



Брюксел, 10.1.2017 г.
COM(2017) 9 final

**СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА,
ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА
НА РЕГИОНИТЕ**

„ИЗГРАЖДАНЕ НА ОСНОВАНА НА ДАННИ ЕВРОПЕЙСКА ИКОНОМИКА“

{SWD(2017) 2 final}

„ИЗГРАЖДАНЕ НА ОСНОВАНА НА ДАННИ ЕВРОПЕЙСКА ИКОНОМИКА“

1. ВЪВЕДЕНИЕ

Данните се превърнаха в основен ресурс за икономически растеж, създаване на работни места и обществен напредък. С анализа на данни се улеснява оптимизирането на процесите и решенията, иновациите и предвиждането на бъдещи събития. В тази глобална тенденция се съдържа огромен потенциал за различни области — от здравето, околната среда, продоволствената сигурност, климата и ресурсната ефективност до енергетиката, интелигентните транспортни системи и интелигентните градове.

„Основаната на данни икономика“¹ се характеризира с екосистема от различни участници на пазара, като например производители, изследователи и доставчици на инфраструктура, които си сътрудничат, за да осигурят достъпността и използваемостта на данните. Това дава възможност на участниците на пазара да извличат стойност от данните чрез създаване на разнообразни приложения с голям потенциал за подобряване на ежедневието (напр. управление на трафика, оптимизиране на добивите и дистанционни здравни грижи).

Стойността на основаната на данни икономика на ЕС е оценена на 257 милиарда евро през 2014 г. или 1,85 % от БВП на ЕС². Цифрата е нараснала до 272 милиарда евро през 2015 г. или 1,87 % от БВП на ЕС (годишен ръст от 5,6 %). В същата оценка се прогнозира, че ако условията на политиката и правната рамка за основаната на данни икономика бъдат създадени навреме, до 2020 г. стойността ѝ ще се повиши до 643 милиарда евро, което ще представлява 3,17 % от общия БВП на ЕС.

По силата на Общия регламент относно защитата на данните (ОРЗД)³, от май 2018 г. ще се прилага единен набор от правила на европейско равнище вместо прилаганите понастоящем 28 национални законодателства. Новосъздаденият механизъм за „обслужване на едно гише“⁴ ще гарантира, че един орган по защита

¹ При основаната на данни икономика се измерва цялостното въздействие на пазара на данни — т.е. пазара, на който цифровите данни се търгуват като продукти или услуги, получени от необработени данни — върху икономиката като цяло. Това включва генериране, събиране, съхранение, обработка, разпределение, анализ, изготвяне, предоставяне и използване на данни, което е възможно благодарение на цифровите технологии (European Data Market study (*Проучване на европейския пазар на данни*), SMART 2013/0063, IDC, 2016 г.).

² Проучване на европейския пазар на данни, SMART 2013/0063, IDC, 2016 г.

³ Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ОВ L 119, 4.5.2016 г., стр. 1.

⁴ Член 56 от ОРЗД.

на данните („ОЗД“) ще отговаря за надзора на трансграничните операции по обработване на данни, извършвани от дружествата в рамките на ЕС. Ще бъде гарантирана последователност в тълкуването на новите правила. По-специално в трансграничните случаи, при които участват няколко национални ОЗД, ще бъде приемано само едно решение, за да се гарантира намирането на общи решения за общите проблеми. Освен това с ОРЗД се създават условия на равнопоставеност между европейските и чуждестранните дружества, тъй като дружествата, установени извън ЕС, ще трябва да прилагат същите правила като европейските дружества, ако предлагат стоки и услуги или наблюдение на поведението на лица в ЕС. Повишеното ниво на доверие от страна на потребителите ще бъде от полза както за ЕС, така и за външните търговски оператори.

Директивата за правото на неприкосновеност на личния живот и електронни комуникации се отнася до поверителността на електронните комуникационни услуги в ЕС. С преразгледаната Директива за правото на неприкосновеност на личния живот и електронни комуникации, предложена едновременно с настоящото съобщение под формата на регламент⁵, се цели да се гарантира високо ниво на защита при пълно спазване на ОРЗД. Със строгите правила за защита на данните се създава доверие, което ще даде възможност за развитие на основаната на данни икономика на международния пазар.

Както подчерта председателят Юнкер в речта си за състоянието на Европейския съюз на 14 септември 2016 г., „[д]а бъдеш европейец означава да имаш правото на защита на личните си данни със силни европейски закони. Европейците не желаят летящи над тях безпилотни летателни апарати да записват всяко тяхно действие, нито дружества, които да складира информация за всяко тяхно движение с мишката. Ето защо Парламентът, Съветът и Комисията се договориха през май тази година за общ европейски регламент за защита на данните. Това е силно европейско законодателство, което се прилага по отношение на дружествата, независимо от мястото им на установяване и мястото, където те обработват вашите данни. Това се прави, защото въпросите, свързани с неприкосновеността на личния живот, са от значение в Европа. Това е въпрос за човешко достойнство.“

В своето съобщение от 2012 г., озаглавено „Защитата на правото на личен живот във взаимосвързания свят — Европейска рамка за защита на данните за 21-ви век“⁶, и в съобщението си от 2014 г. „Към просперираща икономика, основана на данни“⁷, Комисията призна, че са необходими съвременни съгласувани норми в целия ЕС, за да могат данните да преминават безпрепятствено от една държава членка в друга, че Европейската цифрова икономика възприема бавно революцията в данните в сравнение със САЩ и че освен това ѝ липсва съпоставим промишлен капацитет. Прави се заключение, че липсата на пригодена към търговията с данни правна среда в ЕС може да доведе до недостатъчен достъп до големи масиви от данни, възможни пречки за навлизане на пазара пред нови участници и ефект на задущаване на иновациите.

⁵ COM (2017) 10.

⁶ COM (2012) 9.

⁷ COM (2014) 442.

С неоправдани **ограниченията на свободното движение на данни** може да се попречи на развитието на основаната на данни икономика на ЕС. Тези ограничения се отнасят до налагани от публичните органи изисквания относно местонахождението на данните с цел тяхното съхранение или обработка. Въпросът за свободното движение на данни се отнася до всички видове данни: предприятията и участниците в основаната на данни икономика боравят с лични или нелични промишлени и машинно генерирани данни, както и с данни, създадени в резултат на човешка дейност. В Стратегията за цифров единен пазар (ЦЕП) Комисията обяви, че ще предложи инициатива за свободно движение на данни, в рамките на която ще бъдат разгледани ограниченията на свободното движение на данни по причини, различни от тези за защита на личните данни в рамките на ЕС, и неоправданите ограничения относно местонахождението на данните с цел тяхното съхранение или обработка. Такива ограничения включват правни актове, приети от държавите членки, административни правила и практики със същото действие. Тенденцията е броят им да расте паралелно с развитието на основаната на данни икономика, като така да се създава несигурност относно това къде могат да се съхраняват и обработват данните. Това може да засегне всички сектори на икономиката, а също и организации както от частния, така и от общественния сектор, за които може да се окаже трудно да получат достъп до по-иновативни и/или по-евтини свързани с данни услуги. С неоправданите ограничения за местонахождението на данните се нарушава свободата на предоставяне на услуги и свободата на установяване, определени в Договора, като се влиза в противоречие и със съответното вторично право. По този начин има риск от фрагментиране на пазара, понижаване на качеството на услугите за потребителите и намаляване на конкурентоспособността на доставчиците на свързани с данни услуги, особено по-малките предприятия.

Неоправданото изискване за местонахождението на данните е също и част от дискусиите между ЕС и неговите търговски партньори, предвид нарастващото значение в глобалната икономика на данните и на свързаните с данни услуги и евентуалните нагласи на трети държави по този въпрос. В споразумение за свободна търговия правилата на ЕС за защита на данните не може да подлежат на преговори. Както е обяснено в Съобщението относно обмена и защитата на личните данни в един глобализиран свят⁸, диалогът относно защитата на данните и преговорите с трети държави трябва да се водят отделно. Освен това, както се посочва в съобщението „Търговията — за всички“⁹, Комисията ще се стреми да използва търговските споразумения, за да се установят правила за електронната търговия и трансграничните потоци от данни, както и за да се отстраняват новите форми на цифров протекционизъм, като се действа при пълно спазване и ненакърняване на разпоредбите на ЕС за защита на данните.

Освен това, с обхващането на икономиката и обществото от основаната на данни промяна, все по-големи количества данни се генерират от машини или процеси въз основа на нововъзникващи технологии, като например „интернет на нещата“, фабриките на бъдещето и автономните свързани системи. Със самата свързаност се променя начинът, по който може да се получи достъп до данните: все повече

⁸ COM (2017) 7.

⁹ COM (2015) 497.

данните, до които достъпът обикновено е ставал чрез физически връзки, сега вече могат да са достъпни дистанционно. Огромното разнообразие от източници и видове данни, както и богатите възможности за прилагане на познанията от тези данни в множество области, включително разработването на публични политики, тепърва започват да се развиват. За да се възползват от тези възможности, както публичните, така и частните участници на пазара на данни се нуждаят от достъп до големи и разнообразни масиви от данни. Следователно въпросите за достъпа и предаването по отношение на генерираните от тези машини и процеси данни са основни за възникването на основана на данни икономика и изискват внимателна оценка.

Други нововъзникващи проблеми засягат прилагането на правила относно отговорността за вреди, произтичащи от неизправност в свързано устройство или робот, а също и преносимостта и оперативната съвместимост на данните. В контекста на такива нови технологии като „интернет на нещата“ или роботиката съществуват комплексни и сложни взаимозависимости както между продуктите (на базата на хардуер и софтуер), така и между свързаните помежду си устройства. Нещо повече, могат да възникнат нови проблеми, свързани с автономните машини, чието неочаквано и непредвидено поведение би могло да причини вреди на хора и вещи. Тези явления може да създадат правна несигурност по отношение на прилагането на съществуващата рамка относно отговорността и безопасността.

Както е обявено в ЦЕП, целта на Комисията е да се създаде ясна и адаптирана политика и правна рамка за основаната на данни икономика, като се премахнат оставащите бариери пред движението на данни и се намери начин за справяне с правната несигурност, създавана от новите технологии за данни. Други цели, залегнали в съобщението, са насочени към увеличаване на наличието и използването на данни, насърчаване на нови основи на данни бизнес модели, както и подобряване на условията за достъп до данни и анализа на данни в ЕС. За тази цел Комисията представя целенасочени въпроси за обсъждане с оглед „Изграждане на основана на данни европейска икономика“.

В настоящото съобщение се разглеждат съответно следните въпроси: свободно движение на данни; достъп до и предаване на машинно генерирани данни; отговорност и безопасност в контекста на нововъзникващите технологии; преносимост на нелични данни, оперативна съвместимост и стандарти. В това съобщение се дават също и предложения за експериментиране с общи регулаторни решения в реална среда.

Комисията започва широк диалог със заинтересованите страни по разгледаните в съобщението въпроси. Първата стъпка от този диалог е обществена консултация, започната едновременно с пакета за основаната на данни икономика¹⁰.

2. СВОБОДНО ДВИЖЕНИЕ НА ДАННИ

За една добре функционираща и динамична основана на данни икономика се изисква движението на данни на вътрешния пазар да бъде разрешено и защитено. В

¹⁰ <https://ec.europa.eu/digital-single-market/news-redirect/52039>

бързо развиващ се технологичен контекст безопасното и надеждно свободно движение на данни е важно средство за защитата на четирите основни свободи на единния пазар на ЕС, залегнали в Договорите (стоки, работници, предоставяне на услуги и капитал). Свързаните с данни услуги се развиват бързо в ЕС и в целия свят. С ефективен и освободен от бариери единен пазар в този сектор ще се създадат значителни възможности за допълнителен растеж и работни места.

Растежът и иновациите в основаната на данни икономика, както и изпълнението на трансгранични обществени услуги могат да бъдат застрашени от бариери пред свободното движение на данни в ЕС, като например неоправдани изисквания за местонахождението на данните, налагани от публичните органи. С мерките за местонахождението на данните на практика се въвежда отново цифров „граничен контрол“¹¹. Те варират от изисквания от страна на надзорните органи доставчиците на финансови услуги да съхраняват данните си локално до прилагане на правила за професионална тайна, което предполага локално съхранение и обработка на данни, и премахване на регламентирането, което изисква локално съхранение на архивирана информация, генерирана от обществения сектор, независимо от степента ѝ на чувствителност.

Безпокойството за неприкосновеността е основателно, но не следва да се използва от публичните органи като причина за неоправдано ограничаване на свободното движение на данни. Както бе посочено по-горе, с ОРЗД се предоставя единен набор от правила с високо ниво на защита на данните за целия ЕС. С него се укрепва доверието на потребителя в онлайн услугите и се гарантира еднакво прилагане на правилата във всички държави членки чрез по-силни национални органи за защита на данните. С ОРЗД се насърчава необходимото доверие за обработката на данни и това е основата за свободното движение на лични данни в ЕС. В ОРЗД се забраняват ограниченията за свободното движение на лични данни в рамките на Съюза, когато такива ограничения се основават на причини, свързани със защитата на личните данни¹². В ОРЗД не са обхванати обаче ограничения по причини, различни от защитата на личните данни, например съгласно данъчното или счетоводното право. Освен това неличните данни, т.е. данните, които не са свързани с идентифицирано или подлежащо на идентификация физическо лице¹³, остават извън приложното поле на ОРЗД и могат да се отнасят например до нелични машинно генерирани данни.

Ограничения по отношение на местонахождението на данните може да възникнат от правни норми или административни насоки или практики, които изискват

¹¹ ОИСР, „Emerging Policy Issues: Localisation Barriers to Trade“ (*Възникващи въпроси на политиката: свързани с местонахождението бариери пред търговията*), 2015 г. и текуща работа.

¹² Член 1, параграф 3. Например динамичният IP адрес, регистриран от онлайн доставчик на медийни услуги, когато дадено лице получава достъп до уебсайт, който доставчикът прави достъпен за обществеността, ще се счита за лични данни по отношение на този доставчик, ако последният разполага с правни средства, позволяващи му да идентифицира физическото лице, за което се отнасят данните, с допълнителни данни, с които доставчикът на интернет услуги разполага за това лице. Вж. Решение по дело C-582/14, Breyer, EU:C:2016:779, точка 49.

¹³ Съгласно определението в член 4, параграф 1 от ОРЗД.

съхранението и обработката на данни¹⁴ в електронен формат¹⁵ да бъде ограничено до конкретна географска зона или юрисдикция. Понякога ограничения се налагат от държавите членки, като се счита, че надзорните органи могат по-лесно да контролират данните на местно равнище. Местонахождението се използва също и като израз на гаранции по отношение на неприкосновеността, проверката и прилагането на закона, както и на сигурност на данните. На практика обаче тези мерки рядко спомагат за целите, за чието постигане са предназначени.

Освен от мястото, където данните се съхраняват физически, сигурността на информацията зависи от множество фактори, като например поддържането на тяхната поверителност и ненарушимост, когато данните са на разположение извън съоръжението за съхранение. В тази връзка действителните инструменти, които дават възможност за сигурно съхранение и обработка на данни, са не толкова ограниченията по отношение на местонахождението на данните, а авангардните най-добри практики за управление в областта на ИКТ с много по-голям мащаб от индивидуалните системи. Например, за да се предпазят данните от местни природни бедствия или кибератаки, разположените в различни държави членки съоръжения за съхранение може да служат като резервни копия едно на друго и да се използват техническите и организационните мерки, предвидени в Директивата относно сигурността на мрежите и информационните системи¹⁶. Освен това наличието на данни за целите на регламентирането и надзора, което по никакъв начин не се поставя под съмнение, би било гарантирано по-добре чрез засилване на сътрудничеството между националните органи или между такива органи и частния сектор, отколкото чрез ограничения за местонахождението. Действително, в област, която се характеризира с тясно сътрудничество между надзорните органи, например финансовите услуги, изискванията за местонахождението на данните може да се окажат контрапродуктивни¹⁷.

Изискванията за местонахождението на данните биха могли обаче да са основателни и пропорционални в определен контекст или по отношение на определени данни, особено преди да са влезли в сила ефективни споразумения за трансгранично сътрудничество, какъвто е например случаят с гарантирането на сигурна обработка на определени данни, отнасящи се до критична енергийна инфраструктура, или наличието на електронно доказателство (напр. като локализираните копия на масиви от данни) за правоприлагащите органи, или локалното съхранение на данни, които се намират в определени публични регистри.

¹⁴ За данни както частно, така и публично притежание.

¹⁵ Включително копия на масиви от данни.

¹⁶ Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).

¹⁷ В множество разпоредби на ЕС по отношение на финансовите услуги и Европейската система за финансов надзор се изисква надзорните органи да имат достъп до данни за финансовите институции и сделки навсякъде на територията на ЕС. Изискванията данните да се съхраняват на конкретна национална територия или които обвързват достъпа за надзор с административни процедури, биха могли да намалят достъпа на надзорните органи до данни, които са от съществено значение за изпълнението на техните правомощия.

За съжаление тенденцията както в света, така и в Европа е към все по-засилено локализиране на данните — подход, който често се основава на погрешното схващане, че локализираните услуги по презумпция са по-сигурни от трансграничните. Освен това пазарът на свързани с данни услуги е повлиян значително от липсата на прозрачни правила и от силното усещане за необходимост от локализиране на данните. Това може да ограничи достъпа на предприятията и на организациите от обществения сектор до по-евтини и по-иновативни свързани с данни услуги или да принуди предприятията, които осъществяват трансгранична дейност, да осигуряват излишни възможности за съхранение и обработка на данни. Това би могло също така да попречи на основаните на данни предприятия, по-специално стартиращите и МСП, да разширят дейностите си, да навлязат на нови пазари (напр. като трябва да инвестират в центрове за обработка на данни в 28 държави членки) или да съсредоточат информационния и аналитичния си капацитет за разработване на нови продукти и услуги.

Понастоящем в Европа 84 % от крайното търсене на „свързани с ИКТ“ услуги (консултации, хостинг, разработване) се задоволява вътре в рамките на ЕС. Ако тези услуги биха могли да действат по-лесно и през границите на ЕС чрез премахване на изискванията за местонахождението на данните, това би довело до годишна печалба за БВП до 8 милиарда евро като спестени разходи и печалба от ефективност¹⁸.

Местонахождението на данните пречи също и на по-широкото въвеждане на съхранението и изчисленията „в облак“. Това би могло да има и по-широко обществено въздействие. Действително, по-ефективното използване на ИКТ ресурсите би могло да допринесе за намаляването на потреблението на енергия и на въглеродните емисии нетно с 30 % или повече. Преместването на едно малко предприятие „в облак“ би могло да намали потреблението на енергия и въглеродните емисии с повече от 90 %, като приложенията му работят „в облак“ вместо същите тези приложения да работят в собствена инфраструктура на предприятието. Очаква се до края на 2020 г. световният пазар на енергийноефективни центрове за обработка на данни да се разрасне до почти 90 милиарда евро. Един фрагментиран пазар на свързаните с данни услуги би попречил на пълното разгръщане на тези енергийноефективни услуги в ЕС, а също така ще изложи на риск готовността за инвестиране.

За преодоляване на очертаните по-горе проблеми и ограничения и за реализиране на пълния потенциал на основаната на данни европейска икономика, всяко действие на държавите членки, което засяга съхранението или обработката на данни, следва да се ръководи от **„принципа на свободно движение на данни в ЕС“** като естествено следствие от техните задължения съгласно разпоредбите за свободно движение на услуги и свободно установяване, съдържащи се в Договора и в съответното вторично законодателство. Всички настоящи или нови изисквания за местонахождението на данните ще трябва да бъдат внимателно обосновани съгласно Договора и съответното вторично право, за да се провери дали са

¹⁸ „Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States“ (*Отприщване на вътрешните потоци от данни в ЕС: икономическа оценка на мерките за местонахождението на данните в държавите — членки на ЕС*), ECIPE, 2016 г., изчисление въз основа на нарасналия конкурентен натиск при напълно прозрачен по отношение на цената „промишлен“ ЦЕП.

