ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Гергана Върбанова
Адвокатска колегия – Варна

ELECTRONIC IDENTITY AND PERSONAL DATA PROTECTION

Gergana Varbanova, Ph.D
Attorney at law

Резюме: Интернет общуването и дигиталните технологии са неизменна част от ежедневието ни. Предоставянето на електронни публични услуги, нарастващият обем от електронни трансакции и електронният оборот поставят редица въпроси за сигурността на информацията и електронната идентификация на субектите, така че да не съществува съмнение относно участниците в съответните производства или в дигиталния търговски оборот. Поставя се въпросът кой е аналогът на личната карта, който да служи за идентифициране на лицата и другите субекти в дигитална среда. Докладът изследва приложението на електронната идентификация и електронната идентичност в контекста на сигурността на личните данни и възможностите да минимализиране на злоупотребата с лични данни чрез процеса на електронна идентификация.

Ключови думи: електронна идентичност, сигурност, лични данни, електронна идентификация, дигитализация

Abstract: Internet communication and digital technologies are an integral part of our daily lives. The provision of electronic public services, the growing volume of electronic transactions and electronic turnover raise a number of issues with the security of information and electronic identification of entities, so that there is no doubt about the participants in the relevant proceedings or in the digital trade. The question is what is the analogue of the ID card, which should be used to identify individuals and other entities in a digital environment. The report examines the application of electronic identification and electronic identity in the context of personal data security and the possibilities to minimize the misuse of personal data

through the electronic identification process.

Key words: *electronic identity, security, personal data, electronic identification, digitalization*

DOI: <https://doi.org/10.36997/PPDD2021.156>

Въведение

Електронната идентификация ще бъде неизменна част от ежедневието на съвременния човек, който в условията на дигитално общуване предоставя ежедневно личните си данни в глобалната мрежа. Проучване на *Евробарометър* (Attitudes towards the Impact of Digitalisation on Daily, Lives) от месец декември 2019 г. показва, че голяма част от българските граждани използват за целите на електронната идентификация потребителските си профили в социалните мрежи или имейл акаунта си. Голяма част от анкетираните искат да имат контрол върху информацията, която предоставят в глобалната мрежа, в частност, да контролират обема от лични данни, които предоставят както на публично правните субекти, така и на частните лица, а 43% от респондентите заявяват, че не желаят да споделят каквато и да било лична информация и данни, независимо от целите, за които те се изискват. Проучването показва, че обществото подхожда с недоверие към споделяне на лични данни и информация в глобалната мрежа, но същевременно използва и споделя сериозно количество от тях, въпреки нагласите си тези лични данни и информация да останат несподелени. Ситуацията изглежда като *circulus vitiosus*, но достиженията на технологиите дават своето решение – *електронната идентификация*.

Изложение

Електронната идентификация има свое легално определение, което се съдържа в чл.3, т. 1 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО, а именно *електронна идентификация* е процес на използване на данни в електронна форма за идентификация на лица, които данни предста-

вляват по уникален начин дадено физическо или юридическо лице, или физическо лице, представляващо юридическо лице. Понятието *електронна идентификация* по смисъла на регламента е с *по-широк* обхват от понятието електронна идентификация, което влага законодателят в Закона за електронната идентификация (ЗЕИ). Законът регулира само *електронната идентификация на физическите лица* посредством държавна схема за електронна идентификация, докато регламентът предвижда и създаване на *частни схеми за електронна идентификация както на физическите лица, така и на юридически лица, или физически лица, представляващи юридически лица*.

Какво обаче е *електронната идентификация*? Защо изобщо има нужда от нея? Кое е това, което налага създаването на държавни и частни схеми за електронно идентификация, и как това ще повиши сигурността при споделяне на лични данни в интернет?

