

EUROPEAN DATA PROTECTION SUPERVISOR

Становище 4/2015

Към нова етика в областта на цифровите технологии

Данни, достойнство и технологии



EDPS

11 септември 2015 г.

Европейският надзорен орган по защита на данните (ЕНОЗД) е независима институция на ЕС, чиято задача съгласно член 41, параграф 2 от Регламент (ЕО) № 45/2001 „По отношение на обработката на лични данни ... е да гарантира спазването от страна на институциите и органите на Общността на основните права и свободи на физическите лица, и по-специално правото им на личен живот“ и която отговаря „за предоставянето на консултации на институциите и органите на Общността и субектите на данни по всички въпроси, свързани с обработката на лични данни“. Той е назначен през декември 2014 г. заедно с помощник надзорния орган със специалната задача да бъде по-конструктивен и по-проактивен. През март 2015 г. ЕНОЗД публикува петгодишна стратегия, в която посочва как възнамерява да изпълни тази задача и да поеме отговорност за това.

Настоящото становище е следствие от предходното становище на ЕНОЗД във връзка с общия регламент относно защитата на данните, който има за цел да подпомогне основните институции на ЕС за постигането на консенсус по отношение на работни, насочени към бъдещето правила в подкрепа на индивидуалните права и свободи. Подобно на становището относно мобилното здравеопазване от началото на 2015 г. в него се разглеждат произтичащите от „цифровизацията“ трудности за защитата на личните данни — третата задача в стратегията на ЕНОЗД — „приспособяване на съществуващите принципи на защита на данните към глобалната цифрова среда“, също така в контекста на плановете на ЕС за цифровия единен пазар. Становището следва подхода на работната група по член 29 относно свързаните със защитата на данни аспекти на използването на нови технологии, например „интернет на предметите“, за които ЕНОЗД има принос като пълноправен член на групата.



Dignity	Достойнство
Future-oriented rules and enforcement	Насочени към бъдещето правила и изпълнение
Accountable controllers	Отговорни администратори на лични данни
Empowered individuals	Оправомощени физически лица
Innovative privacy engineering	Новаторски инженеринг, зачитащ неприкосновеността на личния живот
Ethics	Етика

„Човешкото достойнство е неприкосновено. То трябва да се зачита и защитава.“

Член 1, Харта на основните права на ЕС

Основните права на неприкосновеност на личния живот и на защита на личните данни повече от всякога имат значение за защитата на човешкото достойнство. Те са гарантирани в Договорите за ЕС и в Хартата на основните права на ЕС. Позволяват на лицата да развиват собствена индивидуалност, да водят независим живот, да въвеждат новости и да упражняват други права и свободи. Принципите на защита на данните, определени в Хартата на ЕС — необходимост, пропорционалност, добросъвестност, минимизиране на данните, ограничаване на целите, съгласие и прозрачност — се прилагат по отношение на обработването на данни в цялост — както при събирането, така и при използването им.

Технологиите не трябва да налагат ценности и права, но в същото време връзката с тях не трябва да се свежда до погрешно противопоставяне. Революцията в областта на цифровите технологии обещава ползи за здравето, околната среда, международното развитие и икономическата ефективност. Съгласно плановете на ЕС за цифров единен пазар компютърните услуги „в облак“, „интернет на предметите“, големите информационни масиви и други технологии се считат за изключително важни за конкурентоспособността и растежа. В бизнес моделите се разработват нови възможности за мащабно събиране, незабавно предаване, комбиниране и повторно използване на лични данни за непредвидени цели, обосновани с дългосрочни и недостъпни политики за защита на личните данни. Това поставя принципите за защита на данните пред нови изпитания, които налагат да се преосмисли тяхното прилагане.

В днешната цифрова среда придържането към закона не е достатъчно; трябва да се отчете етичното измерение на обработването на данните. Нормативната рамка на ЕС вече дава възможност за гъвкави решения и гаранции в зависимост от отделния случай при боравене с лична информация. Реформирането на нормативната рамка ще бъде добра стъпка напред. Съществуват обаче по-сериозни въпроси за влиянието на тенденциите върху достойнството, личната свобода и функционирането на демокрацията в зависимо от данните общество.

Тези проблеми имат технически, философски, правни и морални последици. Настоящото становище изтъква някои основни технологични тенденции, които могат да включват неприемливо обработване на лична информация или да нарушават правото на неприкосновеност на личния живот. То очертава „екосистема за защита на големите информационни масиви“ на четири нива, която да отговори на цифровото предизвикателство: колективно усилие, подплатено със съображения от етично естество.

- (1) Ориентиран към бъдещето регламент относно обработването на данни и зачитането на право на неприкосновеност на личния живот и на защита на данните.
- (2) Отговорни администратори, които определят обработването на лична информация.
- (3) Зачитащ неприкосновеността на личния живот инженеринг и дизайн на продукти и услуги за обработване на данни.
- (4) Оправомощени физически лица.

Европейският надзорен орган по защита на данните желае да насърчи открита и информирана дискусия в ЕС и извън него с участието на гражданското общество, дизайнери, дружества, представителите на академичните среди, публични органи и регулатори. Новият етичен съвет на ЕС в областта на защитата на данните, който ще създадем към ЕНОЗД, ще помогне за определянето на нова етика в областта на цифровите технологии, посредством която по-добре ще бъдат осъзнати ползите от технологиите за обществото и икономиката по начин, който укрепва правата и свободите на гражданите.

СЪДЪРЖАНИЕ

1. Данни навсякъде: тенденции, възможности и предизвикателства	7
1.1 ГОЛЕМИ ИНФОРМАЦИОННИ МАСИВИ	7
1.2 „ИНТЕРНЕТ НА ПРЕДМЕТИТЕ“	8
1.3 ЗАОБИКАЛЯЩИ КОМПЮТЪРНИ ИЗЧИСЛЕНИЯ	9
1.4 КОМПЮТЪРНИ УСЛУГИ „В ОБЛАК“	9
1.5 ЗАВИСИМИ ОТ ЛИЧНИ ДАННИ БИЗНЕС МОДЕЛИ	9
1.6 БЕЗПИЛОТНИ ЛЕТАТЕЛНИ СРЕДСТВА И АВТОНОМНИ ПРЕВОЗНИ СРЕДСТВА	10
1.7 ТЕНДЕНЦИИ С ПОТЕНЦИАЛНО ПО-ГОЛЯМО И ДЪЛГОСРОЧНО ВЪЗДЕЙСТВИЕ.....	10
2. Голяма екосистема за защита на личните данни.....	11
2.1 ОРИЕНТИРАН КЪМ БЪДЕЩЕТО РЕГЛАМЕНТ.....	11
2.2 ОТГОВОРНИ АДМИНИСТРАТОРИ НА ЛИЧНИ ДАННИ.....	12
2.3 ИЖЕНЕРИНГ, ЗАЧИТАЩ НЕПРИКОСНОВЕНОСТТА НА ЛИЧНИЯ ЖИВОТ	13
2.4 ОПРАВОВОЩЕНИ ФИЗИЧЕСКИ ЛИЦА.....	13
<i>Среда на „произвеждащи потребители“</i>	<i>13</i>
<i>Съгласие.....</i>	<i>14</i>
<i>Контрол и „собственост“ върху данните</i>	<i>14</i>
3. Достойнството в центъра на нова цифрова етика	15
3.1 ДОСТОЙНСТВО И ДАННИ	15
3.2 ЕВРОПЕЙСКИ КОНСУЛТАТИВЕН СЪВЕТ ПО ЕТИКА	17
4. Заключение: време е да задълбочим обсъждането	17
Бележки	19

1. Данни навсякъде: тенденции, възможности и предизвикателства

Все по-големи количества лични данни се събират и обработват по все по-неясни и сложни начини. С постъпателното внедряване на компютрите в предприятията и държавните администрации през 80-те години на 20 в. се разпространи и широкото схващане, че практиките на силните правителства и корпорации при обработването на лични данни свеждат хората само до субекти на данни, като застрашават основни права и свободи. Това, което отличава настоящата вълна интегрирани информационни и съобщителни технологии, е тяхната повсеместност и мощ.

Миналата година бе съобщено, че на планетата има повече свързани устройства, отколкото хора¹. Все по-мощните процесори², по-голямото пространство за съхранение и по-високата скорост на пренос означават, че пред обработването на лични данни стоят все по-малко технически ограничения. Очаква се „интернет на предметите“ и средствата за анализ на големи информационни масиви да се слеят с изкуствения интелект, компютърното обработване на естествени езици и биометричните системи с цел разработване на приложения със способност за машинно самообучение, които да дават усъвършенствана информация. Правителствата и компаниите могат да преминат от „извличане на данни“ към „извличане на информация от действителността“, което прониква в ежедневието, общуването и дори мисълта³. В процеса на приспособяване на обществото към изискванията на цифровия пазар се възобновяват усилията за преподаване на програмиране на децата от ранна възраст⁴. Овладяването на тези тенденции в сектор, в който ЕС е водещ потребител, но изостава в предоставянето на услуги, е повтаряща се тема в стратегията на Комисията за цифровия единен пазар⁵.

