение на данните, събирани директно от субекта на данни, тази информация следва да бъде предоставена към момента на събирането (член 13); по отношение на данни, получени по косвен път, информацията следва да бъде предоставена в рамките на сроковете, посочени в член 14, параграф 3.

Пример

Някои застрахователи предлагат застрахователни ставки и услуги, основани на поведението при шофиране на конкретен водач. Елементите, които се отчитат в тези случаи, биха могли да включват изминатото разстояние, прекараното в шофиране време и предприетите пътувания, както и прогнози въз основа на други данни, събирани от сензорите на (интелигентен) автомобил. Събраните данни се използват за профилиране, насочено към откриването на лошо поведение при шофиране (например бързо ускоряване, внезапно спиране и каране с превишена скорост). Тази информация може да бъде съпоставена с други източници (например метеорологичните условия, движението, вида настилка), за да се разбере по-добре поведението на водача.

Администраторът трябва да гарантира, че разполага със законосъобразно основание за този вид обработване на данни. Той също така трябва да информира субекта на данни относно събраните данни и по целесъобразност относно наличието на автоматизирано вземане на решения, посочено в член 22, параграфи 1 и 4, използваната логика, както и значението и предвидените последствия от това обработване.

Конкретните изисквания във връзка с информацията и достъпа до лични данни са разгледани в глави III (раздел Г) и IV (раздел Д).

Обработването също така трябва да бъде добросъвестно и прозрачно.

Профилирането може да бъде недобросъвестно и да поражда дискриминация, например като се отказва достъп на някои лица до възможности за заетост, до кредит или застраховка или ако им се предлагат прекалено рисковани или скъпи финансови продукти. Следният пример, който не отговаря на изискванията на член 5, параграф 1, буква а), илюстрира по какъв начин в резултат на недобросъвестното профилиране на някои потребители може да бъдат предложени по-привлекателни сделки в сравнение с други.

Пример

Брокер на данни продава потребителски профили на финансови дружества без разрешението или знанието на потребителите за съответните данни. В профилите потребителите са класифицирани в категории (с наименования като „От провинцията и едва се справят“, „Етнически малцинства от по-малки градове“, „Трудно начало: самотни млади родители“) или получават точки, като се поставя акцент върху финансовата им уязвимост. Финансовите

австралийските принципи за неприкосновеност на личния живот), май 2016 г., се посочва: „Известията, свързани с неприкосновеността на личния живот, трябва да представят практиките за обработване на данни по ясен и прост, но същевременно изчерпателен и достатъчно конкретен начин, за да бъдат полезни. *Самата технология, която води до повишено събиране на лични данни, също така дава възможност за по-динамични, многослойни и насочени към потребителя известия, свързани с неприкосновеността на личния живот“.* https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles. Осъществен достъп на 24 април 2017 г.

дружества предлагат на тези потребители заеми до заплата и други „нетрадиционни“ финансови услуги (заеми с високи лихви и други рискови финансови продукти)[7].

2. Член 5, параграф 1, буква б) — по-нататъшно обработване и ограничение на целите

Профилирането може да включва използването на лични данни, които първоначално са били събрани за друга цел.

Пример

Някои мобилни приложения предоставят услуги за определяне на местоположението, като позволяват на потребителя да намери близки ресторанти, предлагащи отстъпки. При все това събраните данни се използват и за изграждане на профил на субекта на данни за маркетингови цели — за да се определят предпочитанията му по отношение на храната или начинът му на живот като цяло. Субектът на данни очаква неговите данни да бъдат използвани за намиране на ресторанти, а не за да получава реклами за доставка на пица само защото приложението е установило, че той се прибира късно у дома. Това допълнително използване на данните за местонахождението може и да не е съвместимо с целите, за които данните изобщо са били събрани, и съответно може да изисква да бъде получено съгласието на конкретното лице[8].

Въпросът дали това допълнително обработване е съвместимо с първоначалните цели, за които са събрани данните, ще зависи от редица фактори[9], включително каква информация е предоставил първоначално администраторът на субекта на данни. Тези фактори са отразени в ОРЗД[10] и са обобщени по-долу:

- връзката между целите, за които са събрани данните, и целите на по-нататъшното обработване;
- контекстът, в който са събрани данните, и разумните очаквания на субектите на данни по отношение на по-нататъшното им използване;

[7] Този пример е взет от: Сенат на Съединените американски щати, Комисия по търговия, наука и транспорт. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller (Преглед на сектора за брокерска дейност с данни: събиране, използване и продажба на потребителски данни за маркетингови цели, информативен доклад за председателя Рокфелер), 18 декември 2013 г. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf . Вж. по-специално стр. ii от обобщението и стр. 12 от основната част на документа. Осъществен достъп на 21 юли 2017 г.

[8] Следва да се отбележи, че може да се прилагат и разпоредбите на бъдещия Регламент за правото на неприкосновеност на личния живот и електронните съобщения.

[9] Изтъкнати в Становище 03/2013 на работната група за защита на личните данни по член 29 от 2 април 2013 г. относно ограничението на целите. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf . Осъществен достъп на 24 април 2017 г.

[10] Член 6, параграф 4 от ОРЗД.

- естеството на данните;
- въздействието от по-нататъшното обработване върху субектите на данни; както и
- прилаганите от администратора гаранции за осигуряване на добросъвестно обработване и за избягване на необосновано въздействие върху субектите на данни.

3. Член 5, параграф 1, буква в) — свеждане на данните до минимум

Възможностите за бизнес, които се създават от профилирането, по-ниските разходи за съхранение и способността да се обработват големи количества информация, могат да окуражат организациите да събират повече лични данни, отколкото им трябват в действителност, в случай че се окажат полезни в бъдеще. Администраторите трябва да се уверят, че спазват принципа за свеждане на данните до минимум, както и изискванията за ограничение на целите и принципите за ограничение на съхранението.

Администраторите следва да бъдат в състояние ясно да обяснят и обосноват необходимостта от събиране и запазване на лични данни или да обмислят възможността да използват агрегирани, анонимизирани или (когато по този начин се осигурява достатъчна защита) псевдонимизирани данни за профилиране.

4. Член 5, параграф 1, буква г) — точност

Администраторите следва да отчитат точността на всички етапи от процеса на профилиране, и по-специално при:

- събирането на данни;
- анализа на данни;
- изготвянето на профил за дадено лице; или
- прилагането на профил, за да се вземе решение, което засяга лицето.

Ако използваните данни при процеса на автоматизирано вземане на решения или на профилиране са неточни, получените в резултат на това решения или профили ще бъдат неправилни. Възможно е решенията да бъдат взети въз основа на остарели данни или на неправилно тълкуване на външни данни. Неточностите могат да доведат до неправилни прогнози или твърдения, например относно здравословното състояние, кредитния или застрахователния риск на дадено лице.

Дори ако необработените данни бъдат записани точно, наборът от данни може да не е напълно представителен или анализът може да съдържа прикрита пристрастност.

Администраторите трябва да въведат надеждни мерки за постоянна проверка и гарантиране, че повторно използваните или получените по косвен път данни са точни и актуални. Това подчертава колко е важно да се предоставя ясна информация относно личните данни, които се обработват, така че субектът на данни да може да коригира всички неточности и да подобри качеството на данните.

5. Член 5, параграф 1, буква д) — ограничение на съхранението

Алгоритмите за машинно самообучение са предназначени да обработват големи количества информация и да установяват корелации, които позволяват на организациите да изготвят изключително всеобхватни и задълбочени профили на физически лица. Макар че запазването на данни може да предлага някои предимства в случай на профилиране, тъй като алгоритъмът ще разполага с повече данни за самообучение, при събирането на лични данни администраторите трябва да спазват принципа за свеждане на данните до минимум и да

гарантират, че периодите за запазване на тези лични данни не са по-дълги от необходимото и че са пропорционални на целите, за които се обработват личните данни.

В политиката на администратора за запазване на данни следва да се отчитат правата и свободите на физическите лица в съответствие с изискванията на член 5, параграф 1, буква д).

Администраторът също така следва да гарантира, че данните остават актуални през целия период на запазване, за да се намали рискът от неточности[11].

Б. Законосъобразни основания за обработване

Автоматизираното вземане на решения, определено в член 22, параграф 1, е позволено само ако се прилага едно от изключенията, посочени в глава IV (раздели В и Г). Следните законосъобразни основания за обработване са уместни за всички други случаи на автоматизирано вземане на индивидуални решения и профилиране.

1. Член 6, параграф 1, буква г) — съгласие

Съгласието като основание за обработване е разгледано в общ план в Насоките на РГ29 относно съгласието[12]. Изричното съгласие представлява едно от изключенията от забраната за автоматизирано вземане на решения и профилиране, посочена в член 22, параграф 1.

Възможно е профилирането да не е видимо. Често то зависи от данни, които се извличат или извеждат по дедуктивен път от други данни, а не от данни, предоставени пряко от субекта на данни.

Администраторите, които желаят да използват съгласието като основание за профилиране, ще трябва да демонстрират, че субектите на данни разбират с какво точно се съгласяват, и също така трябва да помнят, че съгласието невинаги представлява подходящо основание за обработване[13]. Във всички случаи субектите на данни следва да разполагат с достатъчна съответна информация относно предвиденото използване и последиците от обработването, за да се гарантира, че предоставеното от тях съгласие представлява информиран избор.

2. Член 6, параграф 1, буква б) — необходимо за изпълнението на договор

Администраторите може да желаят да използват процеси на профилиране и автоматизирано вземане на решения, защото те:

---

[11] Норвежки орган за защита на данните. The Great Data Race – How commercial utilisation of personal data challenges privacy (Голямата надпревара за данни — как използването на лични данни за търговски цели е в разрез с неприкосновеността на личния живот), доклад, ноември 2015 г. Datatilsynet https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/. Осъществен достъп на 24 април 2017 г.

[12] Работна група за защита на личните данни по член 29. Насоки относно съгласието в съответствие с Регламент 2016/679, WP 259, 28 ноември 2017 г., http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=53343. Осъществен достъп на 18 декември 2017 г.

[13] Пак там.

- потенциално позволяват по-голяма последователност или справедливост в процеса на вземане на решения (например като понижават потенциала за човешка грешка, дискриминация и злоупотреба с власт);
- намаляват риска клиентите да не успеят да посрещнат плащания за стоки или услуги (например чрез използване на услуги, свързани с оценка на кредитната история на клиенти); или
- позволяват на администраторите да вземат решения в по-кратък срок и подобряват ефикасността.

Независимо от горепосоченото, тези съображения сами по себе си не са достатъчни, за да се демонстрира, че този вид обработване е *необходимо* за изпълнението на договор съгласно член 6, параграф 1, буква б). Както е описано в становището на РГ29 относно законните интереси[14], необходимостта трябва да се тълкува в тесен смисъл.

Следва пример за профилиране, което *не* отговаря на основанието за профилиране по член 6, параграф 1, буква б).

Пример

Потребител закупува артикули от онлайн търговец на дребно. За да изпълни договора, търговецът на дребно трябва да обработи данните за кредитната карта на потребителя за целите на плащането и данните за адреса на потребителя, за да достави стоките. Изпълнението на договора не зависи от изготвянето на профил на предпочитанията и избора на потребителя във връзка с начина му на живот въз основа на посещенията му в уебсайта. Дори ако в дребния шрифт на договора изрично бъде посочено профилиране, сам по себе си този факт не го прави „необходимо“ за изпълнението на договора.

3. Член 6, параграф 1, буква в) — необходимо за спазването на законово задължение

Такъв може да бъде случаят, когато съществува законово задължение[15] за извършване на профилиране — например с цел предотвратяване на измами или на изпиране на пари. В становището на РГ29 относно законните интереси[16] се посочва полезна информация относно това основание за обработване, включително гаранциите, които трябва да се спазват.

4. Член 6, параграф 1, буква г) — необходимо, за да бъдат защитени жизненоважни интереси

Тук се обхващат ситуации, при които обработването е необходимо, за да се защити интерес от първостепенно значение за живота на субекта на данните или на друго физическо лице.

---

[14] Становище 06/2014 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО. Европейска комисия, 9 април 2014 г. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_bg.pdf. Осъществен достъп на 24 април 2017 г.

[15] Съображения 41 и 45 от ОРЗД.

[16] Стр. 19. Работна група за защита на личните данни по член 29. Становище 06/2014 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО. Европейска комисия, 9 април 2014 г. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_bg.pdf. Осъществен достъп на 24 април 2017 г.

Някои видове обработване могат да обслужват както важни области от обществен интерес, така и жизненоважните интереси на субекта на данните. Примерите за това могат да включват профилиране, което е необходимо за разработването на модели за прогнозиране на разпространението на животозастрашаващи болести или при спешни хуманитарни ситуации. При все това в тези случаи и по принцип администраторът може да използва основанието за жизненоважни интереси само ако не е налично друго правно основание за обработването[17]. Ако обработването включва специални категории лични данни, администраторът също така трябва да гарантира, че изпълнява изискванията на член 9, параграф 2, буква в).

5. Член 6, параграф 1, буква д) — необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия

При определени обстоятелства член 6, параграф 1, буква д) може да представлява подходящо основание за профилиране от публичния сектор. В законодателството трябва да се посочва ясно основание за съответната задача или функция.

6. Член 6, параграф 1, буква е) — необходимо за целите на легитимните интереси[18] на администратора или на трета страна

Профилирането е позволено, ако е необходимо за целите на легитимните интереси[19] на администратора или на трета страна. При все това член 6, параграф 1, буква е) не се прилага автоматично само защото е налице легитимен интерес на администратора или на трета страна. Администраторът трябва да извърши балансиране, за да оцени дали пред неговите интереси преимущество имат интересите или основните права и свободи на субекта на данните.

Следните аспекти са от особено значение:

- доколко е подробен профилът (дали се извършва профилиране на субекта на данни, при което той се поставя в кохорта с общо описание, например „хора, интересуващи се от английска литература“, или се извършва сегментиране и насочване към субекта на данни на по-подробно равнище);
- всеобхватността на профила (дали той описва само малка част от аспектите на субекта на данни или представя по-всеобхватна картина);
- въздействието от профилирането (последиците за субекта на данни); както и
- гаранциите, целящи да се осигури справедливост, недискриминация и точност в процеса на профилиране.

Макар че становището на РГ29 относно законните интереси[20] е основано на член 7 от Директива 95/46/ЕО за защита на данните (наричана по-нататък „Директивата“), то съдържа

---

[17] Съображение 46 от ОРЗД.

[18] Легитимните интереси, посочени в съображение 47 от ОРЗД, включват обработване за целите на директния маркетинг и обработване, строго необходимо за целите на предотвратяването на измами.

[19] „Легитимният интерес“ на администратора не може да направи профилирането законосъобразно, ако обработването попада в обхвата на определението, посочено в член 22, параграф 1.

[20] Работна група за защита на личните данни по член 29. Становище 06/2014 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО. Европейска комисия, 9 април 2014 г., стр. 47, примери на стр. 59 и 60 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_bg.pdf . Осъществен достъп на 24 април 2017 г.

примери, които продължават да бъдат полезни и подходящи за администраторите, които извършват профилиране. Освен това в него се изказва предположението, че за администраторите ще бъде трудно да обосноват използването на легитимните интереси като законосъобразно основание за практики на намеса, свързани с профилиране и проследяване за маркетингови или рекламни цели, например практики, които включват проследяване на физически лица в множество уебсайтове, местоположения, устройства, услуги или брокерска дейност с данни.

Администраторът също така следва да обмисли бъдещото използване или съчетаването на профили, когато оценява валидността на обработването съгласно член 6, параграф 1, буква е).

B. Член 9 — специални категории данни

Администраторите могат да обработват специални категории лични данни само ако изпълняват едно от условията, посочени в член 9, параграф 2, както и едно от условията в член 6. Това включва специални категории данни, извлечени или изведени по дедуктивен път чрез дейности за профилиране.

Профилирането може да създаде специални категории данни, като ги изведе по дедуктивен път от данни, които сами по себе си не представляват специални категории данни, но се превръщат в такива, когато бъдат съчетани с други данни. Например е възможно да се направят изводи за здравословното състояние на дадено лице от регистрираната информация за закупуваните от него храни в съчетание с данни относно качеството и енергийното съдържание на храните.

Могат да бъдат установени корелации, които водят до определени изводи за здравословното състояние на лицата, техните политически убеждения, религиозни вярвания или сексуална ориентация, както става видно от следния пример:

Пример

В едно проучване[21] харесванията във Facebook са съчетани с ограничена информация от анкети и е установено, че изследователите правилно прогнозират сексуалната ориентация на потребителите от мъжки пол в 88 % от случаите; етническия произход на потребителите в 95 % от случаите; и дали потребителят е християнин или мюсюлманин в 82 % от случаите.

Ако от профилирането се извличат чувствителни предпочитания и характеристики, администраторът следва да гарантира, че:

- обработването не е несъвместимо с първоначалната цел;
- е определил законосъобразно основание за обработването на специалните категории данни; както и
- е информирал субекта на данни относно обработването.

Автоматизираното вземане на решения съгласно член 22, параграф 1, което е основано на специални категории данни, е разгледано в глава IV (раздел Г).

21

Michael Kosinski, David Stilwell и Thore Graepel. Private traits and attributes are predictable from digital records of human behaviour (Персоналните черти и характеристики могат да бъдат предвидени от цифрови записи на поведението на хората). Материали на Националната академия на науките на Съединените американски щати, http://www.pnas.org/content/110/15/5802.full.pdf. Осъществен достъп на 29 март 2017 г.

Г. Права на субекта на данни[22]

С ОРЗД се въвеждат засилени права за субектите на данни и се създават нови задължения за администраторите.

В контекста на профилирането тези права позволяват предявяване на искове срещу администратора, който е създал профила, и срещу администратора, който е взел автоматизирано решение относно субект на данни (със или без човешка намеса), ако тези две образувания са различни.

Пример

Брокер на данни извършва профилиране на лични данни. В съответствие със своите задължения по членове 13 и 14 брокерът на данни следва да информира физическото лице относно обработването, включително дали възнамерява да сподели профила с други организации. Брокерът на данни също така представя отделно подробности относно правото на възражение съгласно член 21, параграф 1.

Брокерът на данни споделя профила с друго дружество. Дружеството използва профила, за да изпраща на това лице съобщения за целите на директния маркетинг.

Дружеството следва да информира лицето (член 14, параграф 1, буква в) относно целите, за които използва този профил, и относно източника, от който е получило данните (член 14, параграф 2, буква е). Дружеството също така трябва да информира субекта на данни относно неговото право да възрази срещу включващото профилиране обработване за целите на директния маркетинг (член 21, параграф 2).

Брокерът на данни и дружеството следва да осигурят на субекта на данни правото на достъп до използваната информация (член 15), правото да коригира погрешна информация (член 16) и в определени случаи правото на изтриване на профила или на използваните за създаването му лични данни (член 17). Субектът на данни също така следва да получи информация относно своя профил, например в какви „сегменти“ или „категории“ е поставен. [23]

Ако дружеството използва профила като част от процес за изцяло автоматизирано вземане на решения с правни последици или последици, които засягат по подобен начин субекта на данни в значителна степен, дружеството представлява администраторът, обхванат от разпоредбите на член 22. (Това не освобождава брокера на данни от прилагането на член 22, ако обработването отговаря на съответния праг).

[22] Настоящият раздел е от значение както за профилирането, така и за автоматизираното вземане на решения. По отношение на автоматизираното вземане на решения съгласно член 22 следва да се отбележи, че са въведени и допълнителни изисквания, описани в глава IV.

[23] Норвежки орган за защита на данните. The Great Data Race – How commercial utilisation of personal data challenges privacy (Голямата надпревара с данни — как използването на лични данни за търговски цели е в разрез с неприкосновеността на личния живот). Доклад, ноември 2015 г. https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/ Осъществен достъп на 24 април 2017 г.

1. Членове 13 и 14 — право на информиране

С оглед на основния принцип на прозрачност, залегнал в основата на ОРЗД, администраторите трябва да гарантират, че обясняват ясно и просто на физическите лица как се осъществява процесът на профилиране или автоматизирано вземане на решения.

По-специално когато обработването включва вземане на решения, основаващо на профилиране (независимо дали е обхванато от разпоредбите на член 22), на субекта на данни трябва да бъде посочен ясно фактът, че обработването е за целите както на а) профилирането, така и на б) вземането на решение въз основа на генерирания профил[24].

