РЕЖИМ И ПРАКТИЧЕСКО ПРИЛОЖЕНИЕ НА ЕЛЕКТРОННИТЕ ПОДПИСИ - ОБИКНОВЕН ЕЛЕКТРОНЕН ПОДПИС

Автор:

Адв. Георги Димитров
Адв. дружество Димитров, Петров и Ко.
Хон. преподавател в СУ "Св. Климент Охридски"
Ел.поща: george.dimitrov@dpc.bg

Писмен подпис – електронен подпис

Електронният обмен на съобщения през затворени и отворени мрежи като Интернет стана част от нашия живот. Статистиката показва, че ежедневно се разменят няколко милиарда електронни съобщения. Предимствата са безспорни – икономичност, бързина, улеснение, възможност за неограничено съхраняване на стари съобщения, различни форми за комуникация – видеоконференции, IP телефония, електронна поща, чат, форуми, мейлинг листи и т.н. и т.н. Същевременно комуникационните мрежи се превърнаха в среда за размяна на волеизявления между субектите за встъпване в различни санкционирани от правото отношения и особено за размяна на блага.

Проблемът, с който субектите се сблъскват при този начин на комуникация е свързан със сигурността, целостта и автентичността на изпращаните електронни изявления. С други думи поставя се с острота въпросът как да се установи кой точно е автор на изпратено съобщение, как да се постигне увереност, че съобщението не е променяно от момента на изпращането до момента на получаването и в определени случаи по какъв начин текстът на съобщението да се защити и стане достояние единствено и само на лицето, към което е адресирано.

Такова сигурно средство при традиционните средства за комуникация (напр. чрез писмени изявления) е полагането на саморъчен подпис. Особеностите на движенията на ръката и подобността при полагането му, фактът че подписът се полага под текста на изявлението, както и това, че изявлението и подписът за обективирани върху един и същ материален носител дават увереност за автентичността на изявлението, целостта му и възможност за последваща проверка на тези факти. Липсата на подпис води до затруднения и несигурност при установяването и доказването в евентуален процес на авторството на материализираното върху него писмено волеизявление. Когато едно лице не може на положи саморъчен подпис, като субсидиарно средство за автентификация е полагането на отпечатък от палец.[1]

С развитието на информационните технологии, като аналог на саморъчния подпис и на пръстовия отпечатък, за осигуряване на същата, дори на по-голяма степен на сигурност и възможност за доказване на авторството на електронните изявления, е разработена концепцията за електронния подпис.

Правната уредба на електронния подпис е въведена в нашето право от Закона за електронния документ и електронния подпис.[2]

---

[1] Вж.чл.151 от ГПК
[2] Обн. ДВ бр. 34/06.04.2001, в сила от 07.10.2001, изм. бр.112/2001 в сила от 05.02.2002

Целта на Закона е да приравни по правни последици електронната форма на изявленията с писмената, респ. на електронния подпис със саморъчния. По този начин се създава правна основа за изграждане на сигурността на електронния обмен, с оглед валидността, съдържанието и интегритета на електронните изявления.

Видове електронни подписи. Правни последици

Макар и разработен на основата на Директива 1999/93/ЕС[3], нашият закон има особен подход при дефиниране на понятието "електронен подпис" и при уреждането на статута и правните последици на различните видове електронни подписи.

С Директивата се възвежда уредба на четири вида подписи: обикновен[4], усъвършенстван[5], квалифициран[6] и разширен[7]. Нашият закон урежда два основни вида – обикновен и усъвършенстван и една разновидност на усъвършенствания – универсален подпис.

Съществена разлика съществува в правните последици на различните видове електронни подписи. Според Директивата единствено т.нар. "квалифициран подпис" е приравнен по правни последици на саморъчния подпис[8]. За такъв се счита този, който съдържа реквизити, съгласно Анекс II от директивата, създаден е посредством устройство за сигурно създаване на подписа съгласно Анекс I и за него има издадено удостоверение от доставчик, отговарящ на изискванията на Анекс III от Директивата.

Нашият закон възвежда *относителна правна сила* на различните видове електронни подписи. И обикновения и усъвършенствания електронни подписи са приравнени по правни последици на саморъчния подпис, но само доколкото титуляр или адресат на електронното изявление *не е* държавен орган или орган на местното самоуправление. Единствено универсалният електронен подпис има значението на саморъчен по отношение на всички.[9]

Обикновен е-подпис

"Обикновен подпис" не е легално използувано определение нито от Директивата, нито от нашия закон. То се използува само за улеснение и за отграничението му от другите видове електронни подписи.

Според Директивата обикновен електронен подпис е всяка информация в електронна форма, която е прикачена или логически свързана с друга електронна информация и се използува като средство за автентификация. Например подписