**Втора тема .ДАННИТЕ – ОСНОВА НА ИКОНОМИКАТА**

***Усложнения от етичен характер се появяват при събирането, анализа и обработката на цифровите данни за гражданите – „големите данни“, социални и персонални. На бизнеса те са нужни, за да може да обучава ИИ, за реклама и онлайн търговия. На държавата, за да може да взема управленчески решения, да взаимодейства с гражданите, обезпечаване на държавната сигурност.***

***В тази тема ще се запознаете с основните етични проблеми свързани с данните и до колко тясно те са свързани с ИИ и другите цифрови технологии.***

**Какво разбираме под данни*?***

Преди да преминем към въпроса за етиката сме задължени да направим изравняване на понятийния апарат.

Данните се различават от информацията – самата тя може да бъде представена не само под формата на данни, но и под формата на сведения.

**ИНФОРМАЦИЯ – сведения (съобщения, данни) независимо от формата им на представяне**

В международните документи и закони има различни определения за терминът „данни“ и „информация“. В рамките на този учебник под „данни“ ще използваме значението което е дадено в стандарт ISO/IEC общоприет за в сферата на информационните технологии.

**ДАННИ – информация (факти, понятия и инструкции) под форма възприета за общуване, интерпретация или обработка от хората или от автоматични системи[[1]](#footnote-1).**

В научната и популярната литература се предлагат различни класификации за данни. Много често едни и същи се съотнасят към различни типове и по тази причина настъпват противоречия при представянето на детайлна класификация. Без претенция за изчерпателност предлагаме най-често използваните в различен контекст типове данни.

**ГОЛЕМИ ДАННИ (BIG DATA) – термин даващ характеристиките на натрупан и анализиран информационен ресурс, чиито обеме значително нараснал и превишава възможностите те да бъдат съхранявани и анализирани на основата на по-рано създадените апаратни и програмни средства[[2]](#footnote-2).**

**ГОЛЕМИ ДАННИ ОТ ИНТЕРНЕТ – унифицирани сигнали, постъпващи от датчиците на „умните“ устройства използвани в производството, селското стопанство, преносимите устройства и т. н.**

**ПЕРСОНАЛНИ ДАННИ (ПД) – всяка информация отнасяща се пряко или косвено за определено или определяно като такова физическо лице.**

**СОЦИАЛНИ ДАННИ – свързани с човека, неговото придвижване, поведение и интереси, отношения с другите хора, места, стоки и дори идеология.**

**ДЪРЖАВНИ ДАННИ – информация съдържаща се в информационните ресурси на органите и организациите в държавния сектор (данни на органите на властта, събирани за целите на статистиката, такива свързани с реализацията на държавния бюджет.**

**ОТКРИТИ ДАННИ – информация поместена в интернет под формата на систематизирани данни , организирана във формат допускащ автоматичната и обработка без предварителна промяна от човек с цел еднократно, свободно и безплатно използване.**

Данните се превръщат в критичен ресурс и определят ефективността на дейността на предприятия, държавните органи и икономиката като цяло според Комисията на ООН за науката и техниката с цел развитие още през 2014 година. Това касае особено много създаването на т. нар. „Електронно правителство“ като проява на зрялост и развитие на демокрацията.

***Дата-етиката*** или етиката на данните като форма на приложната етика се появяват сравнително скоро и имат само някакво общо определение. Достатъчно точно работно определение на термина и описание на основа етика предлага британската фреимуорк етика на данните от 2018 година. Тя е ориентирана към внедряването на етични практики в работата с данни в сферата на държавния и публичен сектор: „Етиката на данните само по себе си представлява формиращ отрасъл на приложната етика, описващ ценностните съждения и подходи приети при събирането, анализа и разпространението на данни. Те предполагат добро познаване на законодателството отнасящо се до защитата на данните и многопрофилното законодателство, като същевременно са ангажирани с правилните начини за използване на новите технологии. Те изискват цялостен подход включващ опита натрупан в сферата на компютърните технологии и решаването на етичните задачи и осигуряването на информационна безопасност“[[3]](#footnote-3)

Главен аспект при етика на данните е използването на анализа (data science) по правилния начин. Науката за данните се описва като автоматичен метод който с помощта на анализ извлича от информационните данни определена информация като се предвиждат навлизането на определени технологии свързани както с патерните на традиционната аналетика така и предиктивните технология на базата на машинното обучение.

