СПИСАНИЕ
DE JURE

ОФИЦИАЛНО ИЗДАНИЕ НА
ЮРИДИЧЕСКИЯ ФАКУЛТЕТ НА
ВТУ „СВ. СВ. КИРИЛ И МЕТОДИЙ“

Брой 1/2019 (18), ISSN 1314-2593

ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ

Ивайло Николов

ELECTRONIC IDENTIFICATION

Ivaylo Nikolov

Abstract: *This theoretical overview aims to analyze the law provisions given in the Electronic Identity Act. The overview also regards the process of gradual transition towards e-Justice within the context of the Bulgarian e-government.*

Key words: *e-ID, e-Justice, e-Management, g-Government, ICT.*

ВЪВЕДЕНИЕ

Наличието на законодателна рамка за регламентиране на електронната идентификация е ключов фактор за внедряване принципите на е-управление, е-правосъдие, е-здравеопазване, е-образование. Наличието на законодателна основа и технологични предпоставки за идентифициране на физическите и юридическите лица като правни субекти предоставя възможност за разработване и внедряване на електронни услуги посредством Интернет в здравеопазването, образованието, правосъдието, без да е необходимо физическото посещение на място.

Електронната идентификация е комплексно явление, което се изследва от различни научни направления, като социология, психология, компютърни науки, право и др. Разнообразна е и правната регламентация на това явление, която се определя в голяма степен от нормативната рамка на идентификацията в традиционна среда[1].

1. ОБЗОР НА ДЕЙСТВАЩОТО ЗАКОНОДАТЕЛСТВО В ОБЛАСТТА НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ И ЕЛЕКТРОННОТО ПРАВОСЪДИЕ

Изграждането на ефективно електронно управление в Република България е важна част от процеса на модернизиране на държавната администрация, повишаване качеството на административното обслужване и гарантиране ефективното функциониране на администрацията в условията на пълноправно членство в Европейския съюз[2].

Електронното управление (е-управление) е управление в електронна среда на нормативните взаимовръзки, административните процеси и обслужване и взаимодействието с потребителите с използване на информационни, статистически и математически модели и методи на обработка на данни, информация и знания, които осигуряват много по високо ниво на ефективност на управлението[3].

Електронното правосъдие е средство за повишаване на ефективността на сектор „Правосъдие“ и облекчаване на достъпа до правосъдие от страна на гражданите и бизнеса[4].

Съгласно Стратегията за въвеждане на електронно управление и електронно правосъдие 2014–2020 г. правителството на Република България провежда цялостна държавна политика в областта на електронното управление. Съществено място в стратегията е отделено на електронното правосъдие като средство за повишаване ефективността на сектор „Правосъдие“ и облекчаване

[1] **Хубенова, М**. Електронна идентификация на правни субекти, Автореферат, Софийски университет „Св. Климент Охридски“, София, 2017.

[2] **Михалева, С**. Концепцията „Електронно правителство“ в контекста на Електронното управление. // *e-Journal VFU*, ВСУ „Черноризец Храбър“, № 1, 2015.

[3] Стратегия за развитие на електронното управление в Република България 2014–2020 г.

[4] Стратегия за въвеждане на електронно управление и електронно правосъдие 2014–2020 г.

на достъпа до правосъдие от страна на гражданите и бизнеса. Електронното правосъдие и електронното управление са във взаимовръзка, в технологична и нормативна обвързаност. В тази връзка Министерството на правосъдието и Висшият съдебен съвет въвеждат набор от взаимосвързани средства за:

✓ Опериране с електронни дела и документи от страна на органите на съдебната власт;

✓ Достъп до националните регистри по електронен път в реално време;

✓ Подобряване на взаимодействието и интегрирането на информационните системи на законодателната, съдебната и изпълнителната власт в Република България;

✓ Свързване на националното законодателство и регистри с аналогични европейски регистри и структури;

✓ Предоставяне на административни услуги по електронен път;

✓ Повишаване общата правна култура на гражданите;

✓ Постигане на технологична и семантична съвместимост чрез разширяване на обхвата и максимално прилагане на вътрешните и международните класификатори в съответствие със Стратегията за развитие на електронното управление в Република България 2014–2020, европейското електронно правосъдие и приетата пътна карта, както и поетите ангажименти на сектора към инициативите на ЕС;

✓ Правосъдие максимално близо до и в полза на гражданите и бизнеса.