Въпреки своята актуалност тези тенденции и много от понятията, които се използват днес, са с неясно и припокриващо се значение. За да спомогнем за стимулиране на дебат, искаме да открийм конкретни тенденции, които макар и очевидно неизчерпателни, според нас повдигат най-важните етични и практически въпроси пред прилагането на принципите за защита на данните.

1.1 Големи информационни масиви

Понятието „големи информационни масиви“⁶ се отнася до практиката на съчетаване на огромни обеми информация от разнообразни източници и нейното анализиране, при което често се използват алгоритми за самообучение с цел информиране на решения. Тази информация не винаги представлява лични данни: данните, получени от датчици, които следят природни или атмосферни явления, като метеорологичните условия или замърсяването, или технически аспекти на производствени процеси, не са свързани с „идентифицирано или подлежащо на идентификация лице“⁷. Един от най-ценните аспекти на големите информационни масиви за фирмите и правителствата обаче произтича от следенето на *човешкото* поведение, колективно и индивидуално, и се състои в потенциала му за прогнозиране⁸.

Едно от следствията е появата на модел за генериране на приходи за интернет компании, които разчитат на проследяването на активността онлайн, за да оптимизират икономическата стойност на сделките за доставчиците на услуги не само при насоченото рекламиране, но и при условията и ставките на застрахователни полици, кредити и други договорни отношения. На конкурентния пазар, в който всеки се бори за вниманието на потребителите, повечето хора не осъзнават мащаба на това

проследяване⁹. Тези „големи информационни масиви“ следва да се считат за лични данни дори когато са използвани способи за анонимизиране: става все по-лесно да се открие самоличността на дадено лице посредством комбиниране на данни, за които се твърди, че са „анонимни“, с данни от други масиви, в това число публично достъпна информация, например в социалните мрежи¹⁰. Когато се търгува с данни, особено през граници и юрисдикции, отчетността за обработването на информацията става неясна и трудна за установяване или налагане съгласно правото в областта на защитата на данните, по-специално предвид отсъствието на каквито и да било международни стандарти.

1.2 „Интернет на предметите“

Много свързани с интернет устройства вече са широко разпространени, като смартфоните, таблетите, банкоматите и гишетата за електронно чекиране за полети. Предвижда се, че до 2020 г. свързаността ще бъде нещо стандартно с 25 милиарда свързани предмета (в сравнение с 4,8 милиарда през 2015 г.) — от телемедицинските услуги до превозните средства и от интелигентните измервателни уреди до цяла гама нови стационарни и мобилни устройства за създаване на интелигентни градове¹¹.

Тези датчици ще предоставят незабавна и подробна информация, до която съвременните статистически служби и проучвания нямат достъп, но която не е непременно по-точна и дори може да бъде потенциално подвеждаща¹². Прогнозираните до 2022 г. 1,8 милиарда автомобилни връзки от типа „машина с машина“ биха могли да намалят пътнотранспортните произшествия и замърсяването, да повишат производителността и независимостта на хората в напреднала възраст или с увреждания¹³. Вещите, които носим по себе си, като дрехи и часовници, ще обработват лични данни подобно на други свързани устройства. Те ще могат да засичат съсиреци и да следят за физическата форма и заздравяването на травми; свързаните материали биха могли да осигуряват защита при екстремни заобикалящи условия, например при пожарогасене. Тези устройства ще качват лични данни директно в облака, ще имат връзка със социалните мрежи и потенциално ще излъчват информация публично, като ще позволяват определяне на самоличността на потребителите и проследяване на поведението и движенията на отделни лица и групи от хора¹⁴.

Начинът, по който се борави с тази информация, би могъл да засегне не само неприкосновеността на личния живот на потребителите на устройствата, в това число използваните на работното място, но и правата на други лица, които са наблюдавани или записвани от тези устройства. Макар доказателствата за действителна дискриминация да са ограничени, е ясно, че огромният обем лични данни, събирани от „интернет на предметите“, представлява голям интерес като средство за постигане на максимални приходи чрез по-персонализирано ценообразуване според проследеното поведение, особено в сектора на здравното осигуряване¹⁵. Други специфични за отделни сфери правила също ще бъдат оспорени, например ако устройствата, участващи в обработването на данни за здравословното състояние, не се категоризират формално като медицински изделия и попаднат извън приложното поле на правната уредба¹⁶.

1.3 Заобикалящи компютърни изчисления

Заобикалящите или невидимите компютърни изчисления представляват съществена технология, която стои в основата на „интернет на предметите“. Едни от най-видимите ѝ приложения са „интелигентните домове“ и „интелигентните офиси“, които се състоят от устройства с вградени усъвършенствани способности за обработка на информация, които обещават по-висока енергийна ефективност и по-добре информирани хора, които могат да влияят върху потреблението си дистанционно (макар че това зависи от степента, до която трябва да се съобразяват с наемодателя или домоуправителя на сградата, в която живеят). Трябва да е ясно кой отговаря за предназначението и средствата за обработка на личните данни, които участват в приложенията за заобикалящи компютърни изчисления, не само с цел защита на основните права на лицата, но и надлежно разпределение на отговорността за гарантиране на спазването на изискванията за цялостна сигурност на системата.

1.4 Компютърни услуги „в облак“

Компютърните услуги „в облак“ са познати като централна способстваща технология за усъвършенстваните способности за анализ и извличане на данни, събирането и анализа на големи информационни масиви и огромния приток на данни от „интернет на предметите“, която понастоящем се използва от около една пета от гражданите и предприятията в ЕС¹⁷. Тя позволява съсредоточаването на данни от многобройните устройства, включени в „интернет на предметите“, и разчита на наличието и свързаността на огромни обеми данни в мащабни съоръжения за съхранение и обработка по целия свят¹⁸. Очаква се по-широкото възприемане на компютърните услуги „в облак“¹⁹ от частния и публичния сектор потенциално да доведе до добавяне на общо 449 млрд. евро към БВП на ЕС 28 (0,71 % от общия БВП на ЕС).

Контролът върху личните данни често се споделя между клиента и доставчика на услугата „в облак“, а отговорността за поемането на задължение за защитата им не винаги е ясна. Това може да означава, че на практика не се предоставя достатъчна защита. Тези задължения не са обвързани с **физическото местоположение на съхраняваните данни. Освен това** макар да е само фонова технология, която поддържа бизнес приложенията, инфраструктурата на компютърните услуги „в облак“ сама по себе си може да стане критична и да увеличи неравенството в пазарната мощ, като 30 % от предприятията неотдавна споделиха, че изпитват трудности при прекратяване на абонамента или промяна на доставчиците²⁰.

1.5 Зависими от лични данни бизнес модели

Тези технологии способстваха за появата на нови бизнес модели, които разчитат на информация, генерирана не само от предоставянето на услуги, но и от други източници, като присъствие в социалните мрежи, за да оценяват риска и кредитоспособността и да постигат максимални приходи. Един открояващ се бизнес модел днес е представен от платформи, които свързват продавачи и купувачи, като способстват за споделянето и преразпределението на продукти, услуги, умения и активи. Често наричани „икономика на споделянето“, „съвместно потребление“ или онлайн и мобилни бизнес платформи от типа „peer-to-peer“ („равен с равен“),²¹ тези платформи могат да предложат класическа икономическа ефективност, да повишат конкурентоспособността на пазарите и да намалят загубите. Прогнозите са, че през следващите няколко години стойността им в световен мащаб ще се увеличи четворно

от 26 на 110 милиарда щатски долара²². Такива водени от данните бизнес модели вече генерират огромни приходи в области като общо ползване на автомобили на разменни начала и наеми на жилища, както и във финансовите технологии и социалното кредитиране. Проучванията показват, че потребителите оценяват привидно по-голямата им ценова достъпност и удобство²³.

Валутата на тези платформи обикновено са потребителската репутация, отзивите от други хора и потвърждаването на самоличността. Това потенциално може да се разглежда като повишаване на прозрачността и отчетността, но не непременно по отношение на самия доставчик на платформата. Крупните участници на тези пазари са критикувани с твърдения, че укриват данни за репутацията от самите индивидуални потребители, за които се отнасят. Тук се крие огромният риск тези лица да бъдат изключени от услуги въз основа на репутация, която се гради на неточни данни, които те не могат да оспорят или да поискат да бъдат заличени. Ослабянето на данни от множество източници също поставя под въпрос принципа на правото на ЕС за свеждане на данните до минимум. Степента на бъдещото въздействие на тези и по-нататъшни способствани от технологиите бизнес модели върху хората и обществото заслужава внимателно обмисляне²⁴.