Концепцията на *електронната идентификация* възниква, за да преодолее един съществен недостатък на интернет. Свързвайки се чрез него с неограничен брой субекти, ние реално *не знаем с кого комуникираме*. Интернет е изграден така, че посредством протоколи се осигурява свързаност между различни устройства в мрежата. При тази свързаност ние *нямаме информация кои са субектите, които са отвъд „машината“* и в чиято правна сфера настъпват определени правни последици. Практически ние *не знаем дали в действителност комуникираме с определен субект*. Тази неизвестност излага потребителите на виртуалното пространство на *риск*, доколкото могат да станат *жертва на измама, кражба на самоличност и правата им да бъдат засегнати от недобросъвестни лица* (Preukschat, Reed, 2021). Нещо повече, макар и в мрежата определени устройства да се идентифицират посредством TCP/IP протокол, тази информация може лесно да бъде преднамерено променена, поради което и информацията за местонахождението на определено устройство в мрежата може да не бъде достоверна. Преодоляването на този проблем може да се осъществи чрез *електронната идентификация и създаването на електронна идентичност*.

Електронната идентичност на физическите лица не е нищо повече от електронно представяне на нашата физическа идентичност, тя е аналог на личната ни карта във виртуалното пространство. Електронната идентификация дава възможност на различните субекти във виртуалното пространство да идентифицират субекта, с който

комуникират (повече за електронната идентификация на <https://blog.bozho.net>, блог на Божидар Божанов). Концепцията за електронната идентичност и електронната идентификация залага на идеята, че информацията която споделят физическите лица в процесът на електронна идентификация е по-контролирана и изцяло зависи от тяхното съгласие. Така, ако трябва да удостоверим самоличността си при предоставяне на административна услуга (физически), ние споделяме цялата налична информация от личната си карта – ЕГН, постоянен адрес, данни за цвят на очите, ръст, място на раждане. В процеса на електронна идентификация обаче, идеята е субектът да сподели само онези лични данни, *които са необходими за предоставяне на определена услуга* и за процеса на електронната му идентификация (Kim Cameron's Identity Weblog 2005). В дадения пример, при заявяване на услуга по електронен път чрез средствата за електронна идентификация, ще бъде предоставена не цялата информация, която е налична и е свързана с дигиталната ни идентичност, а само тази, която е необходима за целите на административното производство – най-често това ще бъде ЕГН, като в процеса на електронна идентификация доверяващата страна получава само нужния й обем от идентифициращи данни. Такова лимитиране на предоставяне на личните данни трудно може да бъде постигнато в аналоговия свят, доколкото няма как да бъде отделена и селективно представена информацията от личната карта на физическите лица. Електронната идентификация и предоставянето само на определена информация от електронната идентичност на субектите намалява риска от злоупотреба с личните данни и на практика е много по-сигурна от физическата идентификация с документи за самоличност. При физическото използване на документи за самоличност рискът от злоупотреба с личните данни, кражбата на самоличност или дори изгубване на документите е по-голям отколкото при средствата за електронна идентификация и електронната идентичност. Освен че процесът на електронна идентификация е изцяло под контрола на субекта, той често е обвързан с технологии, които осигуряват допълнителна сигурност – например процеса на автентикация е обвързан с биометрични данни на субекта на електронната идентификация.

Електронната идентификация има за цел да предостави определена информация от електронната идентичност на даден субект, но самото предоставяне се осъществява чрез процеса на електронна

автентикация. Електронната автентикация има за цел да потвърди, че субектът е именно този, за който се представя, и по този начин неговата дигитална идентичност ще бъде потвърдена (Димитров 2020).

Често субектите ползват акаунт във Facebook, Instagram и др. за достъп и използване на интернет приложения, включително като средство за автентикация и достъп до приложение или игра. Подобен достъп обаче крие своите рискове, доколкото се ползва с ниска степен на сигурност и не използва същинска електронна идентификация и данни за електронната идентичност на съответния потребител. Потребителските профили в социалните мрежи по никакъв начин не гарантират, че лицето, което използва потребителския профил, е това за което се представя. Възможно е профилът в някоя социална мрежа да бъде нарочно създаден с цел кражба на самоличност и злоупотреба с лични данни. В този смисъл интегрирането и използването на електронната идентификация и електронната идентичност, която да бъде ползвана за всички онлайн услуги – публични и частни, биха свели до минимум възможностите за злоупотреба с лични данни. Изследване на Европейската комисия посочва, че малка част от субектите (физически и юридически лица) имат достъп до трансгранична услуга по електронна идентификация. Това мотивира и създаването на нова правна рамка, която задължава всяка държава членка да създаде сигурен, надежден и безпроблемен достъп до трансгранични публични и частни услуги, включително да започне издаването на *европейски портфейл за цифрова идентичност*.

