Новите технологии и защитата на личните данни - законодателство и практическо приложение

Автор:

Мария-Магдалена Мартинова Маркова,

Студент по Право, V курс

Софийски университет "Св. Климент Охридски"

Summary

The creation of blockchain technology is a result of the on-going digital revolution in the XXI century. Blockchain's popularity and its inherent qualities, namely decentralisation and immutability, put a significant amount of pressure on the applicable rules on data protection. Many questions arise, such as - is the current legislation capable of coping with the emerging technology, are there enough legal guarantees for the protection of the rights of the data subjects, etc. Although crucial for the technological development of Europe, the application of blockchain raises several concerns as to the protection of the data subjects, more specifically in the light of the right "*to be forgotten*" under Art. 17 of the Regulation. The strict interpretation of the notion of "*erasure*" under Art. 17 (equal to irreversible destruction of data) is not able to lead to successful results in the context of blockchain, but would rather hinder the technical progress in Europe. It is more realistic for alternative measures to destruction to be applied in order for a sufficient amount of protection to be guaranteed. In any case, there are many practical issues before the data subjects, including identification of data controllers and lack of effective means to secure the deletion of the information from all "nodes."

Революцията на дигиталните технологии през XXI век е едно от най-големите предизвикателства пред защитата на личните данни. Множеството технологични иновации, намиращи отражение във всяка една област на обществения живот несъмнено водят до изключителен прогрес на човечеството. Резултат от дигиталната революция е и появата на т.нар. блокчейн технология.[1]

В последно време, особено покрай интереса на масовата публика към криптовалутите, блокчейн технологията започна да придобива изключителна популярност.[2] Прилагането ѝ обаче повдига редица въпроси от гледна точка на регулациите на национално и наднационално ниво и най-вече от гледна точка на Регламент 2016/679 на Европейски парламент и на Съвета от 27 април 2016 година 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**," "**GDPR**").

Какво представлява блокчейн? Най-простото определение, което може да бъде дадено за блокчейн е **синхронизирана база данни, която се записва и съхранява на множество компютри** (т.нар. "*нодове*") на различни места по света.[3] Една от най-характерните черти на блокчейн технологията е **децентрализацията**[4] - информацията лесно се мултиплицира, съхранява се паралелно на множество различни "*нодове*," като всеки "*нод*" има възможността, независимо от останалите, да "*ъпдейтва*" базата данни, т.е. да добавя допълнителна информация. На практика, блокчейнът работи като счетоводна книга, в която информацията се съхранява в специфични регистри - "*леджъри*" (ledger), които съществуват между много и различни участници.[5]

---

[1] Технологията блокчейн е описана за първи път от Сатоши Накамото в Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf, 2009г. Сатоши Накамото е псевдонимът на създателя на криптовалутата биткойн.

[2] Така при проучване извършено в САЩ, 53% от анкетираните смятат, че през 2019г. имплементирането на блокчейн технологиите се е превърнало в "критичен приоритет" за техните компании. https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf

[3] Какво е Блокчейн и как да се възползвате от възхода на технологията?, 2020г., https://admiralmarkets.bg/education/articles/shares/blockchain-1

[4] Atzori, M., "Blockchain technology and decentralized governance: is the state still necessary?," Journal of Governance and Regulation, том 6, изд. 1, 2017г.

[5] Запрянов, Й., Тодоров, Т., Бизнесът, блокчейн и бъдещето, Капитал, 2019г., налично на: https://www.capital.bg/specialni_izdaniia/blockchain/2019/06/30/3930656_biznesut_blokchein_i_budeshteto/

Има различни видове блокчейн, като основното разграничение е на **публични и частни**. Публичните блокчейни са мрежи, които са достъпни за потребителите без предварително дадено разрешение (т.нар. "*permission-less networks*"). Частните блокчейни, от друга страна, оперират в частни мрежи и са достъпни само за определени потребители, които са получили разрешение за достъп от съответния администратор на мрежата (т.нар. "*permissioned network*"). Практическата разлика се крие в това, че при публичните блокчейни всички потребители участват в съответната транзакция (т.е. информацията се репликира на всички "*нодове*" в мрежата), а при частните - информацията се споделя само с конкретни "*нодове*."[6]