1.6 Безпилотни летателни средства и автономни превозни средства

Безпилотните или полуавтономни летателни средства понастоящем се използват основно за военни цели, но все повече започват да служат за наблюдение, картографиране, транспорт, логистика и обезпечаване на обществената сигурност, като овладяване на горски пожари²⁵. Снимки, видеоклипове и други лични данни, събрани от безпилотните летателни средства, могат да се обменят посредством далекосъобщителните мрежи. Използването им носи със себе си рискове от сериозна намеса в личния живот и смразяващ ефект върху свободата на изразяване на мнение. Възниква въпросът как дизайнът и употребата им могат да се регламентират реално, така че субектите на данни да могат да упражняват правата си на достъп до уловените от тези машини данни.

По суша автономните превозни средства или автомобилите без водач ще променят начина, по който се използва и организира индивидуалното пътуване, и може да размият границата между частен и обществен транспорт. Прогнозите са, че до 2035 г. ще има 12 милиона напълно автономни и 18 милиона частично автономни превозни средства, като Европа ще е една от първите възприели тези технологии²⁶. Управляващите автомобили алгоритми ще вземат решения, които може да имат пряко въздействие върху физическата цялост и дори живота или смъртта на хората, например при избора, който е програмиран в случай на неизбежен сблъсък. В допълнение към очевидната нужда да се изясни кой носи отговорност и ще бъде държан отговорен за контрола и сигурността на данните, тези приложения повдигат редица етични въпроси.

1.7 Тенденции с потенциално по-голямо и дългосрочно въздействие

Счита се, че **триизмерният биопечат** на органични тъкани и органи, при който се използват възпроизведени клетки на пациента и „биологичен бинт“ от колаген (т.е. чувствителни данни съгласно правото на ЕС), за да се полагат поредни пластове живи клетки, скоро ще бъде широко достъпен²⁷. Тази технология би улеснила доставянето на персонализирани човешки анатомични части и би била особено ценна в по-бедните и

преживели конфликт райони на света. Биопечатът повдига очевидни въпроси за медицинската етика, опазването на интелектуалната собственост и защитата на потребителите, но и тези за прилагането на правилата за защита на личните данни, тъй като технологията разчита на обработката на интимни и чувствителни данни, свързани със здравето на хората.

Изкуственият интелект, като при роботите, се отнася до технологично изискване за стационарни и мобилни автономни машини. Напредъкът им ще предложи огромни възможности извън настоящото им приложение. Дълбочинно обучаващите се компютри усвояват задачи, като изчисляват големи масиви от данни, използвайки наред с другото нервни системи, които привидно имитират човешкия мозък. Академичните среди и компаниите се стремят да усъвършенстват самостоятелното учене. Вече съществуват алгоритми, които разбират езици и превеждат на тях, разпознават изображения, пишат новинарски статии и анализират медицински данни²⁸. Социалните мрежи са богат източник на лични данни, които са пояснени удобно от самите им субекти. Това може би е най-новото помощно средство в услуга на човешката памет наред с хартията или металото или се внедрява в автономни машини и роботи, но сега е моментът да се замислим за по-широките последици за хората и обществото²⁹.

2. Голяма екосистема за защита на личните данни

Сега ЕС има възможността да застане начело, като демонстрира как правителствата, регулаторните органи, администраторите на лични данни, дизайнерите, програмистите и обикновените хора могат по-добре да действат заедно, за да укрепят правата и да направляват, а не да блокират технологичните иновации. Описаните във втория раздел тенденции според един коментатор са „разширили пропастта между възможното и законното“³⁰. Противно на някои твърдения, неприкосновеността на личния живот и защитата на данните са платформа, а не пречка за устойчива и динамична цифрова среда. Независимите органи за защита на данните като ЕНОЗД играят основна роля за разсейване на тези митове и реагиране на реалните тревоги на гражданите във връзка със загубата на контрол над личните им данни³¹.

Съществува вероятност следващото поколение лични данни да са още по-недостъпни за субектите им. Отговорността за формиране на устойчив цифров единен пазар по необходимост е разпръсната, но и взаимозависима подобно на екосистема, която изисква ефективно взаимодействие между програмисти, предприятия и регулаторни органи в интерес на отделния гражданин. В този раздел очертаваме приноса, който всеки от тези четирима основни участника може да има.

2.1 Ориентиран към бъдещето регламент

Неотдавна призовахме ЕС да се възползва от историческата си възможност да въведе по-опростени правила за боравене с лични данни, които да останат актуални в продължение на едно поколение³². Преговорите по Общия регламент относно защитата на данните и Директивата за защита на данните в полицейския и съдебния сектор са навлезли в крайните си етапи и скоро вниманието ще се обърне към бъдещето на Директивата за правото на неприкосновеност на личния живот и електронните комуникации и новия регламент относно начина, по който самите институции и органи на ЕС обработват лични данни. Тъй като икономическите разходи за събиране и съхранение на данни са почти пренебрежими, органите за защита на данните ще са

онези, които трябва да налагат последователно тези правила, за да се избегне „моралната опасност“ от прекомерно обработване на данни³³.

В Стратегията за цифровия единен пазар се признава връзката между контрола върху големи обеми от данни и пазарната мощ. В нея се споделя убеждението, изразено в предварителното ни становище от 2014 г. относно защитата на личния живот и конкуренцията в ерата на огромното количество данни, а именно, че е необходима по-голяма последователност сред регулаторните органи. ЕС вече разполага с инструментите за коригиране на дисбаланса на силите в цифровия пазар: текущите производства на Европейската комисия срещу нарушения в областта на конкуренцията например са признание за преобладаващото използване на мобилни устройства за достъп до интернет. В рамките на съществуващата правна уредба е възможно по-всеобхватно налагане на изискванията, например посредством клирингов механизъм на ЕС, чрез който надзорните органи могат да преценят дали отделни случаи могат да повдигнат въпроси, свързани с нормативното съответствие спрямо правилата за конкуренция, защита на потребителите и на личните данни. Например:

- Изискване за по-голяма прозрачност на цената на дадена услуга, било то в парично или друго изражение, може да информира и да улесни анализа на производства в областта на конкуренцията³⁴.
- Засичане на нелоялна ценова дискриминация въз основа на лошото качество на данните и нелоялното профилиране и корелации³⁵.

По-тесният диалог между регулаторните органи от различни сектори би могъл да отговори на все по-силните призови за световни партньорства, които могат да създадат „общи ресурси“ от свободно достъпни данни, където информацията и идеите, като статистически данни и карти, ще могат да текат и да са налични и обменяни в полза на обществения интерес при по-малък риск от следене, за да може хората да имат по-голямо влияние върху решенията, които ги засягат³⁶.

2.2 Отговорни администратори на лични данни

Отчетността изисква въвеждане на вътрешни правила и системи за контрол, които гарантират спазване на изискванията и предоставят относими доказателства, по-специално на независимите надзорни органи.

Настоявали сме за елиминиране на бюрокрацията в правото в областта на защитата на личните данни посредством свеждане до минимум на изискванията за ненужна документация, така че да се даде максимално пространство за по-отговорни инициативи от страна на предприятията, подкрепяни от насоки от органите за защита на данните. Принципът, че личните данни следва да се обработват само по начин, съвместим с конкретното предназначение или съответно предназначения, за които са събрани, е от основно значение за зачитането на легитимните очаквания на гражданите. Стабилно доверие в цифровия пазар може да се изгради например с помощта на кодекси за поведение, одити, сертифициране и ново поколение договорни клаузи и задължителни фирмени правила. Лицата, отговарящи за боравенето с лични данни, следва да са много по-динамични и проактивни и да загърбят склонността към т.нар. „черна кутия“, а именно тенденцията към потайност и неяснота на фирмените практики, съчетана с все по-високи изисквания за прозрачност към клиентите³⁷.

2.3 **Инженеринг, зачитащ неприкосновеността на личния живот**

Човешките иновации винаги са били продукт на дейностите на конкретни обществени групи и специфичен контекст, който обикновено отразява обществените норми на епохата³⁸. Решенията при проектирането на технологиите обаче не бива да диктуват социалните ни взаимоотношения и структурата на обществата ни, а по-скоро следва да подкрепят ценностите и основните ни права.

ЕС следва да разработи и популяризира инженерни способности и методи, които позволяват внедряване на технологиите за обработка на данни при пълно зачитане на достойнството и правата на всеки човек. Системните и софтуерните инженери трябва да разбират и да прилагат по-добре принципите на неприкосновеност на личния живот още при проектирането на нови продукти и услуги — на всяка фаза от него и при всички технологии. Отчетността трябва да бъде подкрепена от повече научноизследователска и развойна дейност в сферата на методите и средствата за гарантиране на точни одити и за определяне на нормативното съответствие на администраторите на лични данни и обработващите лица спрямо правилата, например всяка единица лични данни се маркира с метаданни, които описват изискванията за защита.