Дата-етиката се развива и става все по-актуална и това е видимо от наличието вече на съответни държавни, корпоративни и социални документи. Определянето ха границите за етичен достъп към данните е сложен проблем засягащ голям брой страни – гражданите, държавата, корпорациите, обществените институции и т.н., като това изисква сътветно и намирането на комплексно решение. Един особено важен проблем свързан с данните е деперсонализацията на биомедицинските данни. От една страна може да бъде използвано:

ОБЕЗЛИЧАВАНЕ /АНОНИМИЗАЦИЯ – *свързано с действия в резултат на които се загубва връзката между съвкупността на идентифициращите данни и субектните данни.*

* *Данни непосредствено идентифициращи конкретно лице (ЕГН, адрес и пр.) се отделят от базата;*
* *Идентификацията на отделната личност става трудно.*
* *Юридически се опростява използването им когато липсва персонален достъп;*
* *Усложнява се използването им с научна цел до толкова до колкото се премахват данните на етап съхранение в дадена система не позволяващи след това те да бъдат свързани с определен човек в различните бази (примерно рентгеновите снимки с лабораторния протокол и бележките на лекуващия лекар). Същевременно става невъзможно обновяването на данни, ако те не са деноминизирани;*
* *Остава риска за деноминизация с косвената идентичност (примерно допълнителна идентификация по признаци свързани със социалните медии);*

*От друга страна се наблюдава:*

ПСЕВДОНОМИНИЗАЦИЯ *– обезличаване с добавяне на връзка между съвкупност от обезличени данни и един или няколко псевдонима:*

* *Данните за непосредствена идентификация за конкретно лице се премахват или променят (ЕГН, адрес и др.)*
* *Записите за даден човек биват подведени под определен псевдоним, благодарение на което при необходимост могат да бъдат деноминизирани (да се персонофицират);*
* *Благодарение на един псевдоним могат да бъдат обединени данните на един човек в различни бази и могат да бъдат допълвани с нови данни запазвайки неговата конфиденциалност;*
* *Данните стават удобни за аналетика;*
* *Свързването на персоналните данни с псевдоним стават сложни за юридически манипулации;*
* *Рискът от деноминизация е по-висок от този при анонимизацията*
* *Технологично по –сложно и скъпо е от колкото необратимата анонимизация*.

Сведенията отнасящи се до здравето на човека и медицинските процедури безусловно подлежат на контрол поради високия риск от етична колизия.

**2.1.2 Етични проблеми свързани с данните**

Потребността от приложно регулиране с цел обезпечаване на етичните принципи нараства поради натрупването на достатъчно количество данни, чието използване може да бъде както позитивно така и негативно. Новите технологии за събиране на данни, съхраняването им, анализа и използването на направените изводи все по-често карат разработчиците да търсят решения на въпросите свързани с това кое е позволено, до колко е правомерно, рисково, ефективно използването на данни в една или друга ситуация. Какви са преимуществат и недостатъците в използването на данни:

|  |  |  |
| --- | --- | --- |
| ПРЕИМУЩЕСТВА | СИТУАЦИЯ С ИПОЛЗВАНЕ НА ДАННИ | НЕДОСТАТЪЦИ |
| * Развитието на приложните науки; * Големи международни проекти | Събиране и обработка на голяма база данни | * Нарушения в приватността (с голяма база данни се работи както с персонални); * Скрита манипулация на гражданите(покупки, решения) |
| * Персонофицирани сървари; * Нови продукти и услуги; * Цифрови платформи; | Акумулиране на данни в компаниите | * Нарушаване и инфлация на приватността; * Цифров монополизъм; * Дискриминация * на скрининговата система |
| * Обществена безопасност ; * Национална безопасност; * Съкращаване на времето за получаване на административни услуги; * Отвореност на данните; * Актуална статистика за извеждане на държавни решения; | Акумулиране на данни в държавата включително и такива от видеонаблюдение | * Цифров тоталитаризъм; * Големият брат“ * Нови начини за налагане на дискриминация * Нарушаване на приватността; |
| * Бързи услуги * Персонализация на услугите и продуктите * Мащабно развитие на приложните науки; | Предаване на данни за Изкуствен Интелект | * Различни форми на дискриминация; * Скрити грешки * Нарушаване на приватността; |
| * Общуване и себеизразяване в соц. мрежите; * Свобода на словото * Нови форми на СМИ | Ползвателите на данни имат открит достъп | * Нарушаване на приватността (данните са достъпни за обобщаване), разпространяване на чувствителна информация * Измами с използването на социална инженерия и технологията на дипфейк; |

Основната етична дилема е около избора да се съблюдават гражданските права, интересите на социалните групи, държавата от една страна и създаването на нови продукти , услуги, възможностите за пряко или косвено използване на данни от друга.

