

Становище на Европейския икономически и социален комитет относно „Доверие, неприкосновеност на личния живот и сигурност на потребителите и предприятията при „интернет на нещата“**(становище по собствена инициатива)**

(2018/C 440/02)

Докладчик: **Carlos TRIAS PINTÓ**Съдокладчик: **Dimitris DIMITRIADIS**

Решение на Пленарната асамблея	15.2.2018 г.
Правно основание	Член 29, параграф 2 от Правилника за дейността становище по собствена инициатива
Компетентна секция	„Единен пазар, производство и потребление“
Приемане от секцията	4.9.2018 г.
Приемане на пленарна сесия	19.9.2018 г.
Пленарна сесия №	537
Резултат от гласуването	182/3/2
(„за“/„против“/„въздържал се“)	

1. Заключение и препоръки

1.1. Благодарение на взаимосвързаността на хора и предмети интернет на нещата (по-нататък „ИН“) предлага широка гама от възможности за гражданите и предприятията. Тези възможности трябва да бъдат придружени от серия от гаранции и мерки за контрол, за да се осигури безпроблемно въвеждане на ИН.

1.2. Тъй като един от стълбовете на ИН е свързан с автоматичното вземане на решения без човешка намеса, трябва да се гарантира, че решенията не накърняват правата на потребителите, нито водят до рискове от етичен характер или противоречат на основни принципи и права на човека.

1.3. ЕИСК призовава европейските институции и държавите — членки на ЕС:

1.3.1. да гарантират защитата на сигурността и неприкосновеността на личния живот чрез изготвянето на подходящи регулаторни рамки, които да включват стриктни мерки за наблюдение и контрол;

1.3.2. да определят ясно отговорността на всички оператори по веригата за доставка на продукта и свързаните с това информационни потоци, предотвратявайки правни пропуски, които възникват при едновременно участие на различни производители и дистрибутори;

1.3.3. да установят подходящи ресурси и ефективни механизми за координация между Европейската комисия и държавите членки, за да се гарантира съгласувано и хармонизирано прилагане както на преразглежданото законодателство, така и на новите правила, като същевременно се вземе предвид и международната среда;

1.3.4. да следят разработването на нововъзникващите технологии, свързани с ИН, за да се гарантира висока степен на сигурност, пълна прозрачност и справедлив достъп;

1.3.5. да насърчават европейските и международните инициативи за стандартизация с цел гарантиране на надеждността, наличността, устойчивостта и поддържането на продуктите;

1.3.6. да следят пазарите и да защитават еднаквите условия на конкуренция при прилагането на ИН, като избягват концентрацията на транснационална икономическа сила в новите технологични играчи;

1.3.7. да се ангажират да насърчават инициативи за повишаване на осведомеността и изграждане на цифрови умения, отразяващи основните научни изследвания и иновации в тази област;

1.3.8. да гарантират пълното прилагане и ефективното използване на алтернативни механизми за уреждане на спорове както онлайн, така и офлайн;

1.3.9. да насърчават създаването, въвеждането и ефективното функциониране на европейска система за групови иски за прекратяване и получаване на обезщетения и в случаите когато използването на ИН причинява щети или вреди от колективен характер, както както би следвало да бъде съгласно Новия търговски механизъм за потребителите.

1.4. Доверието на потребителите е свързано със стриктното спазване на съответното законодателство и комуникацията във връзка с най-добрите бизнес практики в областта на неприкосновеността на личния живот и сигурността, като задача на институциите е те да бъдат включени в стратегии за корпоративна социална отговорност и социално отговорни инвестиции.

1.5. Социално-икономическото въздействие на ИН ще нараства значително, когато е подходящо обвързано с разработването на социални и екологични политики в рамките на икономиката на споделянето, кръговата икономика и икономиката на функционалността.

2. Основна информация и контекст

2.1. Бурното развитие на интернет през последните петнадесет години доведе до промени във всички сфери на ежедневието, оказвайки въздействие върху различни навици на потребителите. Очаква се, че революцията на интернет на нещата през следващите десет години ще обхване секторите на енергетиката, селското стопанство и транспорта, както и по-традиционните сфери от икономиката и обществото. Това налага разработването на цялостни политики за интелигентен подход към този технологичен пробив.