Инженерните решения следва да оправомощават онези, които искат да запазят неприкосновеността на личния си живот и свободата си чрез независимост. ЕС следва да насърчава проектирането и внедряването на алгоритми, които скриват самоличността и обобщават данните, за да защитят субектите на данни и същевременно да овладеят мощната прогнозираща способност на данните³⁹.

Още днес трябва да положим основите за изпълнение на тези задачи, като съберем програмисти и експерти по защита на данните от различни сфери в широки мрежи, като Инженерната мрежа за неприкосновеността на личния живот в интернет (IPEN), които допринасят за ползотворния интердисциплинарен обмен на идеи и подходи.

2.4 **Оправомощени физически лица**

Среда на „произвеждащи потребители“

Хората не са просто пасивни обекти, които имат нужда законът да ги защитава от експлоатация. Гореописаните цифрови тенденции предоставят положителни възможности за укрепване на ролята на индивида. В наши дни например хората не само потребяват, но и произвеждат съдържание и услуги, и все повече могат да се считат за солидарно отговорни заедно с доставчиците на услуги за обработката на лични данни, освен ако ползването не е изцяло в хода на „домашни занимания“⁴⁰ (понятието „произвеждащ потребител“ се появява, за да опише това развитие⁴¹). Същевременно виртуалните валути предлагат на потребителите анонимност и избягване на необходимостта от потвърждаване на трансакциите от трета страна, а оттам и по-ниски разходи, свързани с трансграничните плащания за стоки и услуги. От друга страна, анонимността и трансграничното (или някои твърдят *безграничното*, попадащо под никаква юрисдикция) естество на тези виртуални валути излагат хората на опасност от измами и престъпни пазари, които се откриват и разследват трудно. В допълнение към задълженията на регулаторните органи, предприятията и инженерите, гражданите също носят отговорност да са съзнателни, внимателни, критични и осведомени, когато правят избор, независимо дали е онлайн, или офлайн⁴².

Съгласие

Освен това, противно на традиционното схващане, не всяко човешко поведение може да се обясни с икономическите принципи, според които хората са изцяло рационални и реагират на икономически стимули⁴³. Това е свързано с бъдещата роля на съгласието от страна на индивида за обработка на личните му данни. По смисъла на правото на ЕС съгласието не е единственото правно основание в повечето случаи на обработка на данни. Макар да играе важна роля, то не освобождава администраторите на лични данни от отговорността им за това, което правят с тях, особено в случаите, в които е получено генерално съгласие за обработка на данни за широк набор от предназначения.

Контрол и „собственост“ върху данните

Субектите на данните трябва да са в състояние да оспорват грешки и несправедливи предубеждения, възникнали вследствие от използваната в алгоритмите логика за определяне на допускания и предвиждания. При проучване на почти 3 000 кредитни досиета на 1 000 потребители в САЩ например е установено, че в 26 процента от тях има „съществени“ грешки, които са достатъчно сериозни, за да променят оценката за кредитоспособност на потребителите, а оттам и себестойността на отпуснатия кредит⁴⁴.

Често данните, подобно на петрола, се определят като ресурс, който може да се търгува в идеалния случай между еднакво информирани страни по сделката⁴⁵. Клиентите не получават справедливо възнаграждение за личните си данни, които са обект на търговия, и се появяват доводи в полза на модел за собственост върху данните. Абсолютен контрол върху личните данни обаче се гарантира трудно — ще се намесят и други съображения, като общественият интерес и правата и свободите на други лица. Контролът е необходимо, но не и достатъчно условие⁴⁶. Човешкото достойнство обаче винаги е константа и съгласно правото на ЕС аналогията със собствеността не може да се приложи в този си вид към личните данни, които са неразривно свързани с конкретната личност. В правото на ЕС в областта на защитата на личните данни няма разпоредба, която да позволява на индивида да се откаже от това свое основно право.

Алтернативен метод за предоставяне на по-силен контрол в ръцете на индивидите върху собствените им данни, т.е. контрол да определят кой да има достъп до тях и за какви цели, би могъл да е използването на т.нар. хранилища или „трезори“ за лични данни⁴⁷. Понятието за такива „лични хранилища“ изисква механизми за сигурност, които да гарантират, че само упълномощените от субекта на данни лица имат достъп до тях или до частта от тях, за която имат разрешение. Хранилищата на лични данни биха били най-ефективни за съхранение на текуща и постоянно актуализираща се информация, като географско-пространствени данни или жизнени показатели. Освен техническите предпазни механизми, потребителите на данни ще бъдат задължени да спазват и правилата за споделяне и използване на данните. Конкуренцията и възможността за смяна на ползваната услуга остават най-ефективното средство за влияние от страна на потребителя върху пазара на услуги, които му се предлагат. Осигуряването на възможност за преносимост на връзките, в това число идентификатори и контакти, се доказва като мощен стимул за конкуренцията и доведе до действително намаляване на потребителските цени вследствие на либерализирането на пазара на далекосъобщителни услуги. Преносимостта на данните, т.е. действителната и практическа възможност за прехвърляне на повечето собствени

данни от един към друг доставчик на услуги, е ефективна отправна точка за създаване на условия за реален избор на потребителите.

3. Достойнството в центъра на нова цифрова етика

В основата на градивните елементи на тази цифрова екосистема трябва да стои етична рамка. ЕНОЗД счита, че по-доброто зачитане и опазване на човешкото достойнство би могло да послужи като противотежест на всепроникващото наблюдение и асиметрията на силите, пред която индивидът е изправен понастоящем. То трябва да е в центъра на нова цифрова етика.

3.1 Достойнство и данни

След индустриалната революция от 18-ти и 19-ти век движението за правата на човека си поставя за цел да осигури по-всеобхватно обществено благо, като намали пречките пред уважението към индивида. С приемането на Хартата на основните права и следвайки Всеобщата декларация за правата на човека и Европейската конвенция за правата на човека, ЕС задава ненакърнимостта на човешкото достойнство като своя отправна точка. Достойнството на човешката личност е не само основно право само по себе си, но представлява фундамент на допълнителни права и свободи, в това число правата на неприкосновеност на личния живот и на защита на личните данни⁴⁸. Накърняването на достойнството може да включва предметяване, при което личността са третира като средство, служещо за постигането на нечия цел⁴⁹. Неприкосновеността на личния живот е неразделна част от човешкото достойнство, а правото на защита на личните данни първоначално е било формулирано през 70-те и 80-те години на 20 в. като начин за компенсиране на евентуалното накърняване на неприкосновеността на личния живот и достойнството посредством мащабна обработка на лични данни. В Германия правото на „информационно самоопределяне“ се основава на правата на лично достойнство и свободно развитие на личността, предвидени в членове 1 и 2 от Конституцията на страната⁵⁰.

През 21 в. обаче от хората се изисква все повече да разкриват много по-голямо количество лични данни по интернет, за да участват в обществени, административни и търговски дела, с все по-ограничени възможности за отказ от такова разкриване. При всички дейности, които потенциално се осъществяват винаги онлайн, понятието за свободно и информирано съгласие е поставено под огромен натиск. „Трохи“ от цифрови данни се разпръскват ежеминутно и се събират с цел категоризиране на индивидите в реално време и създаване на множество, понякога взаимно отричащи се профили. Тези профили могат да се разпространят за микросекунди без знанието на индивидите и да се използват като основа за важни решения, които ги засягат.

Профилите, които се използват за прогнозиране на човешкото поведение, крият риск от стигматизиране, засилване на съществуващи стереотипи, социална и културна сегрегация и изключване⁵¹, като подобен род „колективна информация“ подкопава индивидуалния избор и равните възможности. Подобни „филтрирани балони“ или „лични ехокамери“ биха могли в крайна сметка да задушат самия творчески дух, новаторството, свободата на изразяване на мнение и свободата на сдруженията, които способстваха за разцвета на цифровите технологии.

Същевременно съображението за опазване на сигурността, като постоянно изключение, се използва като оправдание за наслояване на множество накърняващи

неприкосновеността на личния живот способи за наблюдение на действията на индивидите⁵². Проумяването на тази „ескалация на наблюдението“ изисква по-дългосрочна перспектива върху цялостните последици за обществото и поведението.

Съвместно с трети държави ЕС трябва да се занимае сериозно с въпроса как да гарантира, че тези ценности ще се зачитат в действителност, а не само на хартия, и че няма на практика да станат нищожни в киберпространството. Специално ЕС в момента разполага с „критично важен прозорец от време“ преди масовото възприемане на тези технологии, за да внедри в цифровите структури онези ценности, които ще определят обществото ни в бъдеще⁵³. Това изисква нова оценка на въпроса дали потенциалните ползи от новите технологии непременно зависят от събирането и анализа на разкриващи самоличността данни на милиарди хора. Подобна оценка би могла да отправи предизвикателство към програмистите да проектират продукти, които деперсонализират в реално време огромни обеми неорганизирана информация, като така става по-трудно или невъзможно да се разкрие самоличността на конкретен човек.

Вече признаваме, че определени видове обработване на данни, например генетични, не само трябва да бъдат регламентирани в правната уредба, но и да станат обект на оценка с оглед на по-всеобхватни обществени съображения, която да се осъществява например от етични комисии. По своето естество генетичните данни са свързани не само с определен индивид, а и с неговите предци и поколение. Този вид данни служат не само за откриване на родствена връзка — елементи от гените на един индивид могат да дадат информация и за неговите родители и деца и да подтикнат администраторите на лични данни да вземат решения, които влияят върху шансовете им в живота, преди дори да са се родили. Потенциалното струпуване на генетични лични данни в ръцете на няколко гигантски пазарни участника има последици за пазарните икономики и за самите субекти на данните. Нарастващата зависимост от световна система за събиране и анализ на непрестанен поток от данни би могла да направи обществото и икономиката по-уязвими на безпрецедентни дефекти в сигурността и злонамерени атаки.

Съществуващата уредба би могла да претърпи крах, ако не подходим към бъдещето с новаторско мислене. Налице е все по-силно изискване и потребност субектът на данните да се разглежда като човешко същество, а не просто като клиент или потребител. Реално независимите органи за защита на данните играят съществена роля за предотвратяване на бъдеще, в което личностите се определят от алгоритми и техните непрестанни вариации. Те трябва да бъдат снабдени с нужното за упражняване на задължението си да се грижат за хората и тяхното достойнство онлайн. Традиционните понятия и принципи за неприкосновеност на личния живот и защита на личните данни от самото начало съдържат етични нюанси, свързани с опазването на достойнството, като заетост и здравеопазване. Съвременните тенденции обаче отвориха изцяло нова глава и трябва да се проучи въпросът дали принципите са достатъчно стабилни, за да издържат на цифровата ера⁵⁴. Вероятно самото понятие „лични данни“ ще претърпи коренна промяна, тъй като технологиите все повече позволяват да се „реконституира“ самоличността на хората от данни, за които се твърди, че са анонимни. Освен това способността за самообучение на машините и сливането на човешкия и изкуствения интелект ще подкопаят понятията за права и отговорности на индивида.

3.2 Европейски консултативен съвет по етика

Целта ни не е да обрисваме тревожна антиутопична картина. Вече се провеждат обсъждания в правните, политическите, икономическите, социалните, научните и дори религиозните среди⁵⁵. Вероятно опростенческите подходи, които дават едностранно предимство на икономическата печалба или на наблюдението с цел опазване на сигурността, са също толкова безполезни, колкото и прекомерно ограничителното прилагане на съществуващите закони, които задушават новаторството и прогреса. В тази връзка ЕНОЗД предлага да се направи подробен, широк и мултидисциплинарен анализ, за да се дадат препоръки и да се информира общественият дебат по въпроса как едно свободно и демократично общество следва да посрещне технологичното предизвикателство.

В Стратегията на ЕНОЗД⁵⁶ се поема ангажимент за разработване на етичен подход към защитата на данните и се признава, че „постижимостта, полезността или рентабилността не се равняват на устойчивост“, като се подчертава, че „отчетността е по-важна от механичното спазване на буквата на закона“. Възнамеряваме да се обърнем не само към общността на официалните представители на ЕС, юристите и специалистите по информационни технологии, но и към видни личности, които са способни да преценят средносрочните и дългосрочните последици от технологичната промяна и регулаторната реакция спрямо нея. През следващите няколко месеца нашата независима институция ще формира външна консултативна група по етичното измерение на защитата на личните данни, която да изследва отношенията между правата на човека, технологиите, пазарите и бизнес моделите на 21 в.

Нашият консултативен съвет по етика ще се състои от подбрана група изявени личности в областта на етиката и философията, социологията, психологията, технологиите и икономиката, които ще бъдат подпомагани според потребностите от познания и експертни становища в сфери, като здравеопазването, транспорта и енергетиката, социалното взаимодействие и медиите, икономиката и финансите, управлението и демокрацията, сигурността и реда. Членовете на съвета ще бъдат приканени при максимална прозрачност на обсъжданията да разгледат по-широките етични аспекти на генерирането и използването на лични данни.

4. Заключение: време е да задълбочим обсъждането

Неприкосновеността на личния живот и защитата на данните са част от решението, а не проблемът. Засега технологиите се контролират от хората. Не е лесно тези потенциални развития да се класифицират само като добри или лоши, желателни или вредни, полезни или пагубни, още по-малкото, когато трябва да се вземат предвид редица потенциални тенденции. Авторите на политики, разработчиците на технологии, предприемачите и всички ние трябва сериозно да помислим дали и как искаме да въздействаме върху развитието на технологиите и тяхното приложение. Също толкова важно е обаче ЕС спешно да разгледа етиката и мястото на човешкото достойнство в технологиите на бъдещето.

Принципите на защита на данните се оказаха годни да защитят гражданите и личния им живот от рисковете на безотговорното обработване на данни. Съвременните тенденции обаче може да изискват изцяло нов подход. Затова повдигаме нова дискусия, а именно доколко прилагането на принципи като добросъвестност и легитимност е достатъчно. Общността на работещите в областта на защитата на

данните може да изпълнява нова роля, като използва съществуващи инструменти като предварителни проверки и разрешения — тъй като няма други органи, подготвени за подробно изследване на такава обработка на данни. В обстановката, в която технологиите, глобалните иновации и свързаността между хората се развиват с главоломна скорост, ние имаме възможност да привлечем внимание, да събудим интерес и да постигнем консенсус.

С настоящото становище се надяваме да дадем рамка за по-широко и по-задълбочено обсъждане как ЕС може да гарантира неприкосновеността на своите ценности и същевременно да се възползва от новите технологии.

Съставено в Брюксел на 11 септември 2015 г.

(подпис)

Giovanni BUTTARELLI

Европейски надзорен орган по защита на данните

Бележки

¹ Източник: GSMA Intelligence.

² Законът на Мур, който гласи, че броят на транзисторите, които могат да се поставят върху един микрочип, се удвоява приблизително на всеки 18 месеца, по-принцип се оказва верен; Moore, Gordon E. (19.4.1965 г.). „Cramming more components onto integrated circuits“ („Повишаване на гъстотата на компонентите върху интегралните схеми“), Electronics, 22.8.2011 г.

³ Nathan Eagle, Alex (Sandy) Pentland, „Reality mining: sensing complex social systems“ („Извличане на информация от действителността: засичане на данни от сложни социални системи“), Journal Personal and Ubiquitous Computing, том 10, брой 4, март 2006 г., стр. 255 — 268. В статията си, озаглавена „Big Other: surveillance capitalism and the prospects of an information civilization“ („Голямото друго: следящият капитализъм и перспективите за информационна цивилизация“), за Journal of Information Technology (2015 г.), брой 30, стр. 75 — 89, Shoshana Zuboff пише следното: „Вследствие от всепроникващото компютърно опосредстване почти всеки аспект от света се изобразява в ново символично измерение, докато същевременно събитията, предметите, процесите и хората стават видими, познаваеми и възможни за споделяне по нов начин“. Авторката предвижда „появата и възхода на нова универсална архитектура“, която тя нарича „Голямото друго“, „повсеместен режим на свързани в мрежа институции, който записва, изменя и превръща в стоки за потребление ежедневието — от тостерите до човешките тела и от комуникациите до мисълта — с цел създаване на нови пътища към приходи и печалба“ (стр. 77, 81).

⁴ „BBC Micro Bit computer's final design revealed“ („Обявяване на окончателния дизайн на микробит компютъра на BBC“), 7.7.2015 г., <http://www.bbc.com/news/technology-33409311> (достъп на 10.9.2015 г.); „No assembler required: How to teach computer science in nursery school“ („Няма нужда от асемблер: как да преподаваме компютърни науки в детската градина“), The Economist, 1.8.2015 г.

⁵ Нито една от десетте водещи по пазарна капитализация компании в технологичния сектор не е установена в ЕС (осем в САЩ, по една в Китай и Тайван) според данни на „PWC“, посочени в „Global Top Ten Companies by Market Capitalisation, 31 March 2015 Update“ („Водещите десет компании в света по пазарна капитализация, актуализация към 31 март 2015 г.“).

⁶ „Понятието „големи информационни масиви“ се отнася до експоненциалния растеж както на наличието, така и на автоматизираното използване на информация: то се отнася до огромните цифрови масиви от данни, притежавани от корпорации, правителства и други големи организации, които след това се анализират подробно (откъдето произтича и понятието „инструменти за анализ“), като за целта се използват компютърни алгоритми“; Становище 3/2013 на Работната група по член 29 за ограничаване до предвидената цел. В доклад на Белия дом от 2014 г. големите информационни масиви се описват като „нарастващата технологична способност за улавяне, обобщаване и обработване на данни с все по-голям обем, скорост и многообразие“, вж. „Big Data: Seizing Opportunities, Preserving Values“ („Големите информационни масиви: възползване от възможностите, опазване на ценностите“), Изпълнителен кабинет на Президента (т. нар. „Доклад Подеста“), май 2014 г.

⁷ Съгласно правото на ЕС „лични данни“ означава „всяка информация, свързана с идентифицирано или подлежащо на идентификация лице („съответно физическо лице“); за подлежащо на идентифициране лице се смята това лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификационен номер или един или повече специфични признаци, отнасящи се до неговата физическа, физиологическа, психологическа, умствена, икономическа, културна или социална самоличност“; член 2, буква а) от Директива 95/46/ЕО. В широк смисъл това определение е сходно с определенията, възприети от Съвета на Европа в Конвенцията за защита на лицата при автоматизираната обработка на лични данни

(т.нар. Конвенция № 108) и от ОИСР в нейните Основни насоки за защитата на личния живот и трансграничните потоци лични данни. За задълбочен анализ вж. Становище 4/2007 на Работната група по член 29 относно понятието „лични данни“, WP136.

⁸ Вж. например произнесената през 2014 г. реч на председателката на Федералната комисия по търговия на САЩ: „Разпространението на свързани устройства, рязко падащата цена на събирането, съхранението и обработването на информация, както и способността на търговците на данни и други лица да съчетават офлайн и онлайн данни означават, че компаниите могат да натрупват на практика неограничени количества потребителска информация и да я съхраняват за неограничен период от време. От това те могат да узнаят изненадващо много неща за всеки от нас посредством инструменти за прогнозиращ анализ“; Встъпителни бележки на председателката на Федералната комисия по търговия на САЩ Edith Ramirez, „Big Data: A Tool for Inclusion or Exclusion?“ („Големите информационни масиви: инструмент за приобщаване или за изключване?“), Вашингтон, окръг Колумбия, 15 септември 2014 г. Според Sandy Pentland „социалната физика е количествена социална наука, която описва надеждни математически връзки между потока на информация и идеи, от една страна, и поведението на хората, от друга... тя ни дава възможност да прогнозираме производителността на малки групи, отдели в рамките на компаниите и дори цели градове“. Именно „това се изисква за изграждане на по-добри обществени системи“ (стр. 4, 7) и така „[представителите на правителството, ръководителите в промишлеността и гражданите] могат да използват инструментите на стимулите в социалните мрежи, за да *установяват нови норми на поведение*“ (стр. 189) (курсивът е наш); Pentland, „Social Physics: *How Good Ideas Spread: The Lessons from a New Science*“ („Социална физика: как се разпространяват добрите идеи — уроците на една нова наука“).

⁹ Специално проучване на Евробарометър 431 относно защитата на данните от юни 2015 г. и проучване на Pew Research Panel от януари 2014 г. относно обществените схващания за неприкосновеността на личния живот и сигурността в ерата след Сноудън. Според едно от проучванията средното посещение на един уебсайт води до 56 случая на събиране на данни (според Julia Angwin, „Dagnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance“ („Нация на полицейското издирване: в търсене на неприкосновеността на личния живот, сигурността и свободата в свят на безмилостно наблюдение“), 2012 г.). В доклада на Белия дом от 2014 г. относно големите информационни масиви се твърди, че „безпрецедентната изчислителна мощ и степен на усъвършенстване... създават силова асиметрия между тези, които държат данните, и тези, които волно или неволно ги предоставят; „някои от най-дълбоките предизвикателства, установени при този преглед, засягат начина, по който анализът на големите информационни масиви може ... да създаде толкова неясна среда за вземане на решения, че независимостта на отделния индивид да се изгуби в непроницаем набор от алгоритми“.

¹⁰ Самоличността на 87 % от населението на САЩ вероятно може да бъде установена, като се използват обществено достъпните анонимни данни от преброяването на населението през 1990 г., а именно като се съчетаят петцифреният им пощенски код, полът и датата на раждане; вж. Paul Ohm, „Broken promises of privacy: responding to the surprising failure of anonymisation“ („Нарушените обещания за неприкосновеност на личния живот: реакция на изненадващия провал на анонимизирането“), UCLA Law Review, 2010 г., и „Record linkage and privacy: issues in creating new federal research and statistical info“ („Свързване на записите и неприкосновеност на личния живот: проблеми при създаването на нова информация от федерални проучвания и статистически данни“), април 2011 г. ДНК е уникална (с изключение на еднояйчните близнаци) и стабилна през целия живот. Тя съдържа информация за етноса, предразположението към заболявания и може да се използва за откриване на други кръвни роднини. През януари 2013 г. учени успяха да открият самоличността на лица и семейства от анонимни данни за ДНК, съхранявани в обществено достъпни генеалогични бази от данни; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. и Erlich, Y. *Science* 339, 321—324 (2013 г.). Вж. също „Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts“ („Зле анонимизирани регистрационни данни

разкриват подробното местоположение на таксиметровите шофьори в Ню Йорк“), 23.6.2014 г. <http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/> (достъп на 10.9.2015 г.). Вж. също Становище 4/2007 на Работната група по член 29 относно понятието „лични данни“; Становище 3/2013 на Работната група по член 29 за ограничаване до предвидената цел; Становище 6/2013 на Работната група по член 29 относно повторната употреба на свободно достъпни данни и на информация в общественния сектор (ИОС); и Становище 5/2014 на Работната група по член 29 относно техническите способности за анонимизиране.

¹¹ Източник: Gartner.

¹² Вж. например панелната дискуссия на тема „What is the future of official statistics in the Big Data era?“ („Какво е бъдещето на официалната статистика в ерата на големите информационни масиви?“), Кралско статистическо общество, Лондон, 19 януари 2015 г.; <http://www.odi.org/events/4068-future-official-statistics-big-data-era> (достъп на 10.9.2015 г.).

¹³ „Ten technologies which could change our lives: potential impacts and policy implications“ („Десет технологии, които биха могли да променят живота ни: потенциални въздействия и последици за областите на политиката“), Отдел за научни прогнози, Служба на ЕП за парламентарни изследвания, януари 2015 г.

¹⁴ Работната програма на ЕС за периода 2016—2017 г. в рамките на „Хоризонт 2020“ подкрепя тези развития, в това число мащабни пилотни проекти, при които ще се разгледа въпросът за неприкосновеността на личния живот и етичните съображения.

¹⁵ Застраховането е описвано като „първичния бизнес модел, от който произхожда „интернет на предметите“; „From fitness trackers to drones, how the „Internet of Things“ is transforming the insurance industry“ („От проследяващи физическата форма устройства до безпилотни летателни средства: как „интернет на нещата“ преобразява застрахователния бранш“), Business Insider, 11.6.2015 г. Понятието за ценова дискриминация в конкурентното право, произтичащо от член 102 ДФЕС, който забранява на предприятията с господстващо положение на пазара „пряко или косвено налагане на нелоялни покупни или продажни цени или на други несправедливи условия за търговия“, е предмет на сериозни спорове; вж. например Damien Gerardin и Nicolas Petit, „Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles“ („Ценовата дискриминация съгласно конкурентното право на ЕО: още една теория за защита на конкуренцията в търсене на ограничаващи принципи“), юли 2005 г., Global Competition Law Centre Working Paper Series, брой 7/05. По въпроса за големите информационни масиви и техния (все още нереализиран според авторите) потенциал да ускорят персонализираното ценообразуване вж. публикацията на Изпълнителния кабинет на Президента на САЩ „Big Data and Differential Pricing“ („Големите информационни масиви и диференцираното ценообразуване“), февруари 2015 г., както и неотдавнашен анализ, според който персонализираното ценообразуване по принцип е свързано с обработване на лични данни, от което следва, че трябва да спазва предвидения в правото в областта на защитата на лични данни принцип за прозрачност, който изисква от компаниите да уведомяват лицата за предназначението на обработката на личните им данни: ако компаниите персонализират цените, то те трябва да оповестят този факт. А ако компания използва „бисквитка“, за да разпознае някого, то Директивата за правото на неприкосновеност на личния живот и електронните комуникации изисква от нея да уведоми лицето за предназначението на тази „бисквитка“; работен проект от Frederik Borgesius, „Online Price Discrimination and Data Protection Law“ („Ценовата дискриминация онлайн и правото в областта на защитата на личните данни“). На разположение на адрес http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (достъп на 10.9.2015 г.).