Основна цел[5] на електронното управление и електронното правосъдие е предоставянето на висококачествени, икономически ефективни и леснодостъпни електронни административни услуги и достъп до правосъдие, ориентирани към гражданите и бизнеса чрез:

– Използване на електронни документи в сектор „Правосъдие“;

– Широк обществен електронен достъп до информация;

– Използване на ***електронна идентичност*** и електронен подпис в сектор „Правосъдие“;

– Предоставяне на комплексни административни услуги по електронен път;

– Облекчен достъп до правосъдие и услуги за гражданите и бизнеса;

– Подобряване на ефикасността и ефективността на администрацията;

– Повишаване на прозрачността и отчетността;

– Намаляване на корупцията;

– Създаване на възможност за участие на структурите на гражданското общество в управлението.

Налице е ускоряване на процесите за поетапно преминаване към електронно правосъдие в контекста на измененията и допълненията в Закона за съдебната власт:

✓ чл. 77, ал. 5 от ЗСВ (обн. ДВ, бр. 103 от 2017 г., в сила от 01.01.2018 г.) относно задължението на бюрата за съдимост при районните съдилища за служебно предоставяне на информация на административните органи или други държавни органи за съдимостта на гражданите по силата на нормативен акт;

✓ чл. 360в, ал. 2 от ЗСВ (в сила от 10.08.2019 г., обн. ДВ, бр. 62 от 2016 г.) относно осигуряване на възможност чрез Единният портал за електронно правосъдие на възможност за:

– заявяване на извършването на удостоверителни изявления в електронна форма;

– извършване на процесуални действия в електронна форма;

– връчване на съобщения и призовки;

– достъп до поддържаните от органите на съдебната власт електронни дела и публични регистри.

✓ чл. 360ж., ал. 1 от ЗСВ (в сила от 10.08.2019 г., обн. ДВ, бр. 62 от 2016 г.) относно изявленията и актовете, подавани до органите на съдебната власт на хартиен носител, както и всички документи и информация на хартиен носител, да се въвеждат в информационната система на органите на съдебната власт чрез снемане на електронен образ във вид и по начин, позволяващи възпроизвеждането им.

✓ чл. 360з., ал. 1 от ЗСВ (в сила от 9.08.2016 г., обн. ДВ, бр. 62 от 2016 г.,) относно образуване на електронно дело при извършване на процесуално действие, което поставя началото на отделно производство.

✓ чл. 360м., ал. 1 от ЗСВ (в сила от 10.08.2019 г., обн. ДВ, бр. 62 от 2016 г.,) относно автоматизираната обмяна на електронни документи между органите на съдебната власт и лицата, осъществяващи публични функции, организациите, предоставящи обществени услуги, и административните органи съгласно Закона за електронното управление.

[5] Стратегия за развитие на електронното управление в Република България 2014–2020 г.

Освен активизиране на законодателната и изпълнителната власт за внедряване принципите на електронното управление и електронното правосъдие Висшия съдебен съвет прие следните наредби в съответствие с измененията в Закона на съдебната власт и Закона за електронно управление:

✓ Наредба № 4 от 16 март 2017 г. (обн. ДВ, бр. № 28/ 04.04.2017 г.) за воденето, съхраняването и достъпа до регистъра на актовете на съдилищата;

✓ Наредба № 5 за организацията и реда за водене, съхраняване и достъп до електронните дела и начина на съхраняване на доказателствата и доказателствените средства по делата, както и вътрешния оборот и съхраняването на друга информация, обработвана от съдебната администрация;

✓ Наредба № 6 за извършване на процесуални действия и удостоверителни изявления в електронна форма.

На основание чл. 25, т. 1 от Регламент (ЕС) № 910/2014 на Европейския съюз „правната сила и допустимостта на електронния подпис като доказателство при съдебни производства не могат да бъда оспорени единствено на основанието, че той е в електронна форма или че не отговоря на изискванията за квалифицирани електронни подписи“, и още в т. 2 се казва: „правната сила на квалифицирания електронен подпис е равностойна на тази на саморъчния подпис“.

В тази връзка са и приетите от Висшия съдебен съвет наредби за регламентиране воденето, достъпа и съхранението на доказателства и доказателствени средства, извършването на процесуални действия и удостоверителни изявления в електронна форма.