В съображение 60 също така се посочва, че предоставянето на информация относно профилирането е част от задълженията за прозрачност на администратора съгласно член 5, параграф 1, буква а). Субектът на данни има право *да бъде информиран* от администратора и при определени обстоятелства има право *да възрази срещу* „профилирането“, *независимо* дали се извършва изцяло автоматизирано вземане на индивидуални решения, основано на профилиране.

Допълнителни насоки относно прозрачността в общ план могат да бъдат намерени в Насоките на РГ29 относно прозрачността в съответствие с ОРЗД[25].

2. Член 15 — право на достъп

Член 15 дава на субекта на данни правото да получи подробности относно лични данни, които се използват за профилиране, включително категориите данни, които се използват за създаване на профил.

В допълнение към общата информация относно обработването, съгласно член 15, параграф 3 администраторът е длъжен да предостави данните, използвани за създаването на профила, както и да осигури достъп до информация относно профила и подробности в какви сегменти е поставен субектът на данни.

Това е различно от правото на преносимост на данните по член 20, съгласно което администраторът трябва да съобщи само данните, предоставени от субекта на данни или установени от администратора, но не и самия профил[26].

В съображение 63 се предвижда известна защита за администратори, опасяващи се да не разкрият търговски тайни или интелектуална собственост, което може да бъде от особено значение в контекста на профилирането. Съображението гласи, че правото на достъп „не следва да влияе неблагоприятно върху правата или свободите на други лица, включително върху

---

[24] Член 13, параграф 1, буква в) и член 14, параграф 1, буква в) от ОРЗД. Съгласно член 13, параграф 2, буква е) и член 14, параграф 2, буква ж) администраторът е длъжен да информира субекта на данни относно съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 22, параграфи 1 и 4. Това е обяснено по-подробно в глава IV.

[25] Работна група за защита на личните данни по член 29. Насоки относно прозрачността в съответствие с Регламент (ЕС) 2016/679, WP 260, 28 ноември 2017 г., http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, осъществен достъп на 18 декември 2017 г.

[26] Насоки на РГ29 относно правото на преносимост на данните, WP 242, стр. 9, http://ec.europa.eu/newsroom/document.cfm?doc_id=45685. Осъществен достъп на 8 януари 2018 г.

търговската тайна или интелектуалната собственост, и по-специално върху авторското право за защита на софтуера“. Администраторите обаче не могат да използват защитата на своите търговски тайни като оправдание за отказ на достъп или отказ за предоставяне на информация на субекта на данни.

В съображение 63 също така се посочва, че „когато е възможно, администраторът следва да може да предоставя достъп от разстояние до сигурна система, която да предоставя на субекта на данните пряк достъп до неговите лични данни“.

3. Член 16 — право на коригиране, член 17 — право на изтриване и член 18 — право на ограничаване на обработването

Профилирането може да включва елемент на прогнозиране, който повишава риска от неточности. Възможно е използваните данни да бъдат неточни или неподходящи, или пък да са извадени от техния контекст. Възможно е да има проблем с алгоритъма, който се използва за установяване на корелации.

Правото на коригиране по член 16 трябва да се прилага например когато физическо лице бъде поставено в категория, която показва нещо относно неговата способност да изпълни дадена задача, и този профил е основан на невярна информация. Физическите лица могат да поискат да оспорят точността на използваните данни и на всички групи или категории, в които са поставени.

Правата на коригиране и на изтриване[27] се прилагат както към „входните лични данни“ (личните данни, използвани за създаване на профила), така и към „изходните данни“ (самият профил или „точките“, което лицето е получило).

В член 16 също така се предвижда право за субекта на данни да допълва личните данни с допълнителна информация.

Пример

Компютърната система на местна клиника по хирургия поставя дадено лице в групата с най-голяма вероятност от сърдечни заболявания. Този „профил“ не е непременно неточен, дори лицето никога да не развие сърдечно заболяване.
Профилът просто посочва, че при него има *по-голяма вероятност* да се развие такова заболяване. Това може да е фактически вярно от статистическа гледна точка.

Независимо от това, като се отчита целта на обработването, субектът на данни има право да предостави допълнителна информация. В горепосочения сценарий тези допълнителна информация може да бъде основана например на по-усъвършенствана медицинска компютърна система (и статистически модел), като се отчетат допълнителни данни и се извърши по-подробен преглед в сравнение с извършения в местната клиника, която разполага с по-ограничени възможности.

Правото на ограничаване на обработването (член 18) се прилага към всеки етап от процеса на профилиране.

[27] Член 17 от ОРЗД.

4. Член 21 — право на възражение

Администраторът трябва *изрично* да предостави подробности относно правото на възражение съгласно член 21, параграфи 1 и 2 на вниманието на субекта на данни и да ги представи по ясен начин и отделно от всяка друга информация (член 21, параграф 4).

Съгласно член 21, параграф 1 субектът на данни може да възрази срещу обработването (включващо профилиране) на основания, свързани с неговата конкретна ситуация. Администраторите изрично са задължени да предвидят това право във всички случаи, в които обработването е основано на член 6, параграф 1, букви д) или е).

След като субектът на данни упражни това право, администраторът трябва да прекрати[28] (или да не започва) процеса по профилиране, освен ако може да докаже, че съществуват убедителни законови основания, които имат предимство пред интересите, правата и свободите на субекта на данни. Администраторът може също така да е длъжен да изтрие съответните лични данни[29].

В ОРЗД не се обяснява какво би могло да се счита за убедителни законови основания[30]. Възможно е например профилирането да бъде от полза за обществото като цяло (или за по-широката общност), а не само за стопанските интереси на администратора, например профилиране с цел предвиждане на разпространението на заразни болести.

Администраторът ще трябва:

- да отчете значението на профилирането за конкретната си цел;
- да отчете въздействието от профилирането върху интересите, правата и свободите на субекта на данни — то следва да бъде ограничено до необходимия минимум за постигане на целта; както и
- да извърши балансиране.

Винаги трябва да се извършва балансиране между конкуриращите се интереси на администратора и основанието за възражението на субекта на данни (което може да бъде по лични, социални, или професионални причини). За разлика от Директива 95/46/ЕО доказателствената тежест да се посочат убедителни законови основания се понася от администратора, а не от субекта на данни.

От текста на член 21 става ясно, че тестът за балансиране е различен от посочения в член 6, параграф 1, буква е). С други думи, не е достатъчно администраторът просто да демонстрира, че по-ранният му анализ на легитимните интереси е правилен. При този тест за балансиране легитимният интерес трябва да бъде *убедителен*, което предполага по-висок праг за предимство пред възраженията.

Член 21, параграф 2 осигурява *безусловно* право за субекта на данни да възрази срещу обработване на негови лични данни за целите на директния маркетинг, което включва и

---

[28] Член 18, параграф 1, буква г) от ОРЗД.

[29] Член 17, параграф 1, буква в) от ОРЗД.

[30] Вж. обяснението относно законосъобразността, Становище 06/2014 на работната група за защита на личните данни по член 29 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО, 9 април 2014 г., стр. 24—26, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_bg.pdf. Осъществен достъп на 24 април 2017 г.

профилиране, доколкото то е свързано с директния маркетинг[31]. Това означава, че не е необходимо да се балансират интереси; администраторът трябва да уважи желанията на лицето, без да поставя под въпрос причините за възражението. Съображение 70 осигурява допълнителен контекст за това право, като гласи, че то може да бъде упражнено безплатно и по всяко време.

IV. Специфични разпоредби, насочени към изцяло автоматизираното вземане на решения, определено в член 22

Член 22, параграф 1 гласи:

> Субектът на данните има право да не бъде обект на решение, *основаващо се единствено* на автоматизирано обработване, включващо профилиране, което поражда *правни последствия* за субекта на данните или *по подобен начин го засяга в значителна степен*.

Думата „право“ в разпоредбата не означава, че член 22, параграф 1 се прилага само когато субектът на данни изрично се позове на него. В член 22, параграф 1 се установява обща забрана за вземане на решения, основани единствено на автоматизирано обработване. Тази забрана се прилага независимо дали субектът на данни предприема действия във връзка с обработването на неговите лични данни.

Накратко, в член 22 се предвижда, че:

i) по принцип съществува обща забрана за напълно автоматизираното вземане на индивидуални решения, включващо профилиране, което поражда правни последици или последици, които засягат по подобен начин в значителна степен субекта на данните;
ii) съществуват изключения от това правило;
iii) когато се прилага едно от тези изключения, трябва да бъдат въведени мерки за защита на правата и свободите на субекта на данни, както и на легитимните му интереси[32].

С това тълкуване се укрепва идеята, че субектът на данни разполага с контрол върху своите лични данни, което е в съответствие с основните принципи на ОРЗД. Тълкуването на член 22 като забрана, а не като право, което може да бъде упражнено, означава, че лицата са защитени автоматично от потенциалните последици от този вид обработване. Текстът на този член подсказва, че намерението е именно такова, като се подкрепя и от съображение 71, което гласи:

> Въпреки това, вземането на решения въз основа на такова обработване, включително профилиране, **следва да бъде позволено**, когато е изрично разрешено от правото на Съюза или

[31] В съответствие с член 12, параграф 2 администраторите, които събират лични данни от физически лица с цел да ги използват за целите на директния маркетинг, следва в момента на събирането да обмислят дали да предложат на субектите на данни лесен начин да посочат, че не желаят техните лични данни да се използват за целите на директния маркетинг, вместо да изискват от тях да упражняват своето право на възражение на по-късен етап.

[32] В съображение 71 се посочва, че това обработване следва да „подлежи на подходящи гаранции, които следва да включват конкретна информация за субекта на данните и правото на човешка намеса, на изразяване на мнение, на получаване на обяснение за решението, взето в резултат на такава оценка, и на обжалване на решението“.

правото на държава членка [...], или когато е необходимо за сключването или изпълнението на договор [...], или когато субектът на данни е дал изричното си съгласие.

Това предполага, че обработването съгласно член 22, параграф 1 по принцип не е позволено[33].

При все това забраната в член 22, параграф 1 се прилага *само* в конкретни обстоятелства, когато решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, поражда правни последици за дадено лице или по подобен начин го засяга в значителна степен, както е обяснено допълнително в насоките. Определени са изключения, които позволяват извършването на такова обработване дори в тези случаи.

Изискваните предпазни мерки, които са разгледани по-подробно по-нататък, включват правото на информиране (посочено в членове 13 и 14 — по-специално съществена информация относно използваната логика, както и значението и предвидените последствия за субекта на данни) и гаранции, като например правото на човешка намеса и правото на обжалване на решението (посочени в член 22, параграф 3).

За всяко обработване, което има вероятност да породи висок риск за субектите на данни, администраторът е длъжен да извърши оценка на въздействието върху защитата на данните (ОВЗД).[34] Освен че в нея се разглеждат и всички други рискове, свързани с обработването, ОВЗД може да бъде особено полезна за администратори, които не са сигурни дали предложените от тях дейности ще попаднат в приложното поле на определението по член 22, параграф 1 и какви предпазни мерки трябва да бъдат предприети, ако дейностите бъдат позволени съгласно конкретно изключение.

A. „Решение, основаващо се единствено на автоматизирано обработване“

В член 22, параграф 1 се посочват решения, „основаващи се единствено“ на автоматизирано обработване. Това означава, че в процеса по вземане на решение няма човешка намеса.

Пример

Автоматизиран процес по същество води до препоръка по отношение на субект на данни. Ако човек прегледа и отчете и други фактори при вземането на окончателното решение, то няма да бъде „основано единствено“ на автоматизирано решение.

Администраторът не може да заобиколи разпоредбите на член 22, като изфабрикува човешка намеса. Например ако дадено лице рутинно прилага автоматично генерирани профили към физически лица, без това да оказва действително въздействие върху резултата, това пак ще представлява решение, основаващо се единствено върху автоматизирано обработване.

[33] Допълнителни коментари относно тълкуването на член 22 като забрана могат да бъдат намерени в приложение 2.

[34] Работна група за защита на личните данни по член 29. Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679, 4 април 2017 г. Европейска комисия. http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48464 Осъществен достъп на 24 април 2017 г.

За да е налице човешка намеса, администраторът трябва да гарантира, че надзорът по отношение на решението е реален, а не само символичен. Надзорът следва да се извършва от лице, което разполага с правомощия и е компетентно да промени решението. То следва да проучи всички съответни данни като част от анализа.

Като част от своята ОВЗД администраторът следва да определи и отбележи степента на човешка намеса в процеса по вземане на решения, както и етапите, на които се осъществява.

Б. „Правни“ последици или последици, които „засягат по подобен начин в значителна степен“ субекта на данните

В ОРЗД се признава, че автоматизираното вземане на решения, включващо профилиране, може да доведе до сериозни последици за физическите лица. Изразите „правен“ или „засяга по подобен начин в значителна степен“ не са определени в ОРЗД, но от текста става ясно, че член 22 обхваща само сериозни последици със значително въздействие.

„Решение, което поражда правни последици“

Правна последица означава, че решението, основаващо се единствено на автоматизирано обработване, засяга законовите права на дадено лице, например свободата на сдружаване с други лица, гласуване на избори или осъществяване на правни действия. Правна последица също така може да бъде последица, която засяга правния статут на дадено лице или неговите права съгласно договор. Примерите за такъв вид последици включват автоматизирани решения относно физическо лице, които водят до:

- анулиране на договор;
- придобиване на право или отказ на конкретно социално плащане, което се предоставя по закон, например детски надбавки или помощи за жилищно настаняване.
- отказ за приемане в държава или на получаване на гражданство.

„По подобен начин го засяга в значителна степен“

Дори процесът по вземане на решения да не оказва въздействие върху законовите права на хората, той пак може да попада в обхвата на член 22, ако поражда последици, които са равностойни като въздействие или по подобен начин ги засягат в значителна степен.

С други думи, докато когато няма промяна на законовите му права или задължения, субектът на данни пак може да бъде засегнат в достатъчна степен, за да се наложи защита съгласно тази разпоредба. В ОРЗД се въвежда изразът „по подобен начин“ (който не е посочен в член 15 от Директива 95/46/ЕО) към израза „засяга в значителна степен“. Поради това прагът за *значителност* трябва да бъде подобен на прага за решение, пораждащо правна последица.

Съображение 71 съдържа следните обичайни примери: „автоматичен отказ на онлайн искания за кредит“ или „електронни практики за набиране на персонал без човешка намеса“.

За да засяга обработването на данни дадено лице в значителна степен, последиците от обработването трябва да бъдат достатъчно сериозни или важни, за да заслужават да им се обърне внимание. С други думи, решението трябва да разполага с потенциал:

- да засегне в значителна степен положението, поведението или решенията на съответните лица;
- да окаже продължително или постоянно въздействие върху субекта на данни; или
- в най-тежкия случай да доведе до изключване или дискриминация на физически лица.

Трудно е да се прецизира какво точно би се счело за достатъчно *значително*, за да бъде обхванато от изискването, но следните решения биха могли да попаднат в тази категория:

- решения, които засягат финансовото положение на дадено лице, например допустимостта му да получи кредит;
- решения, които засягат достъпа на дадено лице до здравни услуги;
- решения, с които на дадено лице се отказва възможност за заетост или които поставят лицето в много неизгодна позиция;
- решения, които засягат достъпа на дадено лице до образование, например прием в университет.

Това ни отвежда до въпроса за рекламирането онлайн, което все по-често зависи от автоматизирани инструменти и включва изцяло автоматизирано вземане на индивидуални решения. В допълнение към спазването на общите разпоредби на ОРЗД, разгледани в глава III, от значение могат да бъдат и разпоредбите на предложението за Регламент за правото на неприкосновеност на личния живот и електронните съобщения. Освен това се изисква по-голяма защита за деца, както ще бъде обсъдено в глава V.

В много от обичайните случаи решението да се представи целенасочена реклама въз основа на профилиране няма да породи последици, които засягат лицата по подобен начин в значителна степен, например ако става въпрос за реклама за популярен онлайн магазин за модни артикули, основана на обикновен демографски профил: „жени в региона на Брюксел на възраст между 25 и 35 години, които има вероятност да се интересуват от мода и от определени облекла“.

При все това е възможно да се пораждат такива последици в зависимост от конкретните характеристики на случая, включително:

- степента на намеса при процеса на профилиране, включително проследяването на лица в различни уебсайтове, устройства и услуги;
- очакванията и желанията на въпросните лица;
- начина на поднасяне на рекламата; или
- използването на знания относно уязвимите места на съответните субекти на данни.

Обработване, което като цяло може да окаже ограничено въздействие върху физическите лица, по принцип може да окаже значително въздействие върху определени части от обществото, например малцинствени групи или уязвими пълнолетни лица. Например лице, за което е известно или вероятно да има финансови затруднения и към което редовно се отправят реклами за заеми с високи лихви, може да се повлияе от тези предложения и потенциално да натрупа още по-голям дълг.

Автоматизираното вземане на решения, което води до различно ценообразуване в зависимост от личните данни или характеристики, също би могло да породи значителни последици, например ако твърде високите цени на практика не позволяват на дадено лице да закупи определени стоки или услуги.

Последици, които засягат по подобен начин в значителна степен субекта на данните, също така могат да възникнат в резултат на действия на лица, различни от лицето, с което е свързано автоматизираното решение. По-долу е даден такъв пример.

Пример

Хипотетично дружество за кредитни карти може да намали лимита на кредитната карта на свой клиент не въз основа на конкретните му данни за погасяване на задължения, а на основата на нетрадиционни критерии за кредит, например анализ на други клиенти, които живеят в същия район и пазаруват в същите магазини.

В резултат на това е възможно някои лица да бъдат лишени от възможности въз основа на действията на други лица.

В различен контекст благодарение на използването на такива видове характеристики може да се отпусне кредит на лице без конвенционална кредитна история, което в противен случай би получило отказ.

B. Изключения от забраната

В член 22, параграф 1 се определя обща забрана за изцяло автоматизирано вземане на индивидуални решения с правни последици или последици, които засягат по подобен начин в значителна степен субекта на данните, както е описано по-горе.

Това означава, че администраторът следва да не извършва обработването, посочено в член 22, параграф 1, освен ако не се прилага едно от следните изключения по член 22, параграф 2 — когато решението:

а) е необходимо за сключването или изпълнението на договор;
б) е разрешено от правото на Съюза или правото на държава членка, което се прилага спрямо администратора и в което се предвиждат също подходящи мерки за защита на правата и свободите и легитимните интереси на субекта на данните; или
в) се основава на изричното съгласие на субекта на данни.

Когато вземането на решения включва специални категории данни, определени в член 9, параграф 1, администраторът също така трябва да гарантира, че изпълнява изискванията на член 22, параграф 4.

1. Изпълнение на договор

Възможно е администраторите да желаят да използват процеси на изцяло автоматизирано вземане на решения за договорни цели, защото считат, че това е най-подходящият начин за постигане на целта. Рутинната човешка намеса понякога може да бъде непрактична или невъзможна поради огромното количество на обработваните данни.

Администраторът трябва да бъде в състояние да демонстрира, че този вид обработване е необходимо, като отчете дали би могъл да се възприеме метод с по-малка намеса в неприкосновеността на личния живот. [35] Ако съществуват други ефективни средства с по-

[35] Buttarelli, Giovanni. Assessing the necessity of measures that limit the fundamental right to the protection of personal data. A Toolkit. (Оценка на необходимостта от мерки, които ограничават основното право на защита на личните данни. Набор от инструменти. Европейски надзорен орган по защита на данните, 11

малка намеса, с които може да се постигне същата цел, то обработването няма да бъде „необходимо“.

Автоматизираното вземане на решения, описано в член 22, параграф 1, може да бъде необходимо и за обработване преди сключването на договор.

Пример

Предприятие публикува обява за свободна длъжност. Тъй като работата във въпросното предприятие е популярна, то получава десетки хиляди заявления. Поради прекомерно големия обем на заявленията предприятието може да установи, че практически не е възможно да определи подходящи кандидати, без първо да използва напълно автоматизирани средства за пресяване на неподходящите заявления. В този случай може да е необходимо автоматизирано вземане на решения, за да се състави кратък списък с възможни кандидати с намерението да се сключи договор със субект на данни.

Глава III (раздел Б) съдържа повече информация относно договорите като законосъобразно основание за обработване.

2. Разрешено от правото на Съюза или правото на държава членка

Автоматизирано вземане на решения, включващо профилиране, потенциално би могло да се извършва съгласно член 22, параграф 2, буква б), ако използването му е разрешено от правото на Съюза или правото на държава членка. В съответното право също така трябва да са определени подходящи мерки за защита на правата и свободите, както и на легитимните интереси на субекта на данните.