2.2. Концепцията за ИН се заражда първоначално в Масачузетския технологичен институт, като идеята се основава главно на съществуването на свят, пълен с напълно взаимосвързани устройства, чиито различни оперативни съвместими процеси да могат да бъдат автоматизирани. От своя страна, Европейският съюз се подготвя да посрещне цифровата конвергенция и новите предизвикателства на ИН, като се започне от стартирането на плана „i2010 — европейско информационно общество за растеж и заетост“⁽¹⁾ и се стигне до въведения наскоро план за действие в областта на ИН (вж. документа, озаглавен „Напредък в областта на интернет на нещата в Европа“, който е част от съобщението от 2016 г. „Цифровизиране на европейската промишленост. Оползотворяване в пълна степен на предимствата на цифровия единен пазар“)⁽²⁾.

2.3. ЕИСК е изразявал многократно позицията си относно четвъртата индустриална революция, белязана от конвергенцията на цифровите, физическите и биологичните технологии, като би искал да обърне специално внимание на становището си от 2017 г. по тази тема⁽³⁾. Всъщност ИН е идеалното поле за изява на най-усъвършенстваните форми на ИИ, където се изпробват принципите, определени от ЕИСК, и по-специално принципът на „човешкия контрол“.

2.4. Устройствата, базирани на ИН, често не разполагат със стандарти за установяване на автентичност, необходими за гарантиране на сигурността на данните на ползвателите. Това води до появата на проблеми, тъй като устройствата, данните и партньорите по веригата за доставки са застрашени от пробиви в сигурността.

2.5. Нововъзникващите технологии като блоковите вериги могат да решават проблеми, свързани със сигурността и доверието: те могат да се използват за проследяване на измерванията на данните от датчици и не само за избягване на дублирането с каквито и да било други злонамерени данни, но и за запазване на целостта и проследимостта на промените; една споделена счетоводна книга може да даде възможност за идентифициране на устройствата на ИН, удостоверяване на автентичността и сигурния пренос на данни, без пробиви; датчиците на ИН могат да се използват за обмен на данни чрез блокова верига вместо трета страна; използването на интелигентни договори позволява автономност на устройствата, както и индивидуална самоличност и цялост на данните; разходите за създаване и функциониране намаляват поради отсъствието на посредници; и накрая, устройствата на ИН по блоковата верига предоставят информация за свързаните устройства, което е много полезно за разрешаването на евентуални проблеми⁽⁴⁾.

⁽¹⁾ COM(2005) 229 final.

⁽²⁾ COM(2016) 180 final.

⁽³⁾ „Изкуствен интелект — въздействието на изкуствения интелект върху (цифровия) единен пазар, производството, потреблението, заетостта и обществото“ (ОВ С 288, 31.8.2017 г., стр. 1).

⁽⁴⁾ Вж. Khwaja Shaik, *Why blockchain and IoT are best friends* („Защо блоковата верига и ИН са най-добри приятели“), <https://www.ibm.com/us-en/?lnk=m>; за иновациите в европейския финансов сектор вж. ОВ С 246, 28.7.2017 г., стр. 8.

2.6. За разлика от това технологиите на разпределения регистър с отворен код са разработени за обмен на информация и на стойност между устройствата, базирани на ИН. Те не позволяват извличане на данни, но използват архитектура, основана на математическа концепция, наречена „насочена ациклична графика“ (DAG), с която се избягват комисионите и се гарантира, че мрежата може да увеличи капацитета си в съответствие с нарастването на броя на потребителите.

2.7. Накратко, изправени сме пред явление с огромен икономически⁽⁵⁾ и социален потенциал, което поражда големи възможности, но и сериозни предизвикателства, свързани със скрити рискове, като неговият мултидисциплинарен и хоризонтален характер засяга в еднаква степен предприятията и потребителите, администрациите и гражданите. Поради това при разглеждането на този въпрос следва да се възприеме общ подход, като същевременно се вземат предвид особеностите на всяка ситуация. Във връзка с това е достатъчно да се посочи, че по прогнози на Организацията на обединените нации през 2020 г. ще има петдесет милиарда взаимосвързани устройства, с приложения за потребителите чрез телевизионни приемници, хладилници, охранителни видеокameraи, превозни средства и др.