Максималното количество рискове възникват при събирането, анализа и използването на резултатите за хората, като рисковете се оформят в три групи: обработката на данни с помощта на ИИ, видеонаблюдение, проследяване в Интернет. Най-големият риск е свързан с загубата на приватност.

**Големи данни**

Развитието на някой технологии и на първо място ИИ, силно зависят от достъпът до определени типове и голени бази данни. Големите данни и технологиите за тяхната обработка се използват за създаването не само на комерсиални проекти, а и за социални и научно изследователски такива. Като пример може да послужи съвместния проект на Google и Централната водна комисия на Индия с цел създаване на подход за предсказване на наводненията в щата Бихар.[[4]](#footnote-4)

***През 2018 година компанията Google получава достъп до персоналните медицински данни на милиони американци, включително резултатите от лабораторните изследване и диагнозите. Нито един от пациентите не е дал информирано съгласие. Официално обявената цел е обучението на ИИ за повишаване качеството на медицинското обслужване. В случая формално нарушение на американското законодателство няма, поради факта, че в него няма забрана медицинските власти да предоставят такава информация на трети страни при оказване на медицинска помощ. През 1996 година когато се приема закона в него е разрешена такова предаване на данни и тогава дата –корпорация не е съществувала (The Health Insurance Portability and Accountability Act of 1996)[[5]](#footnote-5)***

**Акумулирани от компаниите данни**

Най-опитния и развит участник в пазара на данни са т. нар. дата-корпорации, които са големи IT-компании, чието съществуване стана възможно благодарение на достъпа до голямо количество данни носещи огромно количество печалби от тяхното събиране, обработка и продажба на ползватели. Голямата петорка технологични гиганти са Microsoft, Alphabet ( Googlе e дъщерна) Facebook, Amazon и Apple. В тях се акумулира основният финансов, интелектуален и научен ресурс. В Русия най големите IT-компании са Яндекс, Mail.Ru Group, в Китай — Alibaba Group, Baidu, Tencent, Huawei и др.

Повечето етически проблеми са свързани с данни възникват заради високата себестойност на данните за гражданите и колосалната заинтересованост на компаниите. За да получат по-големи печалби компаниите нарушават човешките права при обработката на данните.

*Google, Apple, Facebook, Amazon и Microsoft събират и обработват милиони аудиозаписи, през автоматизираните гласови помощници и „умните“ колонки през които могат да се извлекът фрагменти от разговори и други звуци. Записите се правят съвсем автоматично без предупреждение за ползвателя, като данните се използват за обучение на ИИ да разпознава човешката реч*[[6]](#footnote-6).

**Акумулирани данни от държавата**

Държавата е един от най-големите притежатели на данни и вероятно в перспектива ще увеличава потенциалът си в тази област. Достъпността на данните и тяхната защитеност повишава доверието на гражданите, стимулира държавните служби в посока ефективност. Същевременно се засилва и контролът върху събирането и съхранението на данните и това е спирачка в посока развитие.

Държавата е гарант за спазването правата на човека и заради това при регулирането на оборота на данните тя трябва да осигури спазването на етичните норми заедно с контрола върху националната сигурност. В такива условия възниква дилемата кое е приоритетно – интересите на гражданите (преди всичко приватността) или интересите на обществото и държавната сигурност?

**Предаване на данни за изкуствен интелект.** За да има развитие технологията на ИИ е необходимо да се събират огромно количество данни – двете са зависими на 100% едно от друго. Въпросът е как да се използват максимум данни с минимум риск? Съвременната изчислителна способност на ИИмогат да се обработват огромни обеми от данни и да се намира дълбока скрита връзка между тях.