В съображение 71 се посочва, че това би могло да включва използването на автоматизирано вземане на решения, както е определено в член 22, параграф 1, за наблюдение и предотвратяване на измами и укриването на данъци или за гарантиране на сигурността и надеждността на услугите, предоставяни от администратора.

3. Изрично съгласие

Съгласно член 22 се изисква *изрично* съгласие. Обработване, което попада в обхвата на определението по член 22, параграф 1, води до значителни рискове за защитата на данните и поради това се счита, че е подходящо високо равнище на индивидуален контрол върху личните данни.

Изразът „изрично съгласие“ не е определен в ОРЗД. Насоките на РГ29 относно съгласието[36] съдържат указания как следва да се тълкува той.

април 2017 г., https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf. Осъществен достъп на 24 април 2017 г.

[36] Работна група за защита на личните данни по член 29. Насоки относно съгласието в съответствие с Регламент 2016/679, WP 259. 28 ноември 2017 г., http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=53343. Осъществен достъп на 18 декември 2017 г.

Глава III (раздел Б) съдържа повече информация относно съгласието в общ план.

Г. Специални категории лични данни — член 22, параграф 4

Автоматизираното вземане на решения (описано в член 22, параграф 1), което включва специални категории лични данни, е позволено само при следните кумулативни условия (член 22, параграф 4):

- налице е приложимо изключение по член 22, параграф 2; както и
- прилага се член 9, параграф 2, букви а) или ж).

Член 9, параграф 2, буква а) — изрично съгласие на субекта на данни; или

Член 9, параграф 2, буква ж) — обработването е необходимо по причини от важен обществен интерес на основание правото на Съюза или правото на държава членка, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните.

И в двата горепосочени случая администраторът трябва да въведе подходящи мерки за защита на правата и свободите, както и на легитимните интереси на субекта на данните.

Д. Права на субекта на данни[37]

1. Член 13, параграф 2, буква е) и член 14, параграф 2, буква ж) — право на информиране

С оглед на потенциалните рискове и намесата, до които води обхванатото от член 22 профилиране по отношение на правата на субектите на данни, администраторите на данни следва да обърнат специално внимание на своите задължения за прозрачност.

Съгласно член 13, параграф 2, буква е) и член 14, параграф 2, буква ж) администраторите са длъжни да предоставят конкретна, лесно достъпна информация относно автоматизираното вземане на решения, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последици или по подобен начин засяга в значителна степен субекта на данните[38].

Ако администраторът взема автоматизирани решения, както е описано в член 22, параграф 1, той трябва:

- да уведоми субекта на данни, че извършва такъв вид дейност;
- да предостави съществена информация относно използваната логика; както и
- да обясни значението и предвидените последствия от обработването.

[37] В член 12 от ОРЗД са посочени приложимите условия за упражняване на правата на субекта на данни.

[38] Посочено в член 22, параграфи 1 и 4. Насоките на РГ относно прозрачността обхващат общите информационни изисквания, определени в членове 13 и 14.

Предоставянето на тази информация също така ще помогне на администраторите да гарантират, че изпълняват някои от изискваните гаранции, посочени в член 22, параграф 3 и съображение 71.

Дори ако автоматизираното вземане на решения и профилирането не отговарят на определението по член 22, параграф 1, предоставянето на горепосочената информация все пак представлява добра практика. Във всеки случай администраторът трябва да предостави достатъчно информация на субекта на данни, така че обработването да е добросъвестно[39], както и за да изпълни всички други изисквания за информация от членове 13 и 14.

Съществена информация относно „използваната логика“

С увеличаването и сложността на машинното самообучение може да бъде по-трудно да се разбере как функционира процесът на автоматизирано вземане на решения или профилирането.

Администраторът следва да намери опростени начини за информиране на субекта на данни относно логиката зад решението или критериите, използвани при достигането до него. Съгласно ОРЗД администраторът е длъжен да предостави съществена информация относно използваната логика, не непременно сложно обяснение на използваните алгоритми или разкриване на пълния алгоритъм[40]. Предоставената информация обаче следва да бъде достатъчно всеобхватна, за да може субектът на данни да разбере причините за решението.

Пример

Администратор използва точкова система за оценка на кредитоспособността, с която оценява и отхвърля искането за заем на физическо лице. Резултатът може да е предоставен от агенция за кредитна информация или да е изчислен директно въз основа на информация, с която разполага администраторът.

Независимо от източника (като информация относно източника трябва да бъде предоставена на субекта на данни съгласно член 14, параграф 2, буква е), когато личните данни не са получени от субекта на данни), ако администраторът използва този резултат, той трябва да бъде в състояние да обясни на субекта на данни резултата и логиката.

Администраторът обяснява, че този процес му помага да взема добросъвестни и отговорни решения относно отпускане на заеми. Той представя подробности относно основните характеристики, които са отчетени при достигането до решението, относно източника на тази информация и относно целесъобразността. Това може да включва например:

- информацията, предоставена от субекта на данни във формуляра за заявление;
- информация относно предишно поведение във връзка управление на банкови сметки,

[39] Съображение 60 от ОРЗД: „Администраторът следва да предостави на субекта на данните всяка допълнителна информация, която е необходима, за да се гарантира добросъвестно и прозрачно обработване на данните, като се вземат предвид конкретните обстоятелства и контекст, в които се обработват личните данни. Освен това субектът на данни следва да бъде информиран за извършването на профилиране и за последствията от това профилиране“.

[40] Сложността не може да се използва като оправдание да не се предостави информация на субекта на данни. В съображение 58 се посочва, че принципът на прозрачност „важи в особена степен за ситуации, където нарастването на участниците и технологичната сложност на тази практика правят трудно за субекта на данни да узнае и разбере дали се събират свързани с него лични данни, от кого и с каква цел, като в случая на онлайн рекламите“.

включително евентуални просрочени плащания; както и
- официална информация от публични регистри, например информация от регистри за извършени измами или регистри по несъстоятелност.

Администраторът също така включва информация, с която обяснява на субекта на данни, че използваните методи за оценка на кредитоспособността подлежат на редовни изпитвания, за да се гарантира, че продължават да бъдат справедливи, ефективни и безпристрастни. Администраторът предоставя данни за връзка, така че субектът на данни да може да поиска преразглеждане на решение за отказ в съответствие с разпоредбите на член 22, параграф 3.

„Значение“ и „предвидени последствия“

Тези изрази предполагат, че трябва да бъде предоставена информация относно планираното или бъдещо обработване и начина, по който автоматизираното вземане на решения може да засегне субекта на данни[41]. За да бъде тази информация съществена и разбираема, следва да бъдат представени реални конкретни примери за вида на възможните последици.

В цифров контекст е възможно администраторите да бъдат в състояние да използват допълнителни инструменти, които да им помогнат да илюстрират тези последици.

Пример

Застрахователно дружество използва процес на автоматизирано вземане на решения, за да определя премиите за автомобилни застраховки въз основа на наблюдение на поведението на клиентите при шофиране. За да илюстрира значението и предвидените последствия от обработването, то обяснява, че опасното шофиране може да доведе до по-големи застрахователни вноски, и предоставя приложение, в което се сравняват фиктивни водачи, включително водач с навици, които се свързват с опасно шофиране, например бързо ускоряване и спиране в последния момент.

В приложението се използват графики, за да се дадат полезни съвети как да се подобрят тези навици и съответно как да се намалят застрахователните премии.

Администраторите могат да използват подобни визуални техники, за да обяснят как е било взето дадено решение в миналото.

2. Член 15, параграф 1, буква з) — право на достъп

Член 15, параграф 1, буква з) дава право на субектите на данни да получават същата информация относно изцяло автоматизирано вземане на решения, включващо профилиране,

[41] Съвет на Европа. Проект на обяснителен доклад относно осъвременената версия на Конвенция № 108 на Съвета на Европа, точка 75: „Субектите на данни следва да имат право да знаят обосновката, залегнала в основата на обработването на техните данни, включително последствията от тази обосновка, които са довели до съответните заключения, по-специално в случаите, при които се използват алгоритми за автоматизирано вземане на решения, включващо профилиране. Например в случай на точкова система за оценка на кредитоспособността те следва да имат право да узнаят логиката, залегнала в основата на обработването на техните данни, която води до положително или отрицателно решение, а не само да получат информация относно самото решение. Без разбиране на тези елементи не може да бъде извършено ефективно упражняване на други важни гаранции, като например правото на възражение и правото за подаване на жалба пред компетентния орган“. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b6ec2. Осъществен достъп на 24 април 2017 г.

като информацията, която се изисква съгласно член 13, параграф 2, буква е) и член 14, параграф 2, буква ж), а именно:

- съществуването на автоматизирано вземане на решения, включващо профилиране;
- съществена информация относно използваната логика; както и
- значението и предвидените последствия от това обработване за субекта на данните.

Администраторът следва вече да е предоставил на субекта на данни тази информация в съответствие със своите задължения по член 13[42].

Член 15, параграф 1, буква з) гласи, че администраторът следва да предостави на субекта на данни информация относно *предвидените последствия* от обработването, а не обяснение на *конкретно* решение. В съображение 63 това се пояснява, като се посочва, че всеки субект на данни следва да има правото да получава „информация“, по-специално относно автоматизираното обработване на данни, включително използваната логика, и последствията от такова обработване, *най-малкото* когато се извършва на основата на профилиране.

Чрез упражняване на своите права по член 15 субектът на данни може да узнае за взето решение във връзка с него, включително решение, което е взето на основата на профилиране.

Администраторът следва да предостави на субекта на данни обща информация (по-специално относно отчетените фактори за процеса на вземане на решения, както и относно съответната им „тежест“ на общо ниво), която също така е полезна за субекта на данни с оглед на обжалването на решението.

Е. Установяване на подходящи гаранции

Ако основанието за обработването е член 22, параграф 2, буква а) или член 22, параграф 2, буква в), съгласно член 22, параграф 3 администраторите са длъжни да приложат подходящи мерки за защита на правата, свободите и легитимните интереси на субектите на данните. Съгласно член 22, параграф 2, буква б) правото на Съюза или правото на държава членка, с което се разрешава обработването, също така трябва да включва подходящи мерки за защита.

Тези мерки следва да включват като минимум начин, по който субектът на данни да упражни правото на човешка намеса, да изрази гледната си точка и да оспори решението.

Човешката намеса представлява ключов елемент. Всеки преглед трябва да се извършва от лице, което разполага с подходящи правомощия и е компетентно да промени решението. Проверителят следва да извърши задълбочена оценка на всички съответни данни, включително на допълнителна информация, предоставена от субекта на данни.