2.8. Приложенията на ИН вече носят икономически и социални ползи в рамките на глобализирания свят, което означава и повече чувствителни спрямо социално-икономическия контекст услуги, по-кратки цикли на обратна връзка, ремонти от разстояние, подкрепа за вземането на решения, по-добро разпределение на ресурсите и дистанционно управление на услугите. При все това съществуват много чувствителни фактори, свързани с този въпрос, като например неприкосновеност на личния живот и сигурност, информационен дисбаланс, прозрачност на трансакциите, комплексни отговорности, блокиране на продукти и системи и нарастващо разпространение на хибридните продукти, което може да засегне въпроса за собствеността и да изложи потребителите на дистанционно прилагане на договорите с последващо ограничаване на гаранциите.

2.9. Огромните правни предизвикателства, пред които са изправени ЕС и неговите държави членки, се обясняват с факта, че много от специфичните характеристики на ИН (високи равнища на сложност и голяма взаимна зависимост, елемента на автономност, компонентите на генериране и/или обработване на данни и отвореното измерение) се споделят с други нововъзникващи цифрови технологии, като например блоковата верига, 3D печата и изчисленията в облак. Според ЕИСК работният документ на службите на Европейската комисия⁽⁶⁾ относно отговорността за нововъзникващите цифрови технологии е още една стъпка в правилната посока.

2.10. Накратко, максималното увеличаване на ползите и свеждането до минимум на рисковете, свързани с ИН, води до улесняване на достъпната, ясна, кратка и точна информация, насърчавайки по-специално приобщаването и цифровата свързаност на най-уязвимите потребители посредством разработването на изцяло проследими продукти и услуги, съдържащи интегрирани правила за доверие, неприкосновеност на личния живот и сигурност.

3. Доверие на потребителите и предприятията в ИН

3.1. ИН е комплексна екосистема, която позволява взаимно свързване на устройства от различни производители, дистрибутори или разработчици на софтуер. Това може да създаде трудности за определяне на отговорността в ситуации на неспазване на правилата или при материални щети или други вреди, причинени на трети страни или на системи от дефектни стоки или от стоки, използвани не по предназначение от трети страни, с изключение на крайните потребители, в интернет. Съществува и възможността много от операторите, които участват във веригата за създаване на обща стойност на продукта, да не разполагат с достатъчно знания или опит по въпросите на сигурността или защитата на данните за устройствата в мрежа.

3.2. Поради това е необходим нов подход към отговорностите, който да гарантира, че и потребителите, и предприятията, които внедряват приложения на ИН, са защитени в среда, в която продуктите с подходяща конфигурация могат да се окажат дефектни или небезопасни в резултат от инциденти, свързани с цифровата сигурност, или неправомерно използване (например хакерски атаки). Тази среда следва да позволява предвиждането, предотвратяването и защитата от автоматизирани решения, които могат да нарушат общоприетите етични принципи и правата на човека.

⁽⁵⁾ По изчисления на Digital McKinsey потенциалното икономическо въздействие на ИН ще бъде между 3,9 и 11,1 млрд. щатски долара годишно през 2025 г.

⁽⁶⁾ SWD(2018) 137.

3.3. ЕИСК приветства преразглеждането на прилагането на Директивата от 1985 г. относно отговорността за вреди, причинени от дефектна стока ⁽⁷⁾, както и неотдавнашното създаване на групата от експерти на различните заинтересовани страни по въпросите на отговорността и новите технологии, с цел да се гарантира справедливо равновесие между интересите на производителите и потребителите. В новата рамка за отговорността следва да се предвиди ясно проследимостта на отговорността и сигурността както на всеки етап от веригата за създаване на стойност на продукта, така и по време на неговия жизнен цикъл, включвайки устойчивостта като нов фактор, което ще доведе до налагането на задължение за актуализиране, усъвършенстване, преносимост, съвместимост, повторна употреба, поправка или настройка на продукта.

3.4. Също така обект на специално внимание по отношение на ИН следва да е определянето на отговорността на всички оператори по веригата за доставка на продукта, като се избягват регулаторни пропуски при едновременното участие на няколко производители и дистрибутори. ЕИСК счита, че е от съществено значение да бъдат посочени ясно процедурите, които потребителите трябва да следват във всеки отделен случай, като се насърчат механизмите за алтернативно решаване на спорове.

3.5. ЕИСК подчертава значението на преддоговорната информация, прозрачните договорни клаузи и ясните инструкции за експлоатация на устройствата. Евантуалните свързани с тях рискове и гаранции следва да бъдат изрично подчертани.

3.6. Оперативната съвместимост и съответствието на устройствата и свързания с тях софтуер трябва да бъдат гарантирани, за да се предотвратят проблемите и да се даде възможност на потребителите да сравняват доставчиците. ЕИСК подчертава, че този фактор също е от ключово значение за създаването на еднакви условия на конкуренция между големите предприятия и МСП.

3.7. Накрая ЕИСК настоява за спазване на мрежова неутралност и призовава Комисията да извършва строг мониторинг на пазарното поведение.

4. Неприкосновеност на личния живот на потребителите в ИН

4.1. Възможността на потребителите да проверяват своите лични данни и предпочитания по отношение на неприкосновеността на личния си живот беше подобрена с новия Общ регламент относно защитата на данните (ОРЗД) ⁽⁸⁾. Ползвателят на дадено устройство трябва да има контрол върху това как се използват генерираните данни и кой може да има достъп до тях, като се има предвид, че многообразието на данните, както и тяхното съсредоточаване и свързването им с други данни, предполага сериозен риск за неприкосновеността на личния живот в екосистемата на ИН.

4.2. Следва да се отчита въздействието, което могат да имат множеството продукти, услуги или субекти върху неприкосновеността на личния живот и защитата на данните, когато последните, поради своята взаимосвързаност, се предават самостоятелно. По същия начин в случаите, в които се обработва или преработва информацията от първоначално безобидни данни, може да се придобие точна картина за навиците, местоположението, интересите и предпочитанията на отделните лица, което увеличава достъпността и проследимостта на профила на потребителя.

4.3. Правните гаранции следва да осигуряват пълната възможност на ползвателите да упражняват своите права на неприкосновеност на личния живот и защита на личните данни без каквото и да било ограничение. По този начин се избягват потенциални вреди като дискриминационни практики, агресивно предлагане, загуба на неприкосновеност или нарушения на сигурността. От своя страна потребителите трябва да разполагат с информация относно икономическата стойност на своите данни и да си запазват правото да могат да ги споделят.

4.4. Съгласно ОРЗД предприятията и регулаторите трябва да преразглеждат периодично обхвата на събирането на лични данни и да оценяват степента, в която обработваните данни са пропорционални и необходими за осъществяването на услугата. Различните аспекти и въздействия по отношение на неприкосновеността на личния живот следва да се оценяват на всеки етап от създаването на концепцията, проектирането и разработването на всеки свързан продукт и мрежовата екосистема, в която той оперира (защита на личния живот още при проектирането). Поради това принципите на защита на личния живот още при проектирането и неприкосновеност на личния живот по подразбиране трябва да бъдат въведени последователно в ИН.

4.5. Също така всички свързани продукти следва да се конфигурират по предварително определен начин, така че да бъде постигнато най-високото равнище на защита на личните данни (още при проектирането и по подразбиране), като се избягва нежеланото проследяване на поведението на потребителите и техните занимания.

⁽⁷⁾ COM(2018) 246 final.

⁽⁸⁾ В сила от 25 май 2018 г.

4.6. При всички случаи потребителите следва да са надеждно запознати с това какви данни се събират, кой има достъп до тях и за какво ще бъдат използвани, докато се поддържа активна връзката с продукта или услугата, както и с приложимата политика на поверителност, а също и дали използваните алгоритми засягат качеството, цената или достъпа до услугата.