¹⁶ Медицинските изделия са определени в правото на ЕС посредством Директива 93/42/ЕИО на Съвета относно медицинските изделия, изменена с Директива 2007/47/ЕО на Европейския

парламент и на Съвета от 5 септември 2007 г. По въпроса за последиците от „мобилното здравеопазване“ за защитата на личните данни вж. Становище 1/2015 на ЕНОЗД.

¹⁷ Според Евростат 21 % от физическите лица и 19 % от предприятията в ЕС използват услуги за съхранение „в облак“.

¹⁸ „Ако световната мрежа бе държава, щеше да е на 12-о място по потребление на електроенергия в света, някъде между Испания и Италия. Това представлява грубо от 1,1 до 1,5 процента от световното потребление на електроенергия (към 2010 г.), а произвежданите ежегодно парникови газове се равняват на количеството, произвеждано от 70 до 90 големи (500-мегаватови) топлоелектрически централи на въглища“. Natural Resources Defense Council (Съвет за опазване на природните ресурси), „Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers“ („Оценка на ефективността на центровете за данни: повишаване на енергийната ефективност в сектора на центровете за данни, оценка на основните двигатели и пречки“), 2014 г.

¹⁹ Доклад от проучването „SMART 2013/0043 — Uptake of Cloud in Europe“ („SMART 2013/0043 — възход на облака в Европа“).

²⁰ Източник: Евростат.

²¹ Понятието „икономика на споделянето“ е критикувано като подвеждащо: „The Sharing Economy Isn't About Sharing at All“ („В икономиката на споделянето няма нищо споделено“), Giana M. Eckhardt и Fleura Bardhi, Harvard Business Review, 28.1.2015 г.

²² Rachel Botsman и Roo Rogers, „What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live“ („Моето е и твое: как съвместното потребление променя начина ни на живот“), 2011 г.

²³ Future of Privacy Forum, „User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy“ („Потребителска репутация: изграждане на доверие и решаване на проблеми с неприкосновеността на личния живот в икономиката на споделянето“), юни 2015 г.

²⁴ Вж. проведения на 9 юни 2015 г. семинар на Федералната комисия по търговия на САЩ на тема „Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy“ („Конкуренция, защита на потребителите и икономически въпроси, повдигнати от икономиката на споделянето“), <https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/> (достъп на 10.9.2015 г.).

²⁵ По въпроса за последиците за защитата на данните от използването на безпилотни или дистанционно управляеми летателни системи вж. Становището на ЕНОЗД относно Съобщението на Комисията до Европейския парламент и до Съвета относно „Нова ера във въздухоплаването — Отваряне на авиационния пазар за сигурно и устойчиво гражданско използване на дистанционно управляеми летателни системи“, ноември 2014 г.

²⁶ Източник: Boston Consulting Group.

²⁷ Gartner.

²⁸ Алгоритъмът за лицево разпознаване DeepFace на Facebook има отчетена успеваемост 97 %, което надминава човешките способности; „DeepFace: Closing the Gap to Human-Level Performance in Face Verification“ („DeepFace: запълване на празнотата в способността на хората да разпознават лица“), публикувано в доклад на конференция на Института на инженерите по електротехника и електроника на тема компютърно зрение и разпознаване на модели, юни 2014 г.

²⁹ Роботът е определен като „пребиваваща в света машина, която усеща, мисли и действа“; Bekey, G, „Current trends in robotics: technology and ethics“ („Актуални тенденции в роботиката: технологии и етика“) в „Robot Ethics — The ethical and social implications of robotics“ („Етиката

на роботите — етичните и социални измерения на роботиката“), The MIT Press², 2012 г., стр. 18. По прогнози, за периода 2013—2016 г. ще бъдат продадени 22 милиона обслужващи робота, IRF World Robotics Report (Световен доклад за роботиката на Международната федерация по роботика), 2013 г. По въпроса за изкуствения интелект вж. „Rise of the Machines“ („Възходът на машините“), Economist, 9.5.2015 г. и Pew Research Centre Internet Project (Интернет проект на научноизследователския център Pew), 2014 г. Компания за изкуствен интелект обвърза придобиването си от водеща технологична корпорация през 2014 г. с условието да се създаде съвет по етика и безопасност и да се забрани използването на изкуствения интелект за военни или разузнавателни цели; Forbes, „Inside Google's Mysterious Ethics Board“ („Във вътрешността на мистериозния съвет по етика на Google“), 3.2.2014 г.

³⁰ Pentland, „Social physics“ („Социална физика“), стр. 147.

³¹ Вж. бележка 9 по-горе. Pentland, „Social Physics“ („Социална физика“), стр. 153: „Големи скокове в здравеопазването, транспорта, енергетиката и безопасността — всичко това е възможно... основните препятствия пред постигането на тези цели са съображенията за неприкосновеността на личния живот и фактът, че все още няма консенсус за компромисите между лични и социални ценности“. Дебатът около пандемията от ебола през 2014 г. в Западна Африка е показателен как се впряга в употреба фиктивното противопоставяне между индивидуалната неприкосновеност на личния живот и нуждите на обществото. Съществува тенденция заболяванията да се проследяват и да се измерва продължителността им посредством анкети и преброявания на населението, които остаряват много бързо и е трудно данните от тях да бъдат екстраполирани с цел предвиждане на бъдещи огнища. Съществуват някои примери за използване на големи информационни масиви за проследяване на огнища на малария в Намибия и Кения, а през 2009 г. — за проследяване на ефективността на здравните предупреждения, отправяни от правителството по време на кризата с мексиканския свински грип. Един източник на данни са записите за мобилни повиквания, които показват коя базова станция е обработила повикването, и могат да дадат в реално време приблизителното местоположение на хората и накъде се движат. Събирането на тези данни не е целенасочено, т.е. по този начин не може да се разграничи кой е носител на ебола и кой не. Шведска организация с нестопанска цел е картографирала движението на населението в Западна Африка, но данните не са използвани, тъй като мобилните оператори са отказали да ги предоставят на одобрени външни учени с довода, че трябва да получат указания от съответните правителства, които на свой ред се позовават на съображения за нарушаване на неприкосновеността на личния живот, което не се допуска съгласно правото на ЕС; <http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola>. (достъп на 10.9.2015 г.)

³² Становище 3/2015 на ЕНОЗД.

³³ Допускането в големите информационни масиви, че N =всичко, се отнася до разглеждането на всички точки с данни, а не само на извадка, Viktor Mayer-Schönberger и Kenneth Cukier, „The Rise of Big Data: How it's changing the way we think about the world“ („Възходът на големите информационни масиви: как това променя начина, по който мислим за света“), 2013 г. Лисабонският съвет и Институтът за прогресивна политика твърдят, че просперитетът ще се повиши чрез максимално използване на „цифровата гъстота“, която представлява „количеството данни, използвани на глава от населението в дадена икономика“ <http://www.lisboncouncil.net/component/downloads/?id=1178> (достъп на 10.9.2015 г.). Международната работна група по защита на данните и телекомуникациите (известна с името „Берлинската група“) предложи дерогации за големите информационни масиви от принципите за защита на данните; http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (достъп на 10.9.2015 г.). Световният икономически форум призова за съсредоточаване върху ползването, а не върху събирането, и за загърбване на изискването за даване на съгласие за събиране на лични данни;

„Unlocking the Value of Personal Data: From Collection to Usage“ („Отключване на стойността на личните данни: от събиране към ползване“), 2013 г.

³⁴ Вж. Предварителното становище на ЕНОЗД относно защитата на личния живот и конкуренцията в ерата на огромното количество данни.

³⁵ Член 21 от Хартата на основните права забранява „всяка форма на дискриминация, основана по-специално на пол, раса, цвят на кожата, етнически или социален произход, генетични характеристики, език, религия или убеждения, политически или други мнения, принадлежност към национално малцинство, имотно състояние, рождение, увреждане, възраст или сексуална ориентация“. Много от тези категории данни („разкриващи расов или религиозен произход, политически идеи, религиозни или философски убеждения, членство в професионални съюзи, както и обработването на данни, свързани със здравословното състояние и половия живот“) се ползват с по-силна защита съгласно член 8 от Директива 95/46/ЕО.

³⁶ Относно идеята за общи цифрови ресурси вж. „Ambition numérique: Pour une politique française et européenne de la transition numérique“ („Цифрови амбиции: за френска и европейска политика за цифровия преход“), Френски съвет за цифрови технологии, юни 2015 г., стр. 276; Bruce Schneier призовава за създаване на „публични пространства без собственик“ в интернет подобно на обществените паркове, „Data and Goliath“ („Данните и Голиат“), стр. 188—189; Sandy Pentland изтъква доводи в полза на „публични общи данни“, „Social Physics“ („Социална физика“), стр. 179. По въпроса за безопасността на публикуването на обобщени масиви под формата на свободно достъпни данни вж. Становище 6/2013 на Работната група по член 29 относно повторната употреба на свободно достъпни данни и на информация в обществения сектор (ИОС).