В съображение 71 се подчертава, че *във всеки случай* подходящите гаранции следва да включват също така:

> [...] конкретна информация за субекта на данните и правото [...] на получаване на обяснение за решението, взето в резултат на такава оценка, и на обжалване на решението.

Администраторът трябва да осигури лесен начин, по който субектът на данни да упражни тези права.

[42] В член 12, параграф 3 от ОРЗД се пояснява сроковете за предоставяне на тази информация.

Така се подчертава необходимостта от прозрачност във връзка с обработването. Субектът на данни ще бъде в състояние да обжалва дадено решение или да изрази гледната си точка само ако разбира напълно как е било взето то и на какво основание. Изискванията за прозрачност са разгледани в глава IV (раздел Д).

Грешки или пристрастност в събраните или споделени данни или в процеса на автоматизирано вземане на решения могат да доведат до:

- неправилно класифициране; както и
- оценки на основата на неточни прогнози; които
- повлияват неблагоприятно на физически лица.

Администраторите следва да извършват редовни оценки на обработваните от тях набори от данни, за да проверяват за случаи на пристрастност, както и да разработят начини за отстраняване на елементи на пристрастност, включително прекомерното разчитане на корелации.
Други полезни мерки включват системи за проверка на алгоритмите и редовни прегледи на точността и целесъобразността на автоматизираното вземане на решения, включващо профилиране.

Администраторите следва да въведат подходящи процедури и мерки за избягване на грешки, неточности[43] или дискриминация на основата на специални категории данни. Тези мерки следва да се използват циклично; не само на етапа на проектиране, а постоянно, тъй като профилирането се прилага към физически лица. Резултатът от това изпитване следва да се използва обратно в проектирането на системата.

Допълнителни примери за подходящи гаранции могат да бъдат намерени в раздела Препоръки.

V. Профилирането и децата

С ОРЗД се въвеждат допълнителни задължения за администраторите на данни, когато обработват личните данни на деца.

В самия член 22 не се прави разграничение дали обработването се отнася до възрастни или деца. В съображение 71 обаче се посочва, че изцяло автоматизираното вземане на решения, включващо профилиране, с правни последици или последици, които засягат по подобен начин в значителна степен, не следва да се прилага към деца[44]. Предвид факта, че тази формулировка не е отразена в самия член, РГ29 не счита, че това представлява абсолютна забрана за този вид обработване във връзка с деца. С оглед на това съображение обаче РГ29 препоръчва по правило администраторите да не разчитат на изключенията по член 22, параграф 2, за да обосноват такова обработване.

[43] Съображение 71 от ОРЗД гласи:
„С цел да се осигури добросъвестно и прозрачно обработване по отношение на субекта на данните, като се отчитат конкретните обстоятелства и контекстът, при които се обработват личните данни, администраторът следва да използва подходящи математически или статистически процедури за профилирането, да прилага съответните технически и организационни мерки, по-специално за да гарантира, че факторите, които водят до неточности в личните данни, се коригират, а рискът от грешки се свежда до минимум [...]“.

[44] Съображение 71 — „такава мярка не следва да се отнася до дете“.

Независимо от това е възможно да съществуват определени обстоятелства, при които на администраторите се налага да извършват изцяло автоматизирано вземане на решения, включващо профилиране, с правни последици или последици, които засягат по подобен начин в значителна степен деца, например с цел защита на тяхното благосъстояние. В такъв случай обработването може да бъде извършено въз основа на някое от изключенията в член 22, параграф 2, букви а), б) или в) по целесъобразност.

В тези случаи трябва да бъдат въведени подходящи гаранции, както се изисква съгласно член 22, параграф 2, буква б) и член 22, параграф 3, и те трябва да бъдат подходящи за деца. Администраторът трябва да гарантира, че тези гаранции осигуряват ефективна защита на правата, свободите и легитимните интереси на децата, чиито данни се обработват.

Необходимостта от специална защита за деца е отразена в съображение 38, което гласи:

> На децата се полага специална защита на личните данни, тъй като те не познават достатъчно добре съответните рискове, последици и гаранции, както и своите права, свързани с обработването на лични данни. Тази специална защита следва да се прилага по-специално за използването на лични данни на деца за целите *на маркетинга или за създаване на личностни или потребителски профили и събирането на лични данни по отношение на деца при ползване на услуги, предоставяни пряко на деца*.

Член 22 не възпрепятства администраторите да вземат изцяло автоматизирани решения във връзка с деца, ако решението не води до правни последици или до последици, които засягат детето по подобен начин в значителна степен. При все това изцяло автоматизираното вземане на решения, които влияят на избора и поведението на дете, потенциално биха могли да доведат до правни последици или до последици, които го засягат по подобен начин в значителна степен, в зависимост от естеството на въпросния избор и поведение.

Тъй като децата представляват по-уязвима група от обществото, като цяло организациите следва да се въздържат от профилирането на деца за целите на маркетинга[45]. Децата могат да бъдат особено податливи в онлайн средата и по-лесно да се повлияват от поведенчески реклами. Например в контекста на онлайн игрите може да се използва профилиране с цел насочване към играчи, които според алгоритъма има по-голяма вероятност да изразходват пари за играта, както и за осигуряване на по-персонализирани реклами. Възрастта и зрелостта на детето могат да повлияят на неговата способност да разбере мотивацията зад този вид маркетинг или последствията от него[46].

В член 40, параграф 2, буква ж) изрично се посочва изготвянето на кодекси за поведение, включващи закрилата на децата; освен това може да е налице възможност за доразвиване на съществуващи кодекси[47].

---

[45] На страница 26 от Становище 02/2013 на РГ29 относно софтуерните приложения за интелигентни устройства (WP 202), прието на 27 февруари 2013 г., в раздел 3.10 относно децата се посочва, че „администраторите на данни не трябва да обработват пряко или непряко данни на деца за целите на поведенческа реклама, тъй като подобна дейност надхвърля възможностите на децата за разбиране, а следователно и границите на законосъобразната обработка“.

[46] Проучване на ЕС относно въздействието на маркетинга посредством социални медии, онлайн игри и мобилни приложения върху поведението на децата установи, че маркетинговите практики оказват ясно изразено въздействие върху поведението на децата. Това проучване се отнася до деца на възраст между 6 и 12 години.

[47] Един пример за кодекс за поведение, насочен към маркетинга за деца, е кодексът (обяснителен меморандум) на Федерацията на европейските асоциации за директен маркетинг (FEDMA), достъпен на

VI. Оценки на въздействието върху защитата на данни (ОВЗД) и длъжностно лице по защита на данните (ДЛЗД)

Отчетността представлява важна част и е изрично изискване съгласно ОРЗД. [48]

В качеството си на основен инструмент за отчетност ОВЗД позволява на администратора да оцени рисковете при автоматизирано вземане на решения, включващо профилиране. Тя е начин да се покаже, че са въведени подходящи мерки за преодоляване на тези рискове и да се демонстрира спазване на ОРЗД.

В член 35, параграф 3, буква а) се подчертава необходимостта администраторът да извърши ОВЗД в случай на:

> *систематична и подробна оценка* на личните аспекти по отношение на физически лица, която се *базира* на автоматично обработване, *включително* профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице;

В член 35, параграф 3, буква а) се посочват оценки, включително профилиране, и решения, които се „базират“ на автоматично обработване, а не на „изцяло“ автоматизирано обработване. Считаме, че това означава, че член 35, параграф 3, буква а) ще се прилага в случай на вземане на решение, включващо профилиране с правни последици или последици, които засягат по подобен начин в значителна степен субекта на данните, което *не* е изцяло автоматизирано, както и изцяло автоматизирано вземане на решения, определено в член 22, параграф 1.

Ако администраторът предвижда „модел“, при който взема *изцяло* автоматизирани решения с *висока степен на въздействие* върху физически лица въз основа на *профили*, създадени във връзка с тях, и *не може* да разчита на съгласието на лицето, на договор с него или на закон, който позволява това, администраторът следва да не извършва такова обработване.

Администраторът пак може да предвиди „модел“ за вземане на решения, основан на профилиране, като значително увеличи степента на човешка намеса, така че моделът *вече да не е изцяло автоматизиран процес на вземане на решения*, макар че обработването пак би могло да поражда рискове за основните права и свободи на физическите лица. В такъв случай администраторът трябва да гарантира, че може да преодолее тези рискове и да изпълни изискванията, посочени в глава III от настоящите насоки.

ОВЗД също така може да представлява полезен начин, чрез който администраторът да определи какви мерки трябва да въведе, за да преодолее рисковете за защитата на данните, породени от обработването. Такива мерки[49] биха могли да включват:

адрес: http://www.oecd.org/sti/ieconomy/2091875.pdf. Осъществен достъп на 15 май 2017 г. Вж. по-специално: „6.2 Търговците, които се насочват към деца или за които децата има вероятност да представляват сегмент от целевата група, не следва да се възползват от доверието, лоялността, уязвимостта или липсата на опит на децата. 6.8.5 Търговците не следва да обвързват достъпа на дете до уебсайт със събирането на подробни лични данни. По-специално не следва да се използват специални стимули като предложения за награди и игри, за да се подмамват децата да разкрият подробни лични данни“.

[48] Съгласно изискванията на член 5, параграф 2 от ОРЗД.

- информиране на субекта на данни относно съществуването на процес на автоматизирано вземане на решения и използваната в него логика;
- обяснение на значението и предвидените последствия от обработването за субекта на данните;
- осигуряване на средства, чрез които субектът на данни може да възрази срещу решението; както и
- позволяване на субекта на данни да изрази своята гледна точка.

Възможно е и други дейности по профилиране да налагат извършването на ОВЗД в зависимост от специфичните характеристики на случая. Администраторите могат да пожелаят да направят справка с Насоките на РГ29 относно ОВЗД[50] за допълнителна информация и за помощ при определянето дали е необходимо да се извърши ОВЗД.

Допълнително изискване за отчетност е определянето на ДЛЗД, когато профилирането и/или автоматизираното вземане на решения представлява основна дейност на администратора и изисква редовно и систематично мащабно наблюдение на субекти на данни (член 37, параграф 1, буква б)[51].

[49] Изисквания, аналогични на изискванията в член 13, параграф 2, буква е), член 14, параграф 2, буква ж) и член 22, параграф 3.