2. СЪЩНОСТ И ВИДОВЕ ЕЛЕКТРОННАТА ИДЕНТИФИКАЦИЯ

„Според някои автори[6] електронната идентификация включва два етапа – идентификация и автентификация. Първият от тях, означаван като идентификация, се състои в свързването на определени индивидуализиращи данни с лицето, за което се отнасят тези данни. Той се означава и като разпознаване на лицето. Вторият процес (автентификация, проверка) е процес, при който в последващ момент се проверява дали конкретно лице, което твърди, че е лицето, идентифицирано при регистрацията, е наистина това лице. Други автори[7] разглеждат понятието „електронна идентичност“ като идентификатор на физическото лице, удостоверен от държавен орган и съхраняван върху сигурен носител на електронната идентичност. Електронната идентификация е онлайн процес, чрез който се проверява предоставената електронна идентичност. Данните за идентификация позволяват да се определи самоличността на физическото или юридическото лице. Електронната идентификация позволява идентифициране на самоличността от разстояние. Чрез електронна идентификация е възможно да се осъществи електронно овластяване (делегиране на права) между две физически лица, между физическо лице и стопански субект или между два стопански субекта.

Съгласно чл. 3, ал. 1 от Регламент (ЕС) № 910/2014 на Европейския парламент „електронна идентификация“ означава процес на използване на данни в електронна форма за идентификация на лица, които данни представляват по уникален начин дадено физическо или юридическо лице, или физическо лице, представляващо юридическо лице.

Изхождайки от това определение, електронната идентификация може да бъде класифицирана по следния начин:

1. Автентификация посредством въвеждане на потребителско и име и парола за достъп до системни или приложни системи;

2. Биометрична идентификация;

3. Софтуерно базирана идентификация посредством цифров електронен подпис;

4. Мобилна идентификация посредством мобилен телефон;

2.1. Автентификация посредством потребителско име и парола;

Автентификация (на английски: Authentification) в компютърната сигурност означава удостоверяване на самоличност (истинност) автен-

[6] **Хубенова, М**. Цит. съч.

[7] **Николова, М.** Електронна идентификация и сигурност при електронните комуникации. *// Научен форум „Национална и международна сигурност*“, том IV, 2017, НБУ, с. 295.

тичност[8]. Един от начините за автентификация[9] на потребител пред компютърна система – например операционна система – е да въведе идентификатор, например име на потребител и парола – които разрешават ползването на определен ресурс. Често процесът се нарича „влизане“ или „логин“ (на английски: *login*). След като получи от потребителя въведеното потребителско име и парола, компютърът ги сравнява със стойностите, които се съхраняват в специална база от данни, и ако съвпадат, допуска потребителя в системата. В този случай правилността на паролата гарантира, че потребителят или устройството са автентични. При всяка следваща употреба потребителят трябва да знае и ползва по-рано заявената парола. Слабост на този начин е, че паролите могат да бъдат откраднати, случайно разкрити или просто забравени, което изисква постигане на високо ниво на сигурност за опазване на информационните ресурси.

2.2. Биометрична идентификация

Биометричната идентификация използва биометричните данни за собственика си, като например: форма на лицето, цвят на очите, форма на ушите, височина, отличителни белези (татуировки, видими белези и рани), както и отпечатъци от пръстите и електронни данни за снимката на лицето или други данни, помагащи лицето да бъде идентифицирано със сигурност[10].

В редица случаи биометричната идентификация не би могла да гарантира еднозначно конкретно физическо лице, например при използване на пръстов отпечатък. Причината за това е, че съществуват редица технологии за снемане на пръстови отпечатъци, което създава предпоставки за последващо манипулиране със снетите идентификационни данни, каквито са пръстовите отпечатъци.

Биометричната идентификация би могла да намери своето приложение в процеса на електронна идентификация в комбинация от няколко идентификатора, например ирисова идентификация, пръстов отпечатък и други.

2.3. Софтуерно базирана идентификация посредством цифров електронен подпис

Електронните подписи осигуряват високо ниво на сигурност, което се гарантира посредством криптиране на самия подпис и чрез системата частен-публичен ключ. Електронния подпис бива персонален за идентифициране на физическо лице и професионален, който се издава на физическо лице за идентифициране на юридическо лице. Електронният подпис се записва върху смарт карта и прочитането му става посредством карточетец за смарт карта и въвеждане на персонален идентификационен номер (ПИН код). Цифровите електронни подписи служат както за идентифициране при вход в информационни системи, така и за подписване на файлове (с данни, музика, графика и други).