Съгласно предложението за изменение на Регламент №910/2014 европейският портфейл за цифрова идентификация трябва да позволява на потребителите: 1. сигурно да изискват и получават, съхраняват, избират, комбинират и споделят по начин, който е прозрачен за и проследим от съответния потребител, необходимите идентификационни данни за юридическите лица и електронно удостоверяване на атрибути за удостоверяване онлайн и офлайн с цел използване на онлайн публични и частни услуги и 2. да подписват с квалифициран електронен подпис.

Предвижда се период от 12 месеца, в който държавите членки трябва да осигурят възможност за издаване на европейския портфейл за цифрова идентификация. В основата на предложението за изменение на регламента е заложено изискването за най-високо ниво на сигурност на личните данни, използвани за удостоверяване на

електронната идентичност, независимо дали тези данни ще бъдат съхраняват локално или чрез технологично, облачно решение. Предложението за изменение предвижда възможността за използване на биометрични данни като метод за идентификация. Биометричните данни представляват уникална характеристика на човек, поради което и обработването им трябва да отговаря на Общия регламент за защита на личните данни. Основната идея на предложението за изменение на регламента е да се гарантира висока степен на сигурност в областта на електронната идентификация, която да предостави на всички субекти от страните – членки на ЕС сигурна електронна идентификация, приложима както за публичния така и за частния сектор. Чрез европейския портфейл за цифрова идентификация субектите ще могат да се идентифицират свободно в дигитална среда, като сами преценят какви цифрови средства за идентификация ще включат в своя портфейл – професионална шофьорска книжка, професионални или образователни квалификации, паспорт и др. Портфейлът за цифрова идентификация ще осигури възможност за удостоверяване в електронна среда на самоличността на субектите, както и за потвърждаване на тяхно определено качество – управител на търговско дружество, професионална квалификация или придобита специалност. Идеята е тази дигитална идентичност да бъде използвана при предоставяне на публични и частни онлайн услуги, като лицата споделят информация от дигиталната си идентичност и то само толкова, колкото е необходима за предоставяне на услуга или удостоверяване на определено качество на субекта в дигитална среда (повече информация за европейския портфейл за цифрова идентификация е достъпна на: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664). Нещо което е невъзможно да бъде постигнато в аналоговия свят.

Заключение

Технологиите се променят, нуждите от сигурно установяване на дигиталната идентичност на субектите нараства в мащаби, които никога не е предполагал, когато интернет е бил създаден. Електронната идентификация и сигурното удостоверяване на електронната идентичност са предизвикателство не само в областта на технологиите, но и за действащия правов ред, който трябва да отговори своевременно

и адекватно на научния напредък и нуждата от регулация в областта на електронната идентификация и електронната идентичност.

Използвана литература

Димитров, Г. (2020). Автентикация, оторизация, електронна идентичност. Цифрови сертификати, електронни подписи, (<http://eng-dimitrov.com>).

Kim Cameron's Identity Weblog, 2005 The Laws of Identity (2005), (<https://www.identityblog.com/>).

Attitudes towards the Impact of Digitalisation on Daily Lives, (<https://europa.eu/eurobarometer/surveys/detail/2228>).

Preukschat, A., D. Reed (2021). Self-Sovereign Identity – Decentralized digital identity and verifiable credentials. New York: Manning Publications.

<https://blog.bozho.net>

https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664

За контакти: д-р Гергана Върбанова
Адвокатска колегия – Варна
e-mail: gergana@varbanova.bg