[50] Работна група за защита на личните данни по член 29. Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679. 4 април 2017 г. http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48464 Осъществен достъп на 24 април 2017 г.

[51] Работна група за защита на личните данни по член 29. Насоки за длъжностните лица по защита на данните („ДЛЗД“). 5 април 2017 г. http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48137. Осъществен достъп на 22 януари 2018 г.

ПРИЛОЖЕНИЕ 1 — Препоръки за добри практики

Следните препоръки за добри практики ще подпомогнат администраторите на данни да изпълнят изискванията на разпоредбите на ОРЗД относно профилирането и автоматизираното вземане на решения[52].

Член	Аспект	Препоръка
Член 5, параграф 1, буква а), членове 12, 13, 14	Право на информиране	Администраторите следва да направят справка с Насоките на РГ29 относно прозрачността (WP 260) за общите изисквания за прозрачност. В допълнение към общите изисквания, когато администраторът обработва данни, попадащи в обхвата на определението по член 22, той трябва да представи съществена информация относно използваната логика. Вместо да представя сложно математическо обяснение как функционират алгоритмите или машинното самообучение, администраторът следва да обмисли как да използва ясни и разбираеми начини за предаване на информацията на субекта на данни, например: • категориите данни, които са били или ще бъдат използвани при профилирането или в процеса на вземане на решения; • защо тези категории се считат за уместни; • по какъв начин се изготвя даден профил, който се използва в процеса на автоматизирано вземане на решения,

[52] Администраторите също така трябва да гарантират, че са въвели надеждни процедури за гарантиране, че могат да изпълнят своите задължения съгласно членове 15—22 в сроковете, предвидени в ОРЗД.

		включително статистически данни, използвани в анализа; • защо този профил е от значение за процеса на автоматизирано вземане на решения; както и • по какъв начин се използва за решение, което засяга субекта на данни. Като цяло тази информация ще бъде от по-голямо значение за субекта на данни и ще допринесе за прозрачността на обработването. Администраторите може да обмислят използването на визуализация и интерактивни техники, за да се подпомогне прозрачността на алгоритъма[53].
Член 6, параграф 1, буква а)	Съгласие като основание за обработване	Ако администраторите използват съгласието като основание за обработване, те следва да направят справка с Насоките на РГ29 относно съгласието (WP 259).
Член 15	Право на достъп	Администраторите могат да обмислят въвеждането на механизъм, чрез който субектите на данни да проверяват своя профил, включително подробности относно информацията и източниците, използвани за създаването му.

[53] Служба на комисаря по информацията — „Big data, artificial intelligence, machine learning and data protection“ (Големи масиви от данни, изкуствен интелект, машинно самообучение и защита на данните), версия 2.0, март 2017 г. Стр. 87, точка 194, март 2017 г. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Осъществен достъп на 24 април 2017 г.

Член 16	Право на коригиране	Администраторите, които предоставят на субектите на данни достъп до техния профил във връзка с правата им по член 15, следва да им дадат възможност да актуализират или променят всички неточности в данните или профила. Това също така може да помогне на администраторите да изпълнят своите задължения по член 5, параграф 1, буква г). Администраторите биха могли да обмислят въвеждането на инструменти за управление на предпочитанията онлайн, като например панел във връзка с неприкосновеността на личния живот. Това осигурява на субектите на данни възможност да управляват случващото се с тяхната информация в рамките на редица различни услуги — като им позволява да променят настройките, да актуализират своите лични данни и да преглеждат или редактират своя профил с цел коригиране на неточности.
Член 21, параграфи 1 и 2	Право на възражение	Субектът на данни трябва изрично да се уведомява за съществуването на правото на възражение по член 21, параграфи 1 и 2, което трябва да му се представя по ясен начин и отделно от всяка друга информация (член 21, параграф 4). Администраторите трябва да гарантират, че информация за това право е поставена на видно място в техния уебсайт или в съответната документация и не е скрита между други условия.
Член 22 и съображение 71	Подходящи гаранции	Следният списък, макар и неизчерпателен, съдържа

		някои предложения за добри практики, които администраторите може да обмислят при вземането на изцяло автоматизирани решения, включващо профилиране (съгласно определението в член 22, параграф 1): • редовни проверки на качеството на техните системи, за да гарантират, че физическите лица се третират по справедлив начин и не се дискриминират, било то на основата на специални категории лични данни или по друг начин; • проверка на алгоритмите — изпитване на използваните алгоритми, разработени от системи за машинно самообучение, за да се докаже, че те действително функционират съгласно предвиденото и че не водят до дискриминационни, грешни или необосновани резултати; • за проверки от независими „трети страни“ (когато вземането на решения на основата на профилиране оказва висока степен на въздействие върху физическите лица) — да се предостави на проверителя цялата необходима информация за това как функционират

		алгоритъмът или системата за машинно самообучение; • получаване на договорни уверения по отношение на алгоритмите на трети страни, че са извършени проверки и изпитвания и че алгоритъмът отговаря на договорените стандарти; • специфични мерки за свеждане на данните до минимум, с които се въвеждат ясни периоди на запазване на профилите и на всички лични данни, които се използват при създаването или прилагането на профилите; • използване на техники за анонимизиране или псевдонимизиране в контекста на профилирането; • начини, които позволяват на субекта на данни да изрази своята гледна точка и да оспори решението; както и • механизъм за човешка намеса при определени случаи, например осигуряване на хиперлинк към процедура на обжалване при известяването на субекта на данни за автоматизираното решение, с договорени срокове за преглед и поименно посочено лице за връзка за евентуални запитвания. Администраторите също така

		могат да обмислят варианти като: • механизми за сертифициране на операциите по обработване на данни; • кодекси за поведение във връзка с проверката на процеси, включващи машинно самообучение; • комисии за етичен преглед, които да оценяват потенциалните вреди и ползи за обществото от конкретни приложения на профилирането.

ПРИЛОЖЕНИЕ 2 — Ключови разпоредби от ОРЗД

Ключови разпоредби от ОРЗД, в които се посочва общо профилиране и автоматизирано вземане на решения

Член	Съображение	Коментари
Член 3, параграф 2, буква б)	**Съображение 24**	Наблюдението на поведението на субектите на данни, доколкото това поведение се проявява в рамките на Съюза. **Съображение 24** „[...] се следят в интернет, [...] използване на техники за обработване на лични данни, които се състоят в профилиране на дадено физическо лице, *по-специално с цел да се вземат* отнасящи се до него *решения* или да се анализират или предвиждат неговите лични предпочитания, поведение и начин на мислене“.
Член 4, параграф 4	**Съображение 30**	Определение на профилиране в **член 4, параграф 4** **Съображение 30** „онлайн идентификатори, [...] като адресите по интернет протокол (IP адреси) или идентификаторите, наричани „бисквитки“, или други идентификатори, например етикетите за радиочестотна идентификация [...] може да бъдат оставени следи, които в съчетание по-специално с уникални идентификатори и с друга информация, получена от сървърите, *може да се използват за създаването на профили на физическите лица и за тяхното идентифициране*“.
Членове 5 и 6	**Съображение 72**	**Съображение 72**: „Профилирането се подчинява на правилата на настоящия регламент относно обработването на лични данни, например правните основания за обработването **(член 6)** или принципите за защитата на данни **(член 5)**.“
Член 8	**Съображение 38**	Използване на личните данни на деца за профилиране. **Съображение 38:** „На децата се полага специална защита [...] по-специално за използването на лични данни на деца за [...] създаване на личностни или потребителски профили“.
Членове 13 и 14	**Съображение 60**	Право на информиране. **Съображение 60**: „Освен това субектът на данни *следва да бъде информиран за извършването на профилиране и за последствията от това профилиране*.“
Член 15	**Съображение 63**	Право на достъп. **Съображение 63:** „[...] правото да е запознат и да получава информация [...] относно целите, за които се обработват личните данни [...] и последствията от такова обработване, *най-малкото* когато се извършва на основата на профилиране“.
Член 21, параграфи 1, 2 и 3	**Съображение 70**	Право на възражение срещу профилирането. **Съображение 70** „[...] право [...] да направи възражение срещу такова обработване, включително профилиране, доколкото то е свързано с директния маркетинг“.

Член 23	**Съобра жение 73**	**Съображение 73:** „Ограничения относно специални принципи и относно [...] правото на оспорване на решения, основани на профилиране [...], могат да бъдат налагани от правото на Съюза или от правото на държава членка, доколкото това е необходимо и пропорционално в едно демократично общество [...]“, за да се защитят специфични цели от общ обществен интерес.
Член 35, параграф 3, буква а)	**Съобра жение 91**	Изисква се ОВЗД в случай на „систематична и подробна оценка на личните аспекти по отношение на физически лица, която се *базира* на автоматично обработване, включително профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице“; **обхваща вземане на решения, включващо профилиране, което не е изцяло автоматизирано**.

Ключови разпоредби от ОРЗД, в които се посочва автоматизираното вземане на решения, определено в член 22

Член	Съображение	Коментари
Член 13, параграф 2, буква е) и **член 14, параграф 2, буква ж)**	**Съображение 61**	Право на информиране относно: • съществуването на автоматизирано вземане на решения съгласно **член 22, параграфи 1** и **4**; • съществена информация относно използваната логика; • значението и предвидените последствия от това обработване.
Член 15, буква з)		Специфични права на достъп до информация относно съществуването на изцяло автоматизирано вземане на решения, включващо профилиране.
Член 22, параграф 1	**Съображение 71**	Забрана за вземане на решения, основаващи се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последици/последици, които засягат по подобен начин в значителна степен субекта на данните. В допълнение към обяснението, посочено в основната част от насоките, в следните точки се описва по-обстойно логиката за тълкуването на член 22 като забрана: • Макар че глава III касае правата на субекта на данни, разпоредбите в членове 12—22 не се отнасят изключително до *активното* упражняване на права. Някои права са *пасивни*; не всички от тях са свързани със ситуации, в които субектът на данни предприема действие, т.е. подава молба, жалба или искане от някакъв вид. Членове 15—18 и членове 20—21 се отнасят до активното упражняване на права от страна на субекта на данни, докато членове 13 и 14 касаят задължения, които администраторът на данни трябва да изпълни без активно