Втората съществена характеристика на блокчейн технологиите е тяхната **неизменност**. Характерно е, че това са структури, към които може само да се добавя информация (т.нар. "*append-only data structures*").[7] Веднъж след като информацията е записана в базата данни, нейното модифициране е изключително обременяващо и почти невъзможно практически.[8] В повечето случаи модификацията би изисквала повторно верифициране на всички транзакции, извършени назад по веригата, разрушаване на целия блокчейн, повторното му построяване блок по блок и повторно регистриране на всяка една от извършените транзакции.[9]

Тук следва да се отбележи, че блокчейнът е **клас технология**[10] и че няма една единствена версия от тази технология. Различните версии се характеризират с различна степен на сложност, технически спецификации и начин на управление. Следователно няма как да се направи преценка дали блокчейн технологията сама по себе си е в съответствие с регулациите за защита на личните данни или не. Така например, от изложеното по-горе е видно, че при частните блокчейни теоретично е по-лесно да се постигне съответствие с приложимото право за защита на личните данни, тъй като участниците в транзакциите са известни и по този начин

---

[6] Sharma, R., Public Vs. Private Permissioned Ledgers And Blockchain Standards, Forbes Technology Council, 2019

[7] Finck, M., Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?, 2019г., стр. 3

[8] Magas, J., Immutability in Doubt: Do we need to protect Blockchain data?, 2018г., налично на: https://cointelegraph.com/news/immutability-in-doubt-do-we-need-to-protect-blockchain-data

[9] Berberich, M. and Steiner, M., Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?, European Data Protection Law Review, 2016г., стр. 422, 426

[10] Beck, R., Müller-Bloch, C. and King, J., Governance in the Blockchain Economy: A Framework and Research Agenda, 2018г. стр. 3

става възможно, например договорно разпределение на правата и задълженията във връзка с обработката на лични данни. Не така стои въпросът с публичните блокчейни, при които броят на участниците и тяхната самоличност са неизвестни. Именно поради тази причина следва да бъде направена уговорката, че преценката за съответствието с приложимото право за защита на личните данни да се изследва във всеки отделен случай за всеки конкретен "вид" блокчейн. Въпреки това, настоящото есе ще се опита да разгледа генерално въпроса възможно ли е въобще съответствие между блокчейн технологията и разпоредбите на GDPR (по-конкретно с правото "*да бъдеш забравен*," закрепено в чл. 17 GDPR).

Правото на защита на личните данни е едно от основните права, закрепени в Хартата на основните права на Европейския съюз ("**Хартата**"). Съобразно чл. 8(1) от Хартата всеки има право на защита на неговите лични данни. Всяко обработване следва да бъде "*добросъвестно, за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено в закона легитимно основание*."[11] Хартата изрично предвижда, че всеки има право на достъп до събраните данни, отнасящи се до него, както и "*правото да изиска поправянето им*."[12]

В опит да гарантира "*последователно и високо ниво на защита на физическите лица, както и за да се премахнат препятствията пред движението на лични данни в Съюза,*"[13] европейският законодател създава GDPR, който започва да се прилага на територията на Съюза от 25 май 2018 г.

Безспорно е, че между блокчейн технологията и GDPR има определена доза напрежение, която се дължи главно на две причини. На първо място това е сблъсъкът "**централизация - децентрализация**." От една страна, GDPR е базиран на предположението, че винаги зад обработката на личните данни стои конкретно физическо или юридическо лице (администратор на лични данни), към което субектите на личните данни могат да насочат своите претенции.[14] От друга страна децентрализираният механизъм на действие на блокчейн технологията прави неясно разпределението на отговорностите за гарантиране на правата

[11] Чл.8(2) от Хартата на основните права на Европейския съюз
[12] Пак там.
[13] GDPR, съображение 10
[14] Finck, M., Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?, 2019г., стр. 2

между множеството "*актьори*" в блокчейна, особено като се има предвид неограничения (и често - неопределен) кръг "*нодове*", които имат достъп до съответната база данни.

На второ място се наблюдава и сблъсък "**изменност - неизменност**." От една страна, GDPR е базиран на идеята, че информацията може да се променя и/или изтрива, когато е необходимо.[15] От друга страна, както бе посочено по-горе, модификацията на блокчейна е изключително обременяваща и дори невъзможна в определени хипотези.

В контекста на този сблъсък между GDPR и блокчейн, логично е да бъде зададен въпросът, който изглежда с най-голямо практическо значение за субектите на лични данни, а именно: приложимо ли е правото "*да бъдеш забравен*," закрепено в чл. 17 GDPR към блокчейн технологията?

Съгласно чл. 17 GDPR, субектът на данни има правото да поиска от администратора **изтриване** на свързаните с него лични данни "*без ненужно забавяне*," а администраторът има **задължението да изтрие** "*без ненужно забавяне*" личните данни, когато е приложимо някое от изрично посочените в чл. 17 GDPR основания.[16] На пръв поглед това задължение за навременно "*изтриване*" на личните данни изглежда почти неприложимо като се имат предвид посочените по-горе характеристики на блокчейн технологията, а именно: **висока степен на децентрализация и неизменност**. Така ли е обаче наистина?

Изглежда, че отговорът на този въпрос (поне донякъде) се крие в **интерпретацията на термина "*изтриване*" ("*erasure*")**. Следва да се отбележи, че GDPR не съдържа дефиниция на термина "*изтриване*" нито в преамбюла си, нито в оперативните разпоредби.[17] Въпреки това, терминът може да бъде интерпретиран по два начина. На първо място - в неговото общоприето значение, а именно: "*унищожаване*," "*премахване напълно*."[18] Очевидно е, че общоприетото значение на термина изисква пълното и безвъзвратно унищожаване на данните. Не изглежда

---

[15] Например във връзка с упражняването на правата по чл. 16 от Регламента ("право на коригиране") и чл. 17 ("право на изтриване" / "право да бъдеш забравен")

[16] Например: а) личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин; б) субектът на данните оттегля своето съгласие, върху което се основава обработването на данните съгласно член 6, параграф 1, буква а) или член 9, параграф 2, буква а), и няма друго правно основание за обработването; в) субектът на данните възразява срещу обработването съгласно член 21, параграф 1 и няма законни основания за обработването, които да имат преимущество, или субектът на данните възразява срещу обработването съгласно член 21, параграф 2 и др.

[17] Finck, M., Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?, 2019г., стр. 75

[18] Речник на българския език, Институт за български език, достъпен на: https://ibl.bas.bg/rbe/

обаче да има единно становище, че европейският законодател е искал да вмени именно това общоприето значение в термина "*изтриване*" при създаването на GDPR.

В литературата съществува становище, че преюдициалното заключение на Съда на Европейския съюз ("**СЕС**," "**Съда**") по делото Google Spain може да бъде интерпретирано в посока, че не е необходимо информацията да бъде безвъзвратно унищожена, а са достатъчни алтернативни мерки, сходни на тези в делото (заличаване на връзките към уеб страници от списък на резултати в интернет търсачка, който се показва след търсене въз основа на името на физическо лице).[19] Подобно тълкуване на делото **не може да бъде подкрепено**. Безспорно в своето решение СЕС не е заключил, че в допълнение към заличаване на връзките към уеб страниците, е необходимо заличаване и на информацията, съдържаща се на конкретните уеб страници. Съдът обаче не е бил сезиран с въпрос относно интерпретацията на термина "*изтриване*," а единствено се е произнесъл по въпроса дали искането на лицето в главното производство (г-н Costeja González), а именно дадена информация да не се предоставя повече на разположение на широката общественост посредством включването ѝ в списък на резултати в интернет търсачка, е в съответствие с разпоредбите на Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни ("**Директива 95/46/ЕО**").[20] Произнасяне, че е налице задължение за изтриване и на информацията, съдържаща се на конкретните уеб страници би излязло извън предмета на делото в главното производство, както и на делото по даване на преюдициално заключение на СЕС. Следователно Google Spain не би могло да бъде използвано като отправна точка за интерпретиране на термина "*изтриване*."

---

[19] Finck, M., Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?, 2019г., , стр. 75

[20] Решение на Съда от 13 май 2014г. по дело C-131/12 Google Spain and Google, ECLI:EU:C:2014:317, пар. 99: "*От изложените по-горе съображения следва, че на третия въпрос, трябва да се отговори, че член 12, буква б) и член 14, първа алинея, буква а) от Директива 95/46 трябва да се тълкуват в смисъл, че при преценката на условията за прилагане на тези разпоредби следва по-специално да се провери дали съответното лице има право въпросната информация, отнасяща се до него, да не се свързва повече с името му [...]. Тъй като с оглед на основните си права по членове 7 и 8 от Хартата съответното лице може да поиска въпросната информация да не се предоставя повече на разположение на широката общественост посредством включването ѝ в подобен списък на резултатите, тези права имат по принцип предимство не само пред икономическия интерес на лицето, което управлява интернет търсачката, но и пред интереса на тази общественост да има достъп до посочената информация при търсене, отнасящо се до името на въпросното лице*."

Въпреки това, редица регулаторни органи на национално ниво са заели становище, че не е необходимо "*изтриване*" да се равнява на "*унищожаване*." Така например според Службата на информационния комисар на Обединеното кралство (ICO) е достатъчно информацията да се извади от употреба ("*to be put beyond use*").[21] В своите насоки, Службата на Обединеното Кралство отбелязва, че "*изтриването*" в буквален смисъл не е винаги е реалистично (например когато по технически причини не е възможно информацията да бъде изтрита, защото това ще доведе до изтриване и на друга, непосредствено свързана информация) и затова трябва да се допусне възможност за "*изваждане от употреба*."[22] Подобно "*изваждане от употреба*" би изисквало администраторът на лични данни:[23]

- да няма възможност да използва личните данни по начин, който да засяга субекта на личните данни;
- да не предоставя достъп на други лица и организации до личните данни;
- да осигури достатъчни технически и организационни мерки зазащита на личните данни;
- да се задължи да изтрие личните данни безвъзмездно, ако и когато това стане възможно;

Австрийският орган за защита на личните данни също дава сходно становище, като според него "*изтриване*" по смисъла на чл. 17 GDPR би могло да бъде осъществено и когато личните данни бъдат **анонимизирани**.[24] Австрийският орган базират становището си на два основни аргумента. На първо място, органът се позовават на съображенията на GDPR, по-специално съображение 26, съгласно което "*принципите на защита на данните н**е следва да се прилагат по отношение на анонимна информация**, т.е. информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице, или по*

---

[21] Information Commissioner's Office, Обединено Кралство, Право да бъдеш забравен, налично на: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

[22] Information Commissioner's Office, Обединено Кралство, Изтриване на лични данни, налично на: https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

[23] Пак там, стр. 5

[24] Австрийски органи по защита на личните данни, становище достъпно на: https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=74ebf6b2-ea8b-4414-a383-1d102d9b678d&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=11.02.2019&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20181205_DSB_D123_270_0009_DSB_2018_00

отношение на лични данни, които са анонимизирани по такъв начин, че субектът на данните да не може или вече не може да бъде идентифициран." На второ място, акцентира върху факта, че дори самият GDPR, когато дефинира понятието "*обработване*" на лични данни в чл. 4(2) прокарва разлика между "*изтриване*" и "*унищожаване.*"[25] Въпреки това, органът поставя ограничение на анонимизацията, а именно: администраторът на лични данни не следва да може да възстанови връзката на данните с даден субект чрез полагането на "*непропорционални усилия.*"[26]

На пръв поглед изглежда, че подобно по-широко тълкуване на термина "*изтриване*" би могло да направи възможно (поне теоретично) приложението на чл. 17 GDPR към блокчейн. Към настоящия момент обаче единствено Френският орган за защита на личните данни е издал официални насоки за съотношението между GDPR и блокчейн технологията. Според френския орган не е необходимо да е налице "*унищожаване*" на данните, а биха могли да бъдат приложени алтернативни методи, например унищожаване на т.нар. "*частен ключ*."[27] По такъв начин конфиденциалността на личните данни би могла да бъде запазена.[28] Въпреки това, органът изрично отбелязва, че към подобни алтернативни мерки следва да се пристъпва предпазливо, доколкото е спорно дали би имало консенсус на ниво ЕС, че подобни действия гарантират в достатъчна степен правата на гражданите на Европейския съюз.