2.4. Мобилна идентификация

Мобилната идентификация служи за идентифициране посредством мобилен телефон. Недостатък при този вид идентифициране е, че се използва сравнително малкият дисплей на мобилния телефон и малката клавиатура на телефона. Това обаче го прави удачно при условията на мобилност.

3. ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ ПО СМИСЪЛА НА ЗАКОНА ЗА ЕЛЕКТРОННАТА ИДЕНТИФИКАЦИЯ

Съществен момент за въвеждане на електронното управление и електронното правосъдие в регламентирането на електронната идентификация са измененията и допълненията в Закона за електронния документ и електронните удостоверителни услуги, изм. и доп. ДВ бр. 14 от 13.02.2018 г., Закона за електронната идентификация, обн. ДВ. бр. 14 от 13.02.2018 г., в сила от 1.01.2019 г., както и в правилниците за тяхното прилагане.

Електронният идентификатор по смисъла на чл. 2, ал. 1 от Закона за електронната иден-

[8] **Балабанов, М.** Терминологичен речник. – https://sites.google.com/site/bglocalize/dict#A, [online] посетен на 26.02.2018 г.

[9] Wikipedia, Автентификация. – https://bg.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1% 8F_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8 E%D1%82%D1% 8A%D1%80%D0% BD%D0%B0_%D1%81%D0% B8%D0%B3% D1%83%D1%80%D0%BD%D0%BE% D1%81%D1%82), [online], посетен на 26.02.2018 г.

[10] Wikipedia, Биометричен паспорт. – https://bg.wikipedia.org/wiki/%D0%91%D0%B8%D0%BE%D0%B%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%B5%D0%BD_%D0%BF%D0%B0%D1%81%D0%BF%D0%BE%D1%80%D1%82, [online], посетен на 26.02.2018 г.

тификация е уникален идентификатор на физическо лице, за който е издадено удостоверение за електронна идентичност. Електронният идентификатор се съдържа в удостоверението за електронна идентичност и посредством него може да се направи еднозначно разграничаване на едно лице от други лица във виртуалната среда с цел осигуряване на достъп до информационни системи или осигуряване на възможност за извършване на електронни изявления. По този начин националното законодателство ограничава по смисъла на чл. 3, ал. 1 от Регламент (ЕС) № 910/2014 на Европейския парламент електронния идентификатор като съвкупност в буквено-числова поредица, без възможност за прилагане на биометрични методи за идентификация, като например ирисово идентифициране, пръстов отпечатък и други.

На основание чл. 7 от Закона за електронната идентичност орган за електронна идентификация е министърът на вътрешните работи, който издава удостоверенията за електронна идентичност. В този смисъл в Закона за българските лични документи, обн. в ДВ, бр.14/2018 г., са направени редица изменения с оглед синхронизиране на действащото законодателство при издаване на лични документи на български граждани и чужденци от Европейския съюз и трети държави. Основните изменения включват волеизявление на лицата по чл. 4, ал. 1, 2 и 3 от ЗБЛД за издаване ли отказ от генериране на електронен идентификатор и квалифициран електронен подпис на български граждани и чужденци, които притежават единен граждански номер, съответно личен номер на чужденец.

4. СИГУРНОСТ НА ЕЛЕКТРОННИЯ ПОДПИС

На основание чл. 21, ал. 1 от Закона за електронния документ и електронния подпис, изм. доп. ДВ, бр. 14 от 13.02.2018 г., доставчиците на удостоверителни услуги трябва да отговарят на изискванията за сигурност по чл. 19 от Регламент (ЕС) № 910/2014. По този начин законодателно е регламентирано изискването към доставчиците на удостоверителни услуги за предприемане на подходящи технически и организационни мерки за управление на рисковете за сигурността на предоставяните от тях удостоверителни услуги. При тези мерки трябва да се вземат предвид най-новите технически достижения, за да се гарантира, че равнището на сигурност е пропорционално на степента на риска. В частност да се предприемат мерки за предотвратяване и свеждане до минимум на въздействието на инциденти, свързани със сигурността, и за информиране на заинтересованите страни относно нежеланите последици от такива инциденти.