		участие на субекта на данни. Поради това включването на член 22 в тази глава само по себе си не означава, че той дава право на възражение; • в член 12, параграф 2 се говори за „упражняването на правата на субекта на данните по членове 15—22“; но това не означава, че самият член 22, параграф 1 трябва да бъде тълкуван като право. В член 22 действително съществува активно право, но то е част от гаранциите, които трябва да се прилагат в случаите, когато се позволява автоматизирано вземане на решения (член 22, параграф 2, букви а)—в): правото на човешка намеса, на изразяване на гледната си точка и на оспорване на решението. То се прилага само в тези случаи, защото обработването, описано в член 22, параграф 1, е забранено да се извършва при други основания; • Член 22 се намира в раздела от ОРЗД, озаглавен „Право на възражение **и** автоматизирано вземане на индивидуални решения“, което предполага, че член 22 *не* се отнася до правото на възражение като член 21. Това се подчертава допълнително от факта, че в член 22 липсва също толкова изрично задължение за информиране като задължението в член 21, параграф 4; • Ако член 22 бъде тълкуван като право на възражение, изключението в член 22, параграф 2, буква в) не би имало смисъл. Изключението гласи, че автоматизирано вземане на решения все пак може да се извършва, ако субектът на данни е дал изрично съгласие (вж. по-долу). Така би настъпило противоречие, тъй като субектът на данни не може да възразява срещу и същевременно да дава съгласие за едно и също обработване; • Възражението би означавало, че трябва да бъде осъществена човешка намеса. Изключенията в член 22, параграф 2, букви а) и в) имат предимство пред член 22, параграф 1, но само при условие че субектът на данни разполага с възможност за човешка намеса, както е посочено в член 22, параграф 3. Тъй като (чрез своето възражение) субектът на данни вече е поискал да бъде осъществена човешка намеса, член 22, параграф 2, букви а) и в) автоматично ще се заобикалят във всеки случай и поради това от тях практически не би имало смисъл. **Съображение 71**: „[...] Това обработване включва „профилиране“, което се състои от всякакви форми на автоматизирано обработване на лични данни за оценка на личните аспекти във връзка с дадено физическо лице, по-специално анализирането или прогнозирането на различни аспекти, имащи отношение към резултатите в работата на субекта на данни, икономическото състояние, здравето, личните предпочитания или интереси, благонадеждността или поведението, местоположението или движенията [...]“. *„Такава мярка не следва да се отнася до дете*“.
Член 22,	**Съображение**	Съгласно **член 22, параграф 2** забраната за обработване се

параграф 2, букви а)—в)	**71**	отменя въз основа на **а)** изпълнението или сключването на договор, **б)** правото на Съюза или от правото на държава членка или **в)** изрично съгласие. **Съображение 71** осигурява допълнителен контекст за член **22, параграф 2, буква б)** и гласи, че обработването, посочено в **член 22, параграф 1:** „[...] следва да бъде позволено, когато е изрично разрешено от правото на Съюза или правото на държава членка, под чиято юрисдикция е администраторът, включително за целите на наблюдението и предотвратяването на измами и укриването на данъци, осъществявани в съответствие с разпоредбите, стандартите и препоръките на институциите на Съюза или националите надзорни органи, и за гарантиране на сигурността и надеждността на услугите, предоставяни от администратора [...]“.
Член 22, параграф 3	**Съображение 71**	В **член 22, параграф 3 и съображение 71** също така се посочва, че дори в случаите, посочени в **член 22, параграф 2, букви а)** и **в)** обработването следва да подлежи на подходящи гаранции. **Съображение 71:** „[...] които следва да включват конкретна информация за субекта на данните и правото на човешка намеса, на изразяване на мнение, на получаване на обяснение за решението, взето в резултат на такава оценка, и на обжалване на решението. Такава мярка не следва да се отнася до дете“.
Член 23	**Съображение 73**	**Съображение 73:** „Ограничения относно специални принципи и относно [...] правото на оспорване на решения, основани на профилиране [...], могат да бъдат налагани от правото на Съюза или от правото на държава членка, доколкото това е необходимо и пропорционално в едно демократично общество [...]“, за да се защитят специфични цели от общ обществен интерес.
Член 35, параграф 3, буква а)	**Съображение 91**	Изискване за извършване на ОВЗД.
Член 47, параграф 2, буква д)		В задължителните фирмени правила, посочени в **член 47, параграф 1**, следва да се уточнява най-малкото „[...] правото на субекта на данни да не бъде обект на решения, основани единствено на автоматизирано обработване, включително профилиране в съответствие с **член 22** [...]“.

ПРИЛОЖЕНИЕ 3 — Допълнителна информация

В настоящите насоки са взети предвид следните текстове:

- Консултативен документ на РГ29 относно основните елементи на определение и разпоредба относно профилирането в рамките на Общия регламент на ЕС относно защитата на данните, приет на 13 май 2013 г.;
- Становище 2/2010 на РГ29 относно поведенческите реклами онлайн, WP 171;
- Становище 03/2013 на РГ29 относно ограничението на целите, WP 203;
- Становище 06/2014 на РГ29 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО, WP 217
- Изявление на РГ29 относно ролята на основан на риска подход към правните рамки за защита на данните, WP 218;
- Становище 8/2014 на РГ29 относно последните разработки в сферата на интернет на нещата, WP 223;
- Насоки на РГ29 за длъжностните лица по защита на данните („ДЛЗД“), WP 243;
- Насоки на РГ29 за определяне на водещ надзорен орган на администратор или обработващ лични данни, WP 244;
- Насоки на РГ29 относно съгласието, WP 259
- Насоки на РГ29 относно прозрачността, WP 260
- Съвет на Европа. Препоръка CM/Rec(2010)13 относно защитата на лицата по отношение на автоматизираното обработване на лични данни в контекста на профилирането;
- Съвет на Европа. Насоки относно защитата на физически лица във връзка с обработването на лични данни в свят на големи масиви от данни, януари 2017 г.
- Служба на комисаря по информацията — „Big data, artificial intelligence, machine learning and data protection“ (Големи масиви от данни, изкуствен интелект, машинно самообучение и защита на данните), версия 2.0, март 2017.
- Служба на комисаря на Австралия — Consultation draft: Guide to big data and the Australian Privacy Principles“ (Проект за консултация: ръководство за големите информационни масиви и австралийските принципи за неприкосновеност на личния живот), май 2016 г.
- Становище 7/2015 на Европейския надзорен орган по защита на данните (ЕНОЗД) — Посрещане на предизвикателствата на големите масиви от данни, 19 ноември 2015 г.
- Datatilsynet – Big Data – privacy principles under pressure (Големи масиви от данни — подложени на натиск принципи за неприкосновеността на личния живот), ноември 2013 г.
- Съвет на Европа. Конвенция за защита на лицата при автоматизирана обработка на лични данни — Проект на обяснителен доклад относно осъвременената версия на Конвенция № 108 на Съвета на Европа, август 2016 г.
- Datatilsynet – The Great Data Race – How commercial utilisation of personal data challenges privacy (Голямата надпревара за данни — как използването на лични данни за търговски цели е в разрез с неприкосновеността на личния живот). Доклад, ноември 2015 г.
- Европейски надзорен орган по защита на данните — Оценка на необходимостта от мерки, които ограничават основното право на защита на личните данни: набор от инструменти
- Съвместен комитет на европейските надзорни органи. Joint Committee Discussion Paper on the use of Big Data by financial institutions (Документ за обсъждане на Съвместния комитет относно използването на големи масиви от данни от страна на финансовите институции), 2016-86. https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf.
- Commission de la protection de la vie privée. Big Data Rapport (Доклад за големите масиви от данни)

https://www.privacycommission.be/sites/privacycommission/files/documents/Big%20Data%20voor%20MindMap%2022-02-17%20fr.pdf.
- Сенат на Съединените американски щати, Комисия по търговия, наука и транспорт. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller (Преглед на сектора за брокерска дейност с данни: събиране, използване и продажба на потребителски данни за маркетингови цели, информативен доклад за председателя Рокфелер), 18 декември 2013 г. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf
- Lilian Edwards & Michael Veale. Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for (Роб на алгоритъма? Защо „правото на обяснение" вероятно не е решението, което търсиш). Научно изследване, публикувано на 24 май 2017 г. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855
- NYTimes.com. Showing the Algorithms behind New York City Services (Показване на алгоритмите зад услугите на Ню Йорк). https://mobile.nytimes.com/2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city-services.html?referer=https://t.co/6uUVVjOIXx?amp=1. Осъществен достъп на 24 август 2017 г.
- Съвет на Европа. Препоръка CM/REC(2018)x на Комитета на министрите към държавите членки относно насоки за насърчаване, защита и упражняване на правата на децата в цифровата среда (преработен проект, 25 юли 2017 г.). https://www.coe.int/en/web/children/-/call-for-consultation-guidelines-for-member-states-to-promote-protect-and-fulfil-children-s-rights-in-the-digital-environment?inheritRedirect=true&redirect=%2Fen%2Fweb%2Fchildren. Осъществен достъп на 31 август 2017 г.
- УНИЦЕФ. Privacy, protection of personal information and reputation rights. Discussion paper series: Children's Rights and Business in a Digital World (Неприкосновеност на личния живот, право на защита на личните данни и на репутацията. Поредица от документи за обсъждане: правата на децата и бизнесът в цифровия свят). https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf. Осъществен достъп на 31 август 2017 г.
- Камара на лордовете. Growing up with the internet (Да израснеш с интернет). Специална комисия по съобщенията, втори доклад от сесиите в периода 2016—2017 г. https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm. Осъществен достъп на 31 август 2017 г.
- Sandra Wachter, Brent Mittelstadt и Luciano Floridi. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation (Защо правото на обяснение за автоматизираното вземане на решения не съществува в Общия регламент относно защитата на данните), 28 декември 2016 г. https://www.turing.ac.uk/research_projects/data-ethics-group-deg/. Осъществен достъп на 13 декември 2017 г.
- Sandra Wachter, Brent Mittelstadt и Chris Russell. Counterfactual explanations Without Opening the Black Box: Automated Decisions and the GDPR (Съпоставителни обяснения без отваряне на черната кутия: автоматизирани решения и ОРЗД), 6 октомври 2017 г. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289. Осъществен достъп на 13 декември 2017 г.
- Правителство на Австралия. Better Practice Guide, Automated Assistance in Administrative Decision-Making (Ръководство за по-добри практики, автоматизирано подпомагане при вземането на административни решения). Методология от шест стъпки плюс обобщение на точки по списък. Седма част, февруари 2007 г. https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf. Осъществен достъп на 9 януари 2018 г.