Същевременно колкото и да са деперсонофицирани тези данни могат да създадат маркер спрямо някой човек с информация за неговите роднини, професия и пр. така пълнотата на данните които са критически значими за успешното разработване на интелектуални системи стават потенциално опасни за опазване на приватността и правата на човека. Правейки събиране и анализ на данни с помощта на ИИ технологичните гиганти могат да правят и корелации, които човек не може да осъзнае и разбере и това може да се случи примерно на основата на някакво целенасочено косвено търсене.

Силното ограничаване (регулиране) на достъпа до данни усложнява и затормозява развитието на технологиите на ИИ за машинно обучение. Добре премисленото законодателство и акуратната употреба може да създаде баланс между обема и степента на анонимизация на персоналните данни, ако не създава прекалено много забрани и такова законодателство е в процес на създаване.

**Ползвателски данни публикувани в откритото пространство.** Събирането на данни „по подразбиране“ се случват естествено в моментите когато човек използва мобилно устройства и интернет. Приема се, че данните които ползвателя поставя в безплатните социални мрежи, електронните съобщения оставят някаква електронна следа, би трябвало да принадлежат на съмите хора които ги излъчват, а дата-компаниите управляват тези данни само по причина на това че владеят базата върху която се случват. Реалността обаче е съвсем друга – такъв тип данни се превръщат в огромен източник на печалби за тези компании.

Стандартния механизъм за получаване на съгласие за обработката на данните става абсолютно неактуален поради факта, че този процес е неконтролируем с течение на времето(примерно 10-20 години) и става очевидно недействителен. Данните се пазят толкова дълго, че в момента на получаване на съгласието става невъзможно човекът да бъде уведомен за това какви данни и как ще бъдат обработвани в бъдеще.

**Изтичане на данни – причини и следствия.** Това е едно масово явление наблюдавано по целия свят и никой не е застрахован срещу него ( нито държавата, нито бизнеса). Пряк целенасочен пробив се случва рядко, но причини за това са:

* Грешки в законодателството;
* Не добре обмислената работа на регулационните органи;
* Грешки на самите разработчици (неправилна настройка на сървър по отношение на достъпа възприет по подразбиране);
* Нелоялност на вътрешни служители копиращи данни с цел лична изгода

Още по-критична е ситуацията с данните в социалните мрежи и ежедневната дейност на хората през инфраструктурите на „Умния град“. Дори преносими „умни“ устройства носят вреди за собственикът си по отношение на предумишлено разкриване на информация.

**Търсене и намиране на етични решения при работа с данни**

***В съвремието сравнително рядко се повдигат въпроси около етиката на данните и етичните въпроси пред бизнеса, разработчиците, законодателите и държавата. Съществуващите закони в сферата на персоналните данни на гражданите в настоящия момент са твърде неефективни, етичен кодекс на данните все още няма задължителен статус и разпространение, за да влия е върху тази област.***

**Регулиране на основа data-етика**

Когато говорим за актове и документи маркиращи етичните принципи при използването на цифровите технологии е важно да отбележим, че в много сфери (медицина, правосъдие) много отдавна съществуват професионални етични кодекси. Те трябва да бъдат вземани под внимание при създаването на нови документи регулиращи използването на цифрови технологии. Създаването на единен кодекс едва ли е възможно в близко време, защото той би бил или твърде общ и съкратен за да отговаря на всички приложни области и отрасли или ще бъде в другата крайност – твърде подробен и противоречив стараейки се да обхване всичко свързано с проблематиката.

Публичния дебат относно използването на един или друг принцип или идея, постиженията и грешките от реалната практика позволяват да се постигне детайлно изследване в областта на етиката на данните . с всяко изминаваща година се разработват все по-нови етични кодекси, фреймуоркове, гайдлайни и подобни препоръки за работата с данни. Съответно те могат да бъдат класифицирани:

* Според сферата в която се прилагат: здравеопазване[[7]](#footnote-7), социална защита, държавна администрация[[8]](#footnote-8), юриспруденция[[9]](#footnote-9), борба с престъпността, финанси[[10]](#footnote-10), промишленост и т.н.:
* Според технологията: разпознаване на лица, системи за ИИ, роботехника, обработка на големи данни и др.
* Според локализацията: документи на ООН, документи касаещи управлението на конкретен град или конкретна компания (примерно правилата за етично използване на технологии за лицево разпознаване от полицията на Лондон или принципите на ИИ на Microsoft[[11]](#footnote-11)

Законодателство защитаващо персоналните данни са приети или се подготвят за прилагане в редица страни, при което повечето са за по-твърдо и стриктно прилагане на регулаторни и праворегулиращи модели. На основата на различните базови ценности могат да се дефинират три модела за регулиране на персоналните данни - *европейски, американски и китайски;*

Правните практики по отношение на една и съща технология могат да се различават кардинално и това показва нагледно разногласията примерно по повод използването на данните от лицево разпознаване.