³⁷ „Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent“ <http://crackedlabs.org/studie-kommerzielle-ueberwachung/info>. По въпроса за квалифицираната прозрачност вж. напр. Frank Pasquale: „The Black Box Society: The Secret Algorithms that Control Money and Information“ („Обществото на черната кутия: тайните алгоритми, които контролират парите и информацията“).

³⁸ „Зад технологиите, които влияят върху обществените отношения, стоят същите тези отношения“, David Noble, „Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools“ („Обществен избор при проектирането на машини: случаят на автоматизираните машинни инструменти“) в „Case Studies in the Labor Process“ („Случаи от практиката в трудовия процес“), ред. Andrew Zimbalist, 1979 г. Вж. също Judy Wacjman, „Pressed for Time: The Acceleration of Life in Digital Capitalism“ („Няма време: забързването на живота в цифровия капитализъм“), 2014 г., стр. 89—90; и Zuboff, „Big Other“ („Голямото друго“) (цитирано в бележка 3 по-горе).

³⁹ Становище 5/2014 относно техническите способности за анонимизиране, прието на 10 април 2014 г. (WP 216).

⁴⁰ По въпроса за стеснителното тълкуване на освобождаването от правилата за защита на данните при упражняване на дейности, които са изключително лични или домашни, вж. Решение на Съда на ЕС по дело C-212/13, František Ryneš срещу Úřad pro ochranu osobních údajů.

⁴¹ Понятието „произвеждащ потребител“ е въведено от Alvin Toffler в „The Third Wave“ („Третата вълна“), 1980 г. За анализ на „средата на произвеждащите потребители“ и начините за нейното регламентиране вж. Ian Brown и Chris Marsden, „Regulating Code“ („Регламентиране на кода“), 2013 г.

⁴² Становище на Европейската група по етика в науката и новите технологии към Европейската комисия: „Ethics of Security and Surveillance Technologies“ („Етика в технологиите за сигурност и наблюдение“), Становище № 28, 20.5.2015 г., стр. 74.

⁴³ Вж. например „Homer Economicus: The Simpsons and Economics“ („Хоумър Икономикус: семейство Симпсън и икономиката“), ред. Joshua Hall, 2014 г.

⁴⁴ Дори при най-консервативното определение за грешка това означава, че в потребителските досиета на 23 милиона американци има съществени грешки. При пет процента от досиетата на участниците в проучването еднократното коригиране на грешката е довело до подобряване на оценката им за кредитоспособност, така че да могат да получат кредит на по-ниска цена; Федерална комисия по търговия, „Report To Congress Under Section 319 Of The Fair And Accurate Credit Transactions Act Of 2003“ („Доклад към Конгреса съгласно член 319 от Закона от 2003 г. за лоялно и точно кредитиране“), декември 2012 г.; Chris Jay Hoofnagle, „How the Fair Credit Reporting Act Regulates Big Data“ („Как Законът за докладване в сферата на лоялното кредитиране контролира големите информационни масиви“), 10 септември 2013 г. Семинар на Future of Privacy Forum по въпросите на големите информационни масиви и неприкосновеността на личния живот: „Making Ends Meet“ („Да свържем двата края“), 2013 г. На разположение на адрес в SSRN: <http://ssrn.com/abstract=2432955>.

⁴⁵ Световният икономически форум определя данните като ценен актив на индивида, чиито права на притежание, използване и унищожаване могат да бъдат преотстъпени на компании и държавни органи в замяна на услуги. Вж. неотдавнашни изказвания на заместник-председателя на Европейската комисия Андрус Ансип, например изказването му от 7.9.2015 г. на годишната среща на мозъчния тръст „Брьогел“, озаглавено „Производителност, иновации и цифровизация — кои са предизвикателствата пред глобалната политика?“, в което той казва: „Собственост и управление на потоците от данни, първично и повторно използване на данните. Управление и съхранение на данните. Това лежи в основата на важни нововъзникващи сектори, като компютърните услуги „в облак“, „интернет на предметите“ и големите информационни масиви“.

⁴⁶ „И така, кой притежава правото да ползва информацията и данните, които не принадлежат неразривно на индивида? Това е въпрос, който излиза извън границите на търговията, етиката и морала и води до проблеми с неприкосновеността на личния живот и нейната защита“; Al-Khoury, ноември 2012 г., http://www.academia.edu/6726887/Data_Owner_ship_Who_Owns_My_Data_036. Вж. също Margaret Jane Radin, „Incomplete Commodification in the Computerized World“ („Непълно комерсиализиране в компютъризирания свят“) в The Commodification of Information, брой 3, стр. 17, ред. Niva Elkin-Koren и Neil Weinstock. 2002 г.: „Има голямо значение дали неприкосновеността на личния живот се схваща като човешко право, присъщо на хората като личности, или като имуществено право, т.е. като нещо, което може да се притежава и контролира от хората. По презумпция човешките права не могат да се отчуждават от пазара, докато имуществените могат“.

⁴⁷ Проектът в кръстосан облак, провеждан от Лабораторията по компютърни науки и изкуствен интелект на Масачузетския технологичен институт с подкрепата на няколко компании, установени в ЕС, има за цел „1) да улесни разработването на многопотребителски („социален“) софтуер с използването единствено на фронтенд програмиране и зачитане на правата и неприкосновеността на личния живот на потребителите; и 2) да даде на потребителите свобода да се придвижват лесно между приложения, хардуерни платформи и социални мрежи, като запазват данните и социалните си връзки.“; <http://openpds.media.mit.edu/#architecture> (достъп на 10.9.2015 г.).

⁴⁸ Вж. разяснението относно член 1 от Хартата на основните права.

⁴⁹ Martha Nussbaum, „Objectification“ („Опредметяването“) във Philosophy and Public Affairs, брой 24, стр. 4, 1995 г.

⁵⁰ Съдебно решение от 15 декември 1983 г., BVerfGE 65, 1-71, Volkszählung.

⁵¹ Вж. Становището на Европейската група по етика в науката и новите технологии „Ethics and Surveillance“ („Етика и наблюдение“), стр. 75. В проучване се излага твърдението, че

алгоритъм за насочване на реклами е бил дискриминационен, тъй като средно при търсения от мъже е извеждал реклами за по-високо платени длъжности, отколкото при търсения от жени, които са посещавали сайтове за намиране на работа; Университет Carnegie Mellon и Международният институт за компютърни науки. Относно тенденцията на цифровите асистенти да се присвоява женски глас по подразбиране вж. например Judy Wajcman, „Feminist theories of technology“ („Феминистки теории за технологиите“). *Cambridge Journal of Economics*, 34 (1), стр. 143—152, 2010 г.

⁵² Giorgio Agamben, „State of Exeption“ („Постоянното изключение“), 2005 г.

⁵³ Neil Richards, Neil и Jonathan King, „Big Data Ethics“ („Етика на големите информационни масиви“), 19 май 2014 г., *Wake Forest Law Review*, 2014 г.

⁵⁴ BBC, Information watchdog investigates ‘charity data sales’ (Активистка организация за права в информационната среда разследва „благотворителни продажби на данни“), 1.9.2015 г.

⁵⁵ Вж. писмото на Future of Life Institute. Папската енциклика „*Laudato Si'*“: „когато медиите и цифровият свят станат всеобщо, влиянието им може да попречи на хората да се научат да живеят мъдро, да мислят задълбочено и да обичат щедро. Така великите мъдrecи от миналото може да останат нечути сред шума и разсейването на вниманието, предизвикани от информационно претоварване. Трябва да се положат усилия за превръщане на тези медии в източници на нов културен напредък за човечеството, а не в заплаха за най-съкровени ценности. Истинската мъдрост, плод на самопознанието, диалога и щедрото съприкосновение между хората, не се придобива чисто и просто чрез натрупване на данни, което в крайна сметка води до претоварване и объркване, нещо като замърсяване на ума. Истинските взаимоотношения с останалите, заедно с всичките им предизвикателства, сега сякаш се заместват от някакъв вид общуване по интернет, което ни позволява да избираме или елиминираме взаимоотношения според прищявките си, при което възниква нов вид изкуствена емоция, която е по-силно свързана с устройствата и дисплеите, отколкото с другите хора и с природата. Днешните медии все пак ни дават възможност да общуваме и да споделяме знанията и чувствата си. При все това понякога те ни служат като щит срещу прякото съприкосновение с болката, страховете и радостите на другите и сложността на личните им преживявания. Поради тази причина трябва да сме разтревожени, че заедно с вълнуващите възможности, предлагани от тези медии, те могат да породят и дълбоко меланхолично разочарование от междуличностните отношения или вредно чувство на изолация“.

⁵⁶ Вж. дейност 4 от Стратегията на ЕНОЗД за периода 2015—2020 г., „Развиване на етично измерение на защитата на личните данни“.