Разбира се, под въпрос остава дали СЕС би приел подобно тълкуване на термина "*изтриване*". В делото Nowak, което касае тълкуване на разпоредбите на Директива 95/46/ЕО, СЕС заявява, че физическо лице - субект на лични данни има право "*да поиска от администратора на данните отговорите му на изпита и коментарите на проверителя по тях след определен период от време да бъдат изтрити,* ***тоест унищожени***." Изглежда, че в

---

[25] „*обработване" означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като [...]* ***изтриване или унищожаване***"

[26] Виж бел. 24: "*Die Entfernung des Personenbezugs („Anonymisierung") von personenbezogenen Daten kann somit grundsätzlich ein mögliches Mittel zur Löschung iSv Art. 4 Z 2 iVm Art. 17 Abs. 1 DSGVO sein. Es muss jedoch sichergestellt werden, dass weder der Verantwortliche selbst,* ***noch ein Dritter ohne unverhältnismäßigen*** *Aufwand einen Personenbezug wiederherstellen kann*."

[27] Частен ключ единият от двойката ключове (публичен-частен), чрез които се осъществява достъп до информацията. За разлика от публичния, частният ключ е известен единствено на притежателя си.

[28] Френски орган по защита на личните данни, Становище - Блокчейн: "Un autre exemple est celui de la suppression de la clé secrète de la fonction de hachage qui aura un effet similaire. Il ne sera plus possible de prouver ou de vérifier quelle information avait été hachée.L'empreinte ne présentera plus, en pratique, de risque sur la confidentialité. L'information devra, ici aussi, être supprimée des autres systèmes où elle aura été stockée pour le traitement," налично на: https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

това дело СЕС възприема един доста стриктен подход, съгласно който "*изтриване*" е еквивалентно на "*унищожаване*." Дали СЕС би запазил подобен подход, в случай че бъде сезиран с преюдициален въпрос по отношение на тълкуването на чл. 17 GDPR в контекста на блокчейн технологиите, **остава неясно**. Следва да се отбележи обаче, че един подобен рестриктивен подход би могъл да се превърне в пречка за технологичното развитие на Европейския съюз и дори да доведе до **техническо изоставането на Европа** в сравнение с други юрисдикции, където се прилага по-адаптивно и гъвкаво законодателство.

Следва да се отбележи, че дори СЕС да възприеме по-широко тълкуване на термина "*изтриване,*" проблемите с приложението на чл. 17 GDPR в контекста на блокчейн не спират дотук. Така например се поставя въпросът дали информацията трябва да бъде изтрита от всички налични устройства ("*нодове*") и ако отговорът е положителен - върху кого лежи правното задължение да осигури изтриването ѝ от всички устройства.

В Мнение 05/2012 от 1 юли 2012г., касаещо "*клауд*" услугите ("*cloud computing*")[29] Работната група по чл. 29 заявява, че правото на "*да бъдеш забравен*" следва да се прилага, независимо дали личните данни се съхраняват на хард диск (т.е. на физически носител) или в друга идеална среда за съхранение (като например т.нар. "*клауд*"). Работната група е категорична, че доколкото личните данни могат да се съхраняват на множество сървъри, разположени на различни локации, **необходимо е да се гарантира изтриването на личните данни от всеки един от тях**.[30] Като се имат предвид техническите сходства между "*клауд*" и блокчейн, може да се заключи, че подобно задължение за изтриване на личните данни съществува и за всеки един "*нод*."

В такъв случай обаче, върху кого лежи правното задължение за изтриване на данните, като се има предвид сложната организационна структура на блокчейн технологията?

На първо място, според чл. 17(1) GDPR "*субектът на данни има правото да поиска **от администратора** изтриване на свързаните с него лични данни*." Така отговорът изглежда прост - задължението лежи върху администратора на личните данни. Кой обаче е администраторът на личните данни в контекста на блокчейн технологиите? Дали това са

[29] Opinion 05/2012 on Cloud Computing, 01.07.2012г., 01037/12/EN, WP 196, достъпно на: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
[30] Пак там, стр. 12

лицата, които създават софтуера; "*копачите*;" "*нодовете*;" или "*потребителите*?" Това е изключително обширен въпрос, който няма да бъде предмет на настоящото есе. Неговият по-подробен анализ е довел някои автори до заключението, че са налице множество **съвместни администратори** по смисъла на чл. 26 GDPR, в т.ч. "*нодовете*" и "*потребителите*," тъй като само те определят не само средствата за обработка на личните данни (за разлика от създателите на софтуера и "*копачите*"), но и целите за обработването.[31] Подобно становище изглежда, че заслужава подкрепа.