*В Китай разпознаването на лица е много популярно, включително се прилага в много скрининги. Учебните заведения го използват по отношение на посещаемостта, заплащането на храната и контрола за въвлечеността на учениците по време на занятия. Въпреки жалбите на учениците и студентите за това, че системата допуска редица грешки или „заплашва“ не съществува и най-малък намек властите да се откажат от тях.*

*В Швеция през август 2019 едно средно училище е било глобено с 200 000 шведски крони (20 000 евро) за това, че използвало камери за разпознаване на лица в контрола си върху посещаемостта. Профилният контролно надзорен орган (Data inspektionen) приема, че съгласието на учениците да се събират техни биометрични данни не е достатъчно основание да се прилага лицево разпознаване , до колкото учиниците са в зависимоположение спрямо училището и съгласието им не било до край доброволно[[12]](#footnote-12)*

**Европейски модел.** В основата му лежат концепции за регулиране на персоналните данни без да се допуска прекомерен контрол над личния живот на човека нито от страна на държавните институции, нито от страна на фирмите. Това е заложено като основен принцип на всички европейски държави[[13]](#footnote-13). Ако внедряването на нови технологии или се въведе нов ред за използването на данни по някакъв начин нарушават човешките права се наблюдава силна обществена резистентност и съпротива. На правителствата им се налага да се справят с подобна резистентност ( прилагане на механизми за убеждане, просвета, етични похвати и т.н) ако използването на такива технологии имат висока значимост в полза на обществото.

Същността на европейският подход е представен най-ярко в регламента за защита на персоналните данни (General Data Protection Regulation, General

Data Protection Regulation, GDPR) приет в ЕС и задействан през 2018 година. Сега GDPR е подложен на широко обсъждане не само в Европа, а в целия свят – в него има твърде високи глоби ако регламентът му не се спазва ( в зависимост кой параграф на регламента е бил нарушен глобите достигат до двадесет милиона евро или 4% от годишния световен стокооборот на компанията). Освен това има и широка екстериториалност на прилагането - той трябва да бъде прилаган не само от страните членки на ЕС, но и от всички оператори от целия свят които обработват персонални данни на граждани на ЕС. Регламента делегира широк спектър от права на субектите носители на персонални данни в сравнение с други страни и бизнеси обработващи такъв тип информация. (примерно всеки гражданин може да изиска копие на данните за себе си които се пазят в дадена фирма и да изиска пълното им заличаване. Нещо повече GDPR изисква всеки оператор на персонални данни да назначава специално длъжностно лице data protection officer с пълномощия да следи за изпълнението на GDPR в съответната компания делегираща му широки пълномощия.

С голямо международна значимост при налагането на правни норми по отношение на личните данни е Конвенцията на Съвета на Европа за защита на частните лица по отношение на автоматизираната обработка на данни от личен характер от 1981 година ( ETS 108 влязла в сила на 1 октомври 1985 г.). през 2020 година започва преработка и допълнение на документа предвиждаща:

* По-строги изисквания към спазването на принципите на пропорционалност и минимизация, а също и на законността на обработката;
* Разширяване на списъка от данни, обработката на които изисква особени гаранции (биометрични, генетични данни и данни за етнически произход);
* Нови положения свързани с правата на лицата в случаите когато решението се взема на база алгоритмизирана обработка на данните с основна идея решението да не бъде вземано без да се вземе под внимание отношението на самия субект;
* Изискване да се внедри вграден алгоритъм за конфиденциалност - privacy-by-design;

Развивайки и допълвайки стандартите на Конвенция 108 спрямо конкретни технологии и жизнени сфери Съветът на Европа разработва „Ръководни принципи за защита на лицата във връзка с обработката на персонални данни в сферата на големите данни“[[14]](#footnote-14). В документа се отразява необходимостта от етично използване на данните, използването на алгоритъм за конфиденциалност, обезпечаване на анонимизация и систематично оценяване на рисковете за реидентификация на персоналните данни, дефиниране на ролята на човека при вземането на решения на база големи данни и пр. ако трябва да обобщим темата за защитата на персоналните данни е подробно разработена в рамките на общоевропейското право, но и допълнително прецизирано в националното право на всяка една от страните членки на ЕС.