необходими и пропорционални за постигане на императивна цел от общ интерес, като например обществената сигурност¹⁹.

Принципът на свободно движение на лични данни²⁰, заложен в първичното и вторичното право, следва да се прилага също в случаите, когато ОРЗД предоставя възможност на държавите членки да регламентират специфични въпроси. Държавите членки следва да се насърчават да не използват отворените клаузи в ОРЗД за допълнително ограничаване на свободното движение на данни.

В заключенията си от 15 декември 2016 г. Европейският съвет призова за премахване на оставащите препятствия в рамките на единния пазар, включително тези, които пречат на свободното движение на данни²¹.

За прилагане на принципа на свободно движение на данни Комисията ще предприеме следните две стъпки:

- След публикуване на настоящото съобщение Комисията ще започне структурирани диалози с държавите членки и други заинтересовани страни относно основанията за и пропорционалността на мерките за местонахождението на данните, като за отправна точка вземе идентифицираните досега от Комисията ограничения.
- След като получи резултатите от диалозите и допълнителното събиране на факти относно обхвата и естеството на ограниченията за локализиране на данните и тяхното въздействие, по-специално върху МСП и стартиращите предприятия, наред с другото, чрез съпътстваща обществена консултация, ако е необходимо, Комисията ще започне производства за установяване на неизпълнение на задължения, за да се разгледат неоправдани или непропорционални мерки във връзка с местонахождението на данните, и при нужда може да предприеме други инициативи във връзка със свободното движение на данни. В този контекст всяко последващо действие ще бъде предприето в съответствие с принципите за по-добро регулиране.

3. ДОСТЪП ДО ДАННИ И ПРЕДАВАНЕ НА ДАННИ

Все по-големи количества данни се генерират от машини или процеси въз основа на нововъзникващи технологии, като например „интернет на нещата“. Тези данни

¹⁹ Като се взема предвид, че изключенията съгласно Договора следва да се тълкуват ограничително. Такова вторично законодателство включва ОРЗД, Директива 2000/31/ЕО (Директивата за електронната търговия), Директива 2006/123/ЕО (Директивата за услугите), а по-отношение на проекта за техническите регламенти и проекта на правила относно услугите на информационното общество — Директива 2015/1535 (Директивата за прозрачността).

²⁰ Свободното движение на лични данни е обхванато от член 16 от Договора за функционирането на Европейския съюз, а правилата за свободното движение на лични данни се определят в настоящото и бъдещото законодателство на ЕС относно защитата на данни. Член 1, параграф 3 от Общия регламент относно защитата на данните предвижда: „Свободното движение на лични данни в рамките на Съюза не се ограничава, нито се забранява по причини, свързани със защитата на физическите лица във връзка с обработването на лични данни.“

²¹ <http://www.consilium.europa.eu/eu/en/press-releases/2016/12/15-euro-conclusions-final/>

все повече се използват като основен компонент за нови, иновативни услуги, за да се подобрят продуктите или производственият процес и да се подкрепи вземането на решения.

Разнообразието на генерираните от тези машини и процеси данни предоставя богати възможности за участниците на пазара на данни да прилагат иновации и да използват информацията, извлечена от данните. Например данните, получени от датчиците, използвани в модерните земеделски стопанства, биха могли да се използват за създаване на приложение за оптимизиране на добивите, а данните, получени от датчиците в светофарите, биха могли да се използват за създаване на приложение за управление на трафика или за оптимизиране на маршрутите.

За извличане на максимална стойност от този вид данни участниците на пазара трябва да имат достъп до големи и разнообразни масиви от данни. Това обаче става по-трудно постижимо, ако тези, които генерират данните, ги запазват за себе си и впоследствие те се анализират в т. нар. „силози“ (изолирани системи). Следователно въпросите за достъпа и предаването по отношение на необработените данни (т.е. данни, които не са били обработвани или променени след записването), генерирани от тези машини и процеси, са основни за възникването на основана на данни икономика и изискват внимателна оценка.

Въпросът за достъпа до машинно генерирани данни понастоящем се разглежда в няколко сектора, като например транспорт, енергийни пазари, интелигентни условия на живот, както и в сектора на здравеопазването и грижите.

Преди да се разгледа настоящата ситуация по отношение на достъпа до данни в ЕС е важно да се изясни видът на данните, които се разглеждат в този контекст.

3.1. Вид на разглежданите данни

По принцип данните могат да бъдат лични и нелични. Например данните, генерирани от домашни температурни датчици, може да бъдат лични по своето естество, ако могат да бъдат свързани с живеещо там лице, докато данните за влажност на почвата не са лични. Личните данни могат да бъдат преобразувани в нелични чрез процес на анонимизиране. Когато данните се квалифицират като лични²², ще се прилага рамката за защита на данните, по-специално ОРЗД.

Машинно генерираните данни се създават без пряката намеса на човек, с помощта на компютърни процеси, приложения или услуги, или от датчици, с които се обработва информация от оборудване, софтуер или машини, били те виртуални или реални.

Машинно генерираните данни могат да бъдат от лично или нелично естество. Когато машинно генерирани данни дават възможност за идентифициране на физическо лице, те се квалифицират като лични данни, като последицата от това е, че за тях се прилагат всички правила относно личните данни докато не бъдат напълно анонимизирани (напр. данни за местонахождение от мобилни приложения).

²² Съгласно определението в член 4, параграф 1 от ОРЗД.

Една често срещана тема, при която свободното движение на данни се свързва с нововъзникващите проблеми с достъпа и предаването на данни, е че предприятията и участниците в основаната на данни икономика ще боравят както с лични, така и с нелични данни, и че потоците и масивите от данни редовно ще съдържат и двата вида. Всяка мярка на политиката трябва да взема предвид тази икономическа реалност и правната рамка относно защитата на личните данни, като същевременно се спазват основните права на лицата.

3.2. Ограничен достъп до данни

За оценяване на този нововъзникващ проблем най-напред е необходимо да се направи анализ на това как дружествата и другите участници на пазара могат да получат достъп до големи и разнообразни масиви от данни, които са необходими в основаната на данни икономика.

От наличната информация²³ става ясно, че дружествата, които притежават големи количества данни, обикновено са склонни да използват главно собствени възможности за анализ на данни. В повечето случаи данните се генерират и анализират от едно и също дружество, а дори и когато анализът на данните се възлага на подизпълнител, може да няма по-нататъшно използване на същите. Освен това в някои случаи производители, дружества, които предлагат услуги, или други участници на пазара, които притежават данни, запазват генерираните от техните машини или чрез техните продукти и услуги данни за себе си, като по този начин потенциално ограничават повторната употреба надолу по веригата на пазарите. Много дружества не се възползват от или не дават възможност за приложни програмни интерфейси (ППИ)²⁴ (които определят как следва да си взаимодействат различните приложения), които могат да служат като безопасни входни портове за нова и иновативна употреба на притежаваните от дружествата данни.

Поради това като цяло обменът на информация остава ограничен. Бавно се зараждат пазари на данни, но те не са широко използвани. Дружествата може да не разполагат с подходящите инструменти и умения за количествено определяне на икономическата стойност на техните данни и може да се страхуват, че ще загубят или намалят конкурентното си предимство, ако данните станат достъпни за конкуренти.

23 IDC, Проучване на европейския пазар на данни, първи междинен доклад, 2016 г.; Подкрепящо проучване за оценка на въздействието относно нововъзникващи проблеми за собствеността, оперативната съвместимост, употребата (повторната употреба) и достъпа до данни, и за отговорността, първи междинен доклад, 2016 г.; Конференция на високо равнище на ГД „Съобщителни мрежи, съдържание и технологии“, 17 октомври 2016 г.

24 Например <https://developer.lufthansa.com/>; <https://data.sncf.com/api>; <https://api.tfl.gov.uk/>; <https://dev.blablacar.com/>

3.3. Необработени машинно генерирани данни: състояние на правната уредба на равнището на ЕС и на национално равнище

Необработените машинно генерирани данни не са защитени от действащите права върху интелектуалната собственост, тъй като се счита, че те не са резултат от интелектуално усилие и/или че нямат никаква степен на оригиналност. Особеното право (*sui generis*) съгласно Директивата за базите данни (96/9/ЕО), с което на производителите на бази данни се дава правото да не се допуска извличане и/или повторно използване на цялата или на съществена част от съдържанието на база данни, може да предостави защита само при условие, че създаването на такава база данни включва съществена инвестиция за придобиването, проверката или оформлението на нейното съдържание. С приетата наскоро Директива относно защитата на търговски тайни (2016/943/ЕС), която следва да се транспонира в националното право до юни 2018 г., ще се гарантира защита на търговските тайни срещу тяхното незаконно придобиване, използване и разкриване. За да бъдат квалифицирани данни като „търговска тайна“, трябва да са взети мерки за защита на секретността на информацията, която представлява „интелектуалния капитал на дружеството“

Според законодателството на различни държави членки може да има правни претенции по отношение на данни само ако те отговарят на специфични условия за квалифицирането им като например право върху интелектуална собственост, право върху база данни или търговска тайна. На равнището на ЕС обаче необработените машинно генерирани данни сами по себе си по принцип не биха отговаряли на необходимите условия.

Следователно в момента няма всеобхватни рамки на политиката на национално равнище или на равнището на Съюза по отношение на необработените машинно генерирани данни, които не могат да бъдат квалифицирани като лични, или относно условията за тяхната икономическа експлоатация и търгуване. Въпросът е оставен до голяма степен на договорни решения. Използването на наличните в Съюза инструменти на съществуващото общо договорно право и конкурентно право може да е достатъчно за справяне с този проблем. Допълнително може да се предвидят и доброволни или рамкови споразумения за обхващане на определени сектори. Въпреки това, когато възможностите за преговаряне на различните участници на пазара са неравностойни, базираните на пазара решения сами по себе си може да не гарантират в достатъчна степен справедливи и благоприятни за иновациите резултати, подпомагане на лесния достъп за нови участници на пазара и избягване на ситуации на обвързване.

3.4. Действително състояние

В някои случаи производителите или доставчиците на услуги може да станат фактически „собственици“ на данните, които се генерират от техните машини и процеси, дори и когато машините са собственост на потребителя. Фактическият контрол над данните може да бъде източник на отличаване или конкурентно предимство за производителите. Това обаче може да бъде проблематично, защото производителят често не допуска потребителят да разреши използването на данните от друга страна.

Следователно различните участници на пазара, които имат контрол над данните, може в зависимост от спецификите на пазарите да се възползват от пропуските в регулаторната рамка или от описаната по-горе правна несигурност, като налагат на потребителите неравноправни стандартни договорни условия или чрез такива технически средства като защитени формати или криптиране. Макар няколко държави членки да са разширили приложното поле на Директивата за защита на потребителите от неравноправните договорни клаузи, за да се обхванат и сделките между предприятия, това не е направено от всички. Така би могло да се стигне например до обвързване на потребители и предприятия със споразумения за изключително използване на данните. Може да се постигне доброволно споделяне на данни, но договарянето на такива споразумения би могло да доведе до съществени разходи по сделката за по-слабите страни поради неравностойната им позиция за преговаряне или до съществени разходи за наемане на правни експерти.

3.5. Бъдеща рамка на ЕС за достъп до данни

Гарантирането на достъп до машинно генерирани данни в момента се проучва от някои държави членки, които може да решат да регламентират сами този въпрос. Един некоординиран подход води до риск от фрагментиране и би бил във вреда на развитието на основаната на данни икономика на ЕС и свързаните с данни трансгранични услуги и технологии на вътрешния пазар.

Комисията съответно има намерение да започне диалог с държавите членки и други заинтересовани страни за проучване на евентуална бъдеща рамка на ЕС за достъп до данни. По мнение на Комисията този диалог следва да е съсредоточен около най-ефективните начини за постигане на следните цели:

- **Подобряване на достъпа до анонимни машинно генерирани данни:** Чрез споделяне, повторно използване и обединяване машинно генерираните данни се превръщат в източник за създаване на стойност, иновации и разнообразие на бизнес модели²⁵.
- **Улесняване и стимулиране на споделянето на такива данни:** Всяко бъдещо решение следва да насърчава ефективния достъп до данни, като се вземат предвид например евентуалните различия във възможностите за преговаряне на участниците на пазара.
- **Защита на инвестициите и активите:** При всяко бъдещо решение трябва да се вземе предвид също и законният интерес на участниците на пазара, които инвестират в развитието на продукт, да гарантират справедлива възвръщаемост на инвестициите си и по този начин да се допринася за иновации. Същевременно с всяко бъдещо решение следва да се гарантира справедливо споделяне на печалбите между притежателите на данни²⁶, обработващите данни и предоставящите приложение по веригите на създаване на стойност.

²⁵ Когато става въпрос за лични данни, се прилага ОРЗД.

²⁶ Субектът, който на практика управлява и задържа машинно генерираните данни.

- **Избягване на разкриването на поверителни данни:** С всяко бъдещо решение следва да се намаляват рисковете от разкриване на поверителни данни, по-специално пред съществуващи или потенциални конкуренти. В тази връзка с него трябва също така да се дава възможност за извършване на правилна класификация на данните преди да се преценява дали определена част от тях може или не може да бъде споделяна.
- **Свеждане до минимум на ефектите на обвързване:** Следва да се вземат предвид неравностойните възможности за преговаряне на дружествата и частните лица. Следва да се избягват ситуации на обвързване, особено за МСП и за стартиращи предприятия и частни лица.

По време на диалозите със заинтересованите страни Комисията възнамерява да обсъди следните възможности за справяне с въпроса за достъпа до машинно генерирани данни, като те се различават по равнището на интервенция:

- **Насоки за стимулиране на предприятията да споделят данни:** За смекчаване на въздействието от различните национални нормативни уредби и за предоставяне на повишена правна сигурност за дружествата, Комисията би могла да издаде насоки как следва да се подхожда в договори по отношение на правото за контрол на нелични данни. Насоките биха се основавали върху съществуващото законодателство, по-специално изискванията за прозрачност и справедливост, определени в правото на ЕС относно предлагането на пазара и защитата на потребителите, Директивата за търговските тайни и законодателството за авторското право, по-специално Директивата за базите данни. Комисията възнамерява да започне през 2017 г. оценка на Директивата за базите данни.
- **Насърчаване на разработването на технически решения за надеждна идентификация и обмен на данни:** Проследимостта и ясната идентификация на източниците на данни са предварителни условия за действителен контрол на данните на пазара. Определянето на надеждни и по възможност стандартизирани протоколи за постоянна идентификация на източниците на данни може да се окаже необходимо за създаване на доверие в системата. Приложните програмни интерфейси (ППИ) също могат да ускорят създаването на екосистема от разработващи приложения и алгоритми, които проявяват интерес към притежаваните от дружествата данни. ППИ могат да помогнат на фирмите и на публичните органи да определят и да се възползват от различни видове повторна употреба на данните, които притежават. На тази база би могло да се обсъди по-широка употреба на отворени, стандартизирани и добре документирани ППИ посредством технически насоки, включително установяване и разпространение на най-добри практики за дружествата и публичните органи. Това може да включва предлагане на разположение на данни в машинночитаеми формати и предоставянето на свързаните с тях метаданни.
- **Договорни правила по подразбиране:** Правилата по подразбиране биха могли да описват еталонен балансиран вариант за свързани с данни договори, като се вземе надлежно предвид осъществяваната в момента проверка за пригодност на цялостното функциониране на Директивата относно неравноправните клаузи в потребителските договори. Те може да се

съчетаят с въвеждане на контрол върху неравноправния характер на договорните отношения между предприятията²⁷, което би довело до обезсилване на договорни клаузи, които се отклоняват прекомерно от правилата по подразбиране. Тези правила може да се допълнят също така и с набор от препоръчителни стандартни договорни условия, изготвени от заинтересованите страни. С такъв подход би могло да се ограничат правните бариери пред малките предприятия и да се намали дисбалансът в позициите при преговори, като същевременно се запази висока степен на свобода на договаряне.

- **Достъп в обществен интерес и за научни цели:** На публичните органи би могло да се осигури достъп до данни, когато това е от „общ интерес“ и би подобрило значително работата на обществения сектор, например достъп за статистическите служби до бизнес данни или оптимизиране на системите за управление на трафика въз основа на данни в реално време от частни превозни средства. Достъпът на статистическите служби до бизнес данни по принцип би допринесъл за облекчаване на тежестта за икономическите оператори от статистическата отчетност. По подобен начин и достъпът до и възможността за комбиниране на данни от различни източници е от решаващо значение за научните изследвания в такива области като медицината, социалните и природните науки.
- **Права на производителя на данни:** На „производителя на данни“, т.е. притежателя или дългосрочния ползвател (т.е. наемател) на устройството, може да се гарантира право на използване и разрешаване на използването на нелични данни. Този подход би имал за цел изясняване на правната ситуация и даване на по-голям избор на производителя на данни чрез откриване на възможност за ползвателите да използват своите данни и следователно да допринасят за деблокирането на машинно генерирани данни. Трябва обаче ясно да се определят съответните изключения, по-специално разпоредбата за неизключителен достъп до данните от страна на производителя или на публичните органи, например за управление на трафика или по екологични съображения. Що се отнася до личните данни, всяко лице ще запази правото си да оттегли съгласието си във всеки момент след като е дало разрешение за използване. Личните данни ще трябва да се анонимизират по такъв начин, че лицето да не може повече да бъде идентифицирано, преди по-нататъшното им използване да може да се разрешава от другата страна. Всъщност ОРЗД продължава да се прилага за всички лични данни (независимо дали са машинно генерирани или по друг начин) докато те не бъдат анонимизирани.
- **Достъп срещу възнаграждение:** За притежателите на данни, като например производители, доставчици на услуги или други страни, би могло да се разработи рамка, която евентуално да се основава на определени основни принципи като справедливи, приемливи и недискриминационни (FRAND) условия, за да се осигури достъп срещу възнаграждение до данните, които

²⁷. Еталонът за степента на неравноправност в отношенията между предприятия очевидно ще трябва да бъде различен от този при договорите между предприятия и потребители, за да се отрази по-високата степен на свобода на договаряне в отношенията между предприятия.

притежават, след тяхното анонимизиране. Ще трябва да се вземат предвид съответните законни интереси, както и необходимостта от защита на търговските тайни. Биха могли също така да бъдат предвидени различни режими на достъп за различните сектори и/или бизнес модели, за да се вземат под внимание особеностите на всеки сектор. Например в някои случаи отвореният достъп до данни (пълен или частичен) би могъл да бъде предпочитаният избор както за предприятията, така и за обществото.

Комисията ще проведе консултации със заинтересованите страни по очертаните по-горе въпроси, за да се съберат повече факти от сектора за функционирането на пазарите на данни и да се проучат възможни решения. В този контекст от съществено значение е широко обсъждане на макро равнище, за да се разискват възможните решения и да се избегнат нежеланите странични ефекти, които биха задушили иновациите или възпрепятствали конкуренцията. В допълнение ще се проведат и конкретни за всеки сектор дискусии със съответните заинтересовани страни по веригата на създаване на стойност от данните.

4. ОТГОВОРНОСТ

Друг нововъзникващ проблем е прилагането в основаната на данни икономика на настоящите правила относно отговорността по отношение на продукти и услуги, основани на нововъзникващи технологии, като например „интернет на нещата“, фабриките на бъдещето и автономните свързани системи. „Интернет на нещата“ е бързо развиваща се мрежа от ежедневни вещи като часовници, автомобили и термостати, които са свързани към интернет. Автономните свързани системи, като например „автомобили без шофьор“, действат независимо от човека и са способни да разбират и тълкуват обкръжаващата ги среда. При тези нововъзникващи технологии се използват датчици за предоставяне на многото видове данни, които често се изискват за работата на продукта или услугата.

Всички тези иновации може да спомогнат за по-безопасен и качествен живот, но неизменно за всяко устройство остава и възможността от грешки при проектирането, неизправности или манипулация. Това може да е резултат от предаването от някой датчик на грешни данни, например поради дефект в софтуера, проблеми със свързването или неправилна работа на машината. Естеството на тези системи означава, че може да се окаже трудно установяването на точния източник на проблема, който води до вреди, с което се повдига въпросът как да се гарантира, че системите са безопасни за ползвателите, така че да се сведе до минимум възникването на вреди, както и кой следва да носи отговорността за вредата, ако такава възникне.

Поради това въпросът как да се осигури сигурност едновременно за ползвателите и за производителите на такива устройства по отношение на евентуалната им отговорност е от основно значение за възникването на основана на данни икономика.

4.1. Правила на ЕС относно отговорността

В гражданското право обикновено се различават два вида правна отговорност: договорна, когато отговорността за вреди произтича от договорни отношения

между страните и извъндоговорна²⁸, когато отговорността е определена в разпоредби, различни от договорните. Важен вид извъндоговорна отговорност е този, който се отнася за отговорността за дефектни продукти. На равнището на ЕС, с Директивата относно отговорността за вреди, причинени от дефект на стока (85/374/ЕИО) („Директива относно отговорността за продукти“) се определя принципът на стриктна отговорност, т.е. производителите може да са отговорни дори и без проявена небрежност или вина от тяхна страна. Може да се окаже трудно или неясно как да се прилагат разпоредбите на тази директива²⁹ в контекста на „интернет на нещата“ и на автономните свързани системи (напр. роботизирани) поради следните причини: характеристиките на системите, например сложен продукт или верига на създаване на стойност на услугата, с взаимозависимост между доставчици, производители и други трети страни; несигурността по отношение на правния характер на устройствата от „интернет на нещата“, т.е. дали са продукти, услуги или продукти, които се доставят с продажбата на дадена услуга; както и автономния характер на тези технологии.

Комисията започна широкообхватна оценка на Директивата относно отговорността за продукти, за да се оцени цялостното ѝ функциониране и дали нейните правила, разработени за много различна среда, остават подходящи за такива нововъзникващи технологии като „интернет на нещата“ и автономните свързани системи.

4.2. Възможни пътища напред

Целта на Комисията е да се увеличи правната сигурност по отношение на отговорността в контекста на нововъзникващите технологии и така да се създадат благоприятни условия за иновации. Освен съществуващото положение³⁰, могат да се проучат различни подходи, включително:

- **Подходи за създаване на риск или за управление на риска:** При тези подходи отговорността може да се припише на участниците на пазара, които създават най-голям риск за другите, или на онези участници на пазара, които са в най-добра позиция да сведат до минимум или да избегнат възникването на такъв риск.
- **Доброволни или задължителни схеми за застраховане:** Такива схеми може да са съчетани с горепосочените подходи към отговорността. При тях ще се дава обезщетение на страните, понесли вредата (напр. потребителя). При този подход ще трябва да се осигури правна защита на направените от предприятието инвестиции, като същевременно се даде увереност на

²⁸ Правилата на ЕС относно отговорността се отнасят единствено до извъндоговорната отговорност.

²⁹ Позовавания на стриктната отговорност на производителите в случай на дефектни продукти се правят и в други части от законодателството относно безопасността на продуктите, като например Директивата за радиосъоръженията (2014/53/ЕС), Директивата за медицинските изделия, Директивата за машините (2006/42/ЕО) и Директивата относно общата безопасност на продуктите (2001/95/ЕО).

³⁰ Комисията би могла да издаде насоки за прилагането на правилата на ЕС относно отговорността по отношение на „интернет на нещата“ и роботизираните системи.

жертвите, що се отнася до получаването на справедливо обезщетение или подходяща застраховка в случай на вреда.

При всеки подход ще трябва да се вземат предвид действията на използващото технологията лице, и по-точно да се определи каква следва да бъде ролята на ползвателите на тази технология.

Комисията ще проведе консултации със заинтересованите страни относно адекватността на действащите правила на ЕС относно отговорността в контекста на „интернет на нещата“ и автономните свързани системи, както и относно възможните подходи за преодоляване на настоящите трудности при разпределяне на отговорността. Едновременно с това се провежда също и обществена консултация за цялостната оценка на прилагането на Директивата относно отговорността за продукти. Комисията ще оцени резултатите и ще разгледа възможности за бъдещи действия.

5. ПРЕНОСИМОСТ, ОПЕРАТИВНА СЪВМЕСТИМОСТ И СТАНДАРТИ

Други нововъзникващи проблеми в основаната на данни икономика, са преносимостта на нелични данни, оперативната съвместимост на услугите, за да се даде възможност за обмен на данни, и подходящите технически стандарти за изпълнение на реална преносимост.

5.1. Преносимост на нелични данни

Преносимост на данните означава, че потребителите и предприятията могат лесно да преместват данните си от една система към друга. Това обикновено се свързва с ниски разходи за прехвърляне и следователно с ограничени пречки за въвеждане в основаната на данни икономика. С ОРЗД на лицата ще се даде право да получават предоставените на доставчика на услуги лични данни в структуриран, широко използван, пригоден за машинно четене формат, както и правото да ги прехвърлят на друг доставчик³¹.

По отношение на неличните данни обаче в момента няма задължения да се гарантира дори и минимално ниво на преносимост на данните, дори и за широко използвани онлайн услуги като доставчиците на хостинг в облак. Това се дължи отчасти на факта, че изискванията за изпълнение на преносимостта на данните може да бъдат скъпи и обременяващи от техническа гледна точка, тъй като различните доставчици на една и съща услуга може да съхраняват данните по различен начин.

За реалната преносимост на нелични данни трябва да се вземат предвид също и по-общи съображения за управление на данните, които включват прозрачност за потребителите, управляван достъп и оперативна съвместимост за свързване заедно на различни платформи по начини, с които да се стимулират иновациите.

³¹ Член 20.

5.2. Оперативна съвместимост

Съображенията относно преносимостта на данните често са тясно свързани с въпроси за тяхната оперативна съвместимост, която дава възможност множество цифрови услуги да обменят безпроблемно данни благодарение на подходящи технически спецификации. В Директивата относно информацията в общественния сектор и свързаните насоки (включително Европейската рамка за оперативна съвместимост) се подчертава значението на наличието на богати, стандартизирани метаданни по установени терминологични речници за улесняване на търсенето и оперативната съвместимост. В момента за пространствените данни³² в общественния сектор се прилага Директивата за създаване на инфраструктура за пространствена информация в Европейската общност (INSPIRE) и свързаните с нея регламенти за оперативна съвместимост и насоки относно услугите за пространствени данни и за данни, включително данните от наблюдение с датчици.

В случая на онлайн платформите, такава оперативна съвместимост на данните улеснява не само превключването, но също и едновременното използване на няколко платформи (така нареченото „многостранно свързване“ (multi-homing), както и широко разпространения обмен на данни между платформи, който има потенциал за насърчаване на иновациите в цифровата икономика

5.3. Стандарти

Ефективните политики за преносимост трябва да се подкрепят с подходящи стандарти, за да се постигне реална преносимост по технологично неутрален начин. Комисията се е ангажирала³³ да подкрепи подходящите стандарти за подобряване на оперативната съвместимост, преносимостта и сигурността на услугите в облак чрез по-доброто интегриране на общностите с отворен код в процесите по стандартизиране на европейско равнище. Примери за такъв подход са спецификацията за приложения в облак (TOSCA), с която се цели засилване на преносимостта и оперативното управление на приложенията и услугите в облак³⁴, както и техническите спецификации и насоките от регламентите за изпълнение на INSPIRE³⁵.

5.4. Възможни пътища напред

Възможните пътища напред за справяне с посочените по-горе проблеми включват:

- **Разработване на препоръчителни договорни условия за улесняване на смяната на доставчиците на услуги:** Тъй като преносимостта на данните и смяната на доставчиците на свързани с данни услуги са взаимозависими,

³² Машинно генерираните данни са „пространствени данни“, тъй като заедно с измерванията датчиците обикновено предават също и своето пряко или косвено местоположение (местонахождение).

³³ COM(2016) 176 final: Приоритети за стандартизацията в областта на ИКТ за цифровия единен пазар

³⁴ <https://www.oasis-open.org/committees/tosca>

³⁵ Законодателство по INSPIRE: <http://inspire.ec.europa.eu/inspire-legislation/26>

може да се проучи разработването на стандартни договорни условия, с които се изисква доставчикът на услуги да прилага преносимост на данните на даден потребител.

- **Разработване на допълнителни права за преносимост на данните:** Въз основа на правото на преносимост на данните, предоставено с ОРЗД, и предложените правила относно договор за предоставяне на цифрово съдържание, може да се въведат допълнителни права за преносимост на нелични данни, по-специално за да се обхванат отношенията между предприятия, като същевременно се вземат надлежно предвид резултатите от осъществяваната в момента проверка за пригодност на основни части от правото на ЕС относно предлагането на пазара и защитата на потребителите³⁶.
- **Специфични за секторите експерименти за стандарти:** За разработване на стабилен подход към правилата за преносимост, кодирани чрез стандарти, може да се създадат специфични за секторите експериментални подходи. Това обикновено ще предполага сътрудничество на множество заинтересовани страни, включително определящи стандартите субекти, представители на промишлеността, техническата общност и публични органи.

Комисията ще проведе консултации със заинтересованите страни по тези въпроси и въз основа на това ще определи дали се изисква по-нататъшно действие, евентуално под формата на горепосочените действия — поотделно или заедно.

6. ЕКСПЕРИМЕНТИРАНЕ И ИЗПИТВАНЕ

Експериментирането е важна част от проучването на нововъзникващи проблеми в основаната на данни икономика. Ще се проучи потенциалът за използване на финансиране по „Хоризонт 2020“ в подкрепа на такива изпитвания и експерименти.

Преди да се направят заключения доколко възможните решения за достъпа до данни и за отговорността са подходящи, следва да се организира специално изпитване за тестване на тези въпроси в реална среда, в партньорство със заинтересованите страни. Необходимо е европейско решение, постигнато при сътрудничество и експериментиране в отделните държави членки.

За такова изпитване може да се разгледа съвместната, свързана и автоматизирана мобилност³⁷, като се има предвид трансграничното измерение на този сектор.

В много държави членки вече са в ход проекти за разработване на съвместни системи и по-високи нива на автоматизация³⁸. С тези проекти на превозните

³⁶ http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

³⁷ Вж. COM (2016) 766 от 30.11.2016 г.

³⁸ Вж. COM (2016) 766: Европейска стратегия за съвместни интелигентни транспортни системи

средства се дава възможност да се свързват помежду си и с пътната инфраструктура, като например светофари и пътни знаци. Освен това Комисията има намерение да работи с група от заинтересовани държави членки за създаване на правна рамка за изпитване за провеждане на експерименти въз основа на хармонизирани правила относно достъпа до данни и отговорността. За да се даде възможност за достъп до достатъчно голям обем от данни, изпитванията следва да се направят на базата на 5G, като се работи при безпрепятствено паралелно функциониране с вече внедрени технологии и на принципа на допълняемост³⁹.

Като пример за интересен експеримент може да бъде даден геопространствения сектор с появата на нова основана на данните екосистема, изградена във връзка с „Коперник“, програмата на ЕС за наблюдение на Земята и третият най-голям доставчик на данни в света. Комисията разработва новаторски решения, за да насърчи разработването на приложения, базирани на „Коперник“ и други пространствени данни, по-специално насочени към решаването на проблемите с достъпа до данни, оперативната съвместимост и предвидимостта.

7. ЗАКЛЮЧЕНИЕ

За изграждане на основаната на данни икономика ЕС се нуждае от рамка за политиката, която дава възможност данните да се използват по цялата верига на създаване на стойност за научни, обществени и промишлени цели. За тази цел Комисията започва широкообхватен диалог със заинтересовани страни по разгледаните в съобщението въпроси. Първата стъпка от този диалог ще бъде обществена консултация. Въпросите за достъпа до данни и за отговорността ще бъдат изпитани и в реални условия в областта на съвместната, свързана и автоматизирана мобилност.

Що се отнася до свободното движение на данни, Комисията ще продължи да работи по този въпрос в съответствие с очертаните по-горе подход за пълно прилагане на принципа на свободно движение на данни в рамките на ЕС, включително, ако е необходимо и целесъобразно, чрез приоритизирано действие за прилагане. Комисията ще продължи също така да наблюдава и да събира факти и, ако е необходимо, може да обмисли предприемане на допълнителни инициативи относно свободното движение на данни.

Въз основа на резултатите от диалога със заинтересованите страни Комисията ще реши също така дали е необходимо допълнително действие по нововъзникващите проблеми и ще предложи съответни решения. В този контекст експериментирането в реални условия може да изиграе важна роля.

³⁹ Вж. COM (2016) 588: 5G за Европа: план за действие