Според чл. 17(2) GDPR обаче, когато администраторът е направил личните данни "*обществено достояние*" и е задължен да ги изтрие (т.е. налице е искане по смисъла на чл. 17(1)), той, "*като отчита наличната технология и разходите по изпълнението, предприема разумни стъпки, включително технически мерки,* ***за да уведоми администраторите, обработващи личните данни****, че субектът на данните е поискал изтриване от тези администратори на всички връзки, копия или реплики на тези лични данни*." Тук следва да се отбележи обаче, че задължението по чл. 17(2) GDPR е **задължение за действие, а не за резултат** - т.е. задълженията на администратора на лични данни се изчерпват с информирането на останалите администратори, а не след обезпечаване извършването на активни действия от тяхна страна, насочени към заличаване на данните.[32]

Какъв е практическият резултат? Дори да бъде възприето едно по-широко значение на термина "*изтриване*" по смисъла на чл. 17 GDPR, едно физическо лице - субект на лични данни ще бъде изправено пред няколко изключителни сложни практически проблема: **1**) идентифициране на конкретен администратор на лични данни и насочване на претенция към него; **2**) възможна практическа невъзможност от страна на администратора на лични данни да идентифицира всички останали администратори и да ги информира за искането на субекта на личните данни; **3**) дори всички администратори да бъдат идентифицирани и информирани - възможно бездействие от тяхна страна. Действително, съгласно чл. 26(3) GDPR субектът на

---

[31] Finck, M., Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?, 2019г., стр. 45-49

[32] Съображение 66 от GDPR: "*За тази цел администраторът следва да предприеме разумни мерки, като вземе предвид наличните технологии и средствата на разположение на администратора, в това число технически мерки,* ***за да информира администраторите****, които обработват личните данни, за искането на субекта на данните*."

данни може да упражнява своите права по отношение на "*всеки и срещу всеки от администраторите*." Спорно е обаче дали подобни усилия са пропорционални, като се има предвид възможния огромен брой участници в блокчейна.

Какъв е изводът? От една страна, ако се възприеме буквалното тълкуване на термина "*изтриване*," Европа би била изправена пред катастрофален сблъсък между скорострелно развитие на технологиите и неадаптивни регулаторни мерки. От друга страна, дори да се прилага по-гъвкаво тълкуване на термина "*изтриване*," субектите на лични данни биха се сблъскали с изключително много практически трудности с оглед гарантирането на ефективна защита на правата си. Изглежда, че от ситуацията има два изхода.

Първият вариант - изменение и актуализиране на Регламента, така че да бъде адаптиран към актуалната технологична конюнктура. Вторият вариант би изисквал полагането на **взаимни усилия**, както от страна на техническите специалисти, които стоят зад блокчейн технологията (които да вложат повече ресурси в усъвършенстване на механизмите за защита на правните субекти), така и на държавните регулаторни органи по защита на личните данни (които да окажат нужното съдействие, да дадат необходимите насоки и да осигурят съответните гаранции за защита, което да даде допълнителен тласък за технологичния прогрес на Европа. Разбира се, приложението на единия вариант не изключва другия. Дори Европейският законодател да реши да измени приложимото право, необходимостта от полагането на взаимни усилия на страните в процеса няма да изчезне.

Настоящото есе не изчерпва напълно проблема за приложението на правото "*да бъдеш забравен*" в контекста на блокчейн. Съвсем отделен е въпросът за всички останали проблеми, които вече са възникнали или тепърва ще възникнат във връзка с обработката и защитата на личните данни. Пределно ясно е, че много от тези проблеми няма да намерят решение веднага. Това е основното предизвикателство, което поставя всяка една иновация пред правото. Това, което трябва да се случи обаче е намирането на баланс между развитието на технологията и защитата на правата на гражданите. Такъв баланс, може да бъде осъществен само чрез ясна стратегия, рационални усилия и въвеждането на гъвкави, адаптивни и своевременни мерки, които да позволят по-нататъшното развитие на технологиите (а може би и до възникването на множество бъдещи предизвикателства пред регулаторните мерки).