**Американски модел.** В САЩ се отдава голямо значение на свободата на информацията, предприемачеството и безопасността на обществото. С тази аргументация правителството позволява по-голям достъп до персоналните данни от колкото в Европа. Неслучайно именно в САЩ се появяват информационни гиганти чиито бизнес се гради на обработката и анализа на данни.

В САЩ журналистическото лоби и неправителствените организации са особено силни, но въпреки това има голяма свобода в използването на данни. На федерално има редица отраслови актове за конфиденциалността и безопасността на данните, в това число актове по отношение на финансовите служби и здравеопазването и пр. Компаниите имат значително голяма свобода при използването на данни освен най-чувствителните. В различните щати има стотици разнообразни актове по защита на персоналните данни. Един от най-обсъжданите нови закони е този на Калифорния „ За защита на личния живот на потребителите“ (California Consumer Privacy Act, CCPA) който влиза в сила през 2020 година. Той се прилага в различни сектори на икономиката и предвижда значителен обем права върху субективните данни (включително правото за унищожаването на данни) като същевременно делегира редица задължения на компаниите при работа с данни, определени ограничения при обработката, използването и разкриването на персонални данни. Както и при Европейския GDPR, CCPA се използва в широк кръг компании регистрирани извън Калифорния.

**Китайски модел.** Отличителна черта е доминацията на интересите на Китайската комунистическа партия от една страна и държавата над интересите на гражданите от друга. Условията на новата цифрова икономика по отношение на данните се диктуват от държавата действаща в тандем с големите дата-компании. Обществените обсъждане тук има значително по-малка тежест. В държавната организационна система на Китай се приема за съвсем уместно и логично да има строг контрол по отношение на персоналните данни, тъй като бенифициент в случая е държавата, а не отделния гражданин.

Нормативно правното регулиране от страна на държавата е само едно от възможните средства за решаването на етичния казус. Другият са обществените организации и професионалните организации с задача да създадат етичен кодекс.

*Консълтинговата компания Accenture препоръчва на дата-аналитиците и всички останали които работят с данни да спазват общи принципи на дада-етика включващи:*

* *Уважението към човека стоящ зад данните е висш приоритет;*
* *Трябва да се осигури гарантирана приватност и безопасност на такова ниво на което би желал да ги види субекта на такива данни;*
* *Всички продукти и методи на изследванията трябва да бъдат съобразени със съответните вътрешни норми на компаниите и да са достъпни за проверка от вън.*

Acceture предлага общо 10 етични принципа спрямо големите данни насочени към спазване на гражданските права и обезпечаване на безопасността на данните[[15]](#footnote-15).

До колкото темата за големите данните е свързана с Изкуствения Интелект голяма част от препоръките за етичното им използване са систематизирани в етичен кодекс регулиращ ИИ и роботехниката и той се нарича „Асиломарски принципи на ИИ“ (Конфереция в Асиломар за ИИ)[[16]](#footnote-16). Неговата инициация е направена от Инженерния институт по електротехника и електроника (Institute of Electrical and Electronics Engineers, IEEE).

\*\*\*

Ако требва да обобщим етичните аспекти на регулирането на пазара на данни все още не е достатъчно утвърден – няма нито един документ на ниво международна авторитетна организация, който да е приет от всички страни. В перспектива ангажираността да се спазват някакви етични аспекти в работата с данни изглежда ниска и латентно генерира скрита дискриминация – автоматизираните системи за вземане на решения в здравеопазването, образованието и социалното подпомагане скоро неизбежно ще навлязат в живота ни. Изтичането на данните и грешките при вземането на решения поради некачествена инфраструктура, води до ниско качество на данните.