5. Сигурност на потребителите и на предприемачите в ИН

5.1. Взаимосвързаността на устройствата, характерна за екосистемата на ИН, може да насърчи развитието на незаконни или нежелателни технологични практики, превръщайки се в среда, която насърчава уязвимостта и нейното „вирусно“ разпространение. Поради това следва да се следи за цялостната сигурност на всички елементи на системата.

5.2. Предлагащите продукти и актуализации, свързани с киберсигурността, следва да са обосновани и да обхващат не само отделните устройства, но и рисковете за сигурността, произтичащи от взаимната свързаност с други устройства в ИН, без да се снижават стандартите за качество на сигурността заради броя на устройствата.

5.3. В тази връзка предложението за регламент относно Агенцията на ЕС за киберсигурност⁽⁹⁾ включва рамка за сертифициране на информационните и комуникационните технологии, която позволява доброволно сертифициране за сигурност и етикетирание на различните видове продукти, включително базираните на ИН. Въпреки че приветства въвеждането на тази мярка, ЕИСК изразява загриженост относно незадължителния ѝ характер.

5.4. Мерките за киберсигурност следва да покриват рисковете от всякаква форма на уязвимост, и по-специално хакерство, неразрешен достъп или злоупотреби, както и рисковете, свързани с начините на плащане и финансовите измами. В тази връзка ЕИСК подкрепя правомощията, дадени на групата от експерти на различните заинтересовани страни по въпросите на отговорността и новите технологии.

5.5. Освен това следва да се разгледа и въпросът за личната безопасност и сигурност на потребителите с оглед на рискове като използването на близостта, споделянето честотни ленти, излагането на електромагнитни полета и възможните смущения в работата на свързаните животоподдържащи устройства. ЕИСК подкрепя прилагането на мерки за надзор и превантивно изтегляне на продукти с оглед на рискове, засягащи здравето и сигурността на потребителите или техните лични и икономически интереси.

5.6. Предприятията следва да приемат стандарти за добри практики, например по отношение на сигурността, още при проектирането и по подразбиране, както и да подлежат на независими външни оценки. В случай на инциденти, свързани със сигурността, или пробив в базата данни, предприятията са длъжни да съобщават въпросните инциденти, включително информацията относно отговорността за щетите и неспазването на правилата.

5.7. Предприятията следва да предоставят на потребителите опростена и достъпна информация, която да им позволява да вземат подходящи решения и да възприемат сигурни практики, като осигуряват необходимите актуализации на сигурността в хода на жизнения цикъл на продукта.

5.8. Следва да се разгледа въпросът за липсата на съгласувани правила във връзка с мрежите на ИН. Трябва да се въведат модерни широколентови мрежи и технологии от ново поколение, с които да се подобри съществуващата инфраструктура.

6. Предложения за действия в рамките на публичната политика⁽¹⁰⁾

6.1. При упражняването на своите правомощия в различните територии на Европейския съюз публичните администрации трябва да участват активно в разработването на политиките и планове за действие в областта на ИН с цел да се постигне равновесие между различните заинтересовани страни, да се предвидят евентуалните проблеми и да се предприемат мерки срещу възможни неблагоприятни последици. ЕИСК призовава за:

6.1.1. създаване на опитна среда („пясъчна кутия“), т.е. физически пространства, клъстери и др. за осъществяване на пилотни проекти и проекти за тестване на концепции. Тяхната цел следва да е изпробване не само на технологии, но и на регулаторни модели⁽¹¹⁾;

⁽⁹⁾ Вж. COM(2017) 477 final.

⁽¹⁰⁾ Вж. Група на Световната банка, *Internet of Things: The New Government-to-Business Platform* (Доклад относно „Интернет на нещата: новата платформа за взаимодействие между правителствата и бизнеса“).

⁽¹¹⁾ Вж. <https://ec.europa.eu/digital-single-market/en/news/eu-and-eea-member-states-sign-cross-border-experiments-cooperative-connected-and-automated>.