В Регламент (ЕС) № 910/2014 е указано, че в случай на пробив в сигурността или нарушаване на целостта, които имат съществено въздействие върху предоставяната удостоверителна услуга или върху съхраняваните лични данни, доставчиците на квалифицирани и неквалифицирани удостоверителни услуги трябва да уведомяват за това без излишно забавяне, но при всички случаи в срок от 24 часа от момента, в който са узнали за настъпилото събитие, надзорния орган и, когато е приложимо, други компетентни органи, например компетентния национален орган в областта на информационната сигурност или органа по защита на данните.

Когато има вероятност пробивът в сигурността или нарушаването на целостта да окажат негативно въздействие върху физическо или юридическо лице, на което е предоставена удостоверителната услуга, доставчикът на удостоверителни услуги уведомява без излишно забавяне за пробива в сигурността или нарушаването на целостта и въпросното физическо или юридическо лице.

При необходимост и особено ако пробивът в сигурността или нарушаването на целостта засяга две или повече държави членки, уведоменият надзорен орган информира надзорните органи в останалите засегнати държави членки и ENISA.

Ако прецени, че разгласяването на пробива в сигурността или нарушаването на целостта е в обществен интерес, уведоменият надзорен орган информира обществеността или изисква от доставчика на удостоверителни услуги да направи това.

Използването на двойка ключове, частен и публичен, прави електронния подпис сигурно средство за идентифициране. При полагане на електронен подпис се създава уникален шифър, посредством който еднозначно се идентифицира собственикът на електронния подпис чрез публичния ключ, съхраняван в регистъра на удостоверенията на доставчика на удостоверителни услуги.

ЗАКЛЮЧЕНИЕ

Законодателните промени в Закона за електронна идентификация, Закона за електронния документ и електронния подпис, Закона за съдебната власт, Закона за българските лични до-

кументи и съответните наредби създават необходимите условия за поетапно въвеждане принципите на електронното управление в различни сфери като образование, правосъдие, здравеопазване. Наличието на технологична възможност, която гарантира необходимата сигурност за идентифициране на физическите и юридическите лица, създава предпоставки за разработване на различни електронни услуги и внедряването им в различни сфери на държавното управление. Свидетели сме на активната политика от страна на законодателната, съдебната и изпълнителната власт за реализиране на електронното управление в интерес на гражданите, държавата и юридическите лица.

БИБЛИОГРАФИЯ

Балабанов, М. Терминологичен речник. – https://sites.google.com/site/bglocalize/dict#A, [online] посетен на 26.02.2018 г. // **Balabanov, M.** Terminologichen rechnik.

Михалева, С. Концепцията „Електронно правителство“ в контекста на Електронното управление. // *e-Journal VFU*, ВСУ „Черноризец Храбър“, № 1, 2015. // Mihaleva, S. Kontseptsiyata „Elektronno pravitelstvo“ v konteksta na Elektronnoto upravlenie. // *e-Journal VFU*, VSU „Chernorizets Hrabar“, № 1, 2015.

Николова, М. Електронна идентификация и сигурност при електронните комуникации. // *Научен форум „Национална и международна сигурност“*, том IV, 2017, НБУ. // **Nikolova, M.** Elektronna identifikatsiya i sigurnost pri elektronnite komunikatsii. // *Nauchen forum „Natsionalna i mezhdunarodna sigurnost“*, tom IV, 2017, NBU.

Стратегия за развитие на електронното управление в Република България 2014–2020 г. // Strategia za razvitie na elektronnoto upravlenie v Republika Balgaria 2014–2020 g.

Хубенова, М. Електронна идентификация на правни субекти, Автореферат, Софийски университет „Св. Климент Охридски“, София, 2017. // **Hubenova, M**. Elektronna identifikatsia na pravni subekti, Avtoreferat, Sofiyski universitet „Sv. Kliment Ohridski“, Sofia, 2017.

Wikipedia, Автентификация, https://bg.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D1%8A%D1%80%D0%BD%D0%B0_%D1%81%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82), [online], посетен на 26.02.2018 г.

Wikipedia, Биометричен паспорт, https://bg.wikipedia.org/wiki/%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%B5%D0%BD_%D0%BF%D0%B0%D1%81%D0%BF%D0%BE%D1%80%D1%82, [online], посетен на 26.02.2018 г.