1. ISO/IEC 2382:2015(en) Information technology — Vocabulary // ISO. URL:https://www.iso.org/obp/ui/#iso:std:

   iso-iec:2382:ed-1:v1:en [↑](#footnote-ref-1)
2. Доклад на Генералния секретар на ООН “Използване на информационно-комуникационните технологии за инклузивно социално-икономическо развитие//Организация на Обединените НацииURL: https://undocs.org/bg/E/CN.16/2014/3 [↑](#footnote-ref-2)
3. Data Ethics Framework//Gov.uk. URL: https://www.gov.uk/government/publications/data-ethics-framework/

   data-ethics-framework [↑](#footnote-ref-3)
4. Nevo S. An Inside Look at Flood Forecasting // Google AI Blog. URL: https://ai.googleblog.com/2019/09/ an-inside-look-at-flood-forecasting.html; [↑](#footnote-ref-4)
5. Copeland R. Google’s ‘Project Nightingale’ Gathers Personal Health Data on Millions of Americans // The Wall Street Journal. URL:https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-

   data-on-millions-of-americans-11573496790; Murphy B. Google’s Project Nightingale Secretly Gathers Private

   Health Dataon Millions of Americans, Accordingtoa Report.Most Patients Have No Idea It’s Happening//Inc.

   URL: https://www.inc.com/bill-murphy-jr/googles-project-nightingale-secretly-gathers-private-health-data-on-

   millions-of-americans-according-to-a-report-most-patients-have-no-idea-its-happening.html [↑](#footnote-ref-5)
6. Frier S. Facebook Paid Contractors to Transcribe Users’ Audio Chats//Bloomberg. URL:https://www.bloomberg.com /news/articles/2019-08-13/facebook-paid-hundreds-of-contractors-to-transcribe-users-audio; Smith D. Microphone Gate:The world’s biggest tech companies were caught sending sensitive audio from customers to human contractors. Here’s where they stand now//Business Insider. URL:https://www.businessinsider.com/amazon-apple-google-

   microsoft-assistants-sent-audio-contractors-2019-8 [↑](#footnote-ref-6)
7. Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the

   protection of health-related data // Council of Europe.

   URL:https://search.coe.int/cm/pages/result\_details.aspx?objectid=090000168093b26e;Recommendation of the Council on OECD Legal Instruments Health Data Governance//OECD. URL:https://www.oecd.org/health/health-systems/Recommendation-of-OECD-Council-on-Health-Data-Governance-Booklet.pdf [↑](#footnote-ref-7)
8. Data Ethics Framework // Gov.uk. URL:https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework [↑](#footnote-ref-8)
9. European ethical Charter on the use of artifcial intelligence (AI) in judicial systems and their environment //Council of Europe. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>;

   CEPEJ European Ethical Charter on the use of artifcial intelligence (AI)in judicial systems and their environment // Council of Europe.

   URL: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artiʔcial-intelligence-ai-in-judicial-systems-and-theirenvironment#:~:text=Council%20of%20Europe%20adopts%20first,artificial%20intelligence%20in

   %20judicial%20systems&text=The%20Charter%20provides%20a%20framework,AI%20in%20national%20judicial%20processes [↑](#footnote-ref-9)
10. General principles for the use of Artifcial Intelligence in the fnancialsector// De Nederlandsche Bank.

    URL:https://www.dnb.nl/en/binaries/General%20principles%20for%20the%20use%20of%20Artificial%20Intelligence%20 in%20the%20ʔnancial%20sector2\_tcm47-385055.pdf [↑](#footnote-ref-10)
11. Microsoft AI principles// Microsoft. URL: https://www.microsoft.com/en-us/ai/our-approach-to-ai [↑](#footnote-ref-11)
12. Sweden has gotten its frst GDPR fine // Aigine. URL: https://aigine.se/en/sweden-has-gotten-its-first-gdpr-fine/gdpr/ [↑](#footnote-ref-12)
13. „Европейска конвенция за защита правата на човека и основните свободи“ и „Конвенция на Съвета на Европа за защита на физическите лица при автоматизирана обработка на персоналните данни „ [↑](#footnote-ref-13)
14. Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data.T-PD(2017)01.23 January2017//Directorate Generalof Human Rights and Rule of Law. URL:https://rm.coe.int/16806ebe7a [↑](#footnote-ref-14)
15. The Ethics of Data Sharing: A guide to best practices and governance // Accenture. URL: https://www.accenture.com/ \_acnmedia/PDF-35/Accenture-The-Ethics-of-Data-Sharing.pdf [↑](#footnote-ref-15)
16. Asilomar AI principles // Future of Life Institute. URL: https://futureoflife.org/ai-principles/?cn-reloaded=1; [↑](#footnote-ref-16)