- 6.1.2. финансиране на технологична инфраструктура, която да позволява разработването на иновативни проекти в областта на ИН в рамките на новата програма „Хоризонт Европа“;
- 6.1.3. определяне на независими институти и агенции, които да работят за улесняване и в подкрепа на проектите в областта на ИН. ЕИСК приветства съответните мерки, предвидени в Регламента от 2017 г. относно киберсигурността, и призовава Комисията ефективно да насърчава процесите на стандартизация в цифровия сектор с помощта на подходящи бюджетни средства⁽¹²⁾;
- 6.1.4. насърчаване на публично-частните платформи и партньорства, обединявайки научните среди, промишлеността и потребителите;
- 6.1.5. стимулиране на инвестициите в разработване на местни бизнес модели, които да използват предимствата на ИН и да помагат за справянето със сложни аспекти като защитата на данните и собствеността върху тях;
- 6.1.6. действия за изграждане на капацитет на равнище предприятия по отношение на съвместната отговорност. Следва да се гарантира, че принципите на сигурност и защита на личния живот още при проектирането и по подразбиране са включени в продуктите и услугите на ИКТ в съответствие с т. нар. принцип на „задължение за полагане на грижи“, посочен в новия Регламент относно киберсигурността. Във връзка с това ЕИСК приветства предвиденото съставяне на **кодекси за поведение**, които да допълват регламента;
- 6.1.7. насърчаване на инициативите за европейска и международна стандартизация, за да се гарантира, че системите на ИН притежават основните характеристики, а именно надеждност, сигурност, наличност, стабилност, възможност за поддръжка и експлоатация. По-специално стандартизацията е от съществено значение за бързото осъществяване на високоцифровизираните процеси на промишлено производство;
- 6.1.8. гарантиране, че ползвателите на ИН, особено най-уязвимите или живеещите в слабо населени райони, имат висококачествен достъп на достъпни цени;
- 6.1.9. насърчаване на кампании за повишаване на осведомеността и образователни програми с цел да се подпомогне приемането на ИН от страна на предприятията и потребителите, като се създадат условия за придобиване на необходимите умения и компетентности⁽¹³⁾ и като се обърне специално внимание на уязвимите групи и многообразието;
- 6.1.10. стартиране на инициативи в областта на образованието за подходяща превенция с оглед на ранното включване на децата в цифровата среда;
- 6.1.11. провеждане на диагностични анализи и проучвания на въздействието на ИН върху области като новите модели на устойчиво производство и потребление;
- 6.1.12. гарантиране на пълното прилагане и ефективното използване на алтернативни механизми за уреждане на спорове както онлайн, така и офлайн;
- 6.1.13. насърчаване на създаването, въвеждането и ефективното функциониране на европейска система за групови искове за прекратяване и получаване на обезщетения и в случаите когато използването на ИН причинява щети или вреди от колективен характер, както би следвало да бъде съгласно Новия търговски механизъм за потребителите.
- 6.2. ЕИСК призовава също Комисията да извърши оценка на пряко или непряко свързаните с ИН правила, и, където е необходимо, да пристъпи към подобряване на съществуващото законодателство. Във връзка с това **Новият търговски механизъм за потребителите** следва да се съсредоточи и върху взаимосвързаните устройства и мрежи и тяхната сигурност, както и върху данните, свързани с тези устройства.
- 6.3. В заключение ЕИСК подчертава значението на създаването на механизми за сътрудничество и координация между държавите членки за ефективно и единно прилагане на предвидените правила, както и за споразуменията, които Европейският съюз следва да сключи извън своята територия поради местонахождението на седалищата на различните предприятия и доставчици, със специален акцент върху обмена на добри практики. Международната политика относно трансграничния поток от данни трябва да бъде координирана, така че участващите държави да могат да установят еднакво високи материални и процедурни стандарти за защита в националното си законодателство.

Брюксел, 19 септември 2018 г.

Председател
на Европейския икономически и социален комитет
Luca JAHIER

⁽¹²⁾ ОВ С 197, 8.6.2018 г., стр. 17.

⁽¹³⁾ ОВ С 434, 15.12.2017 г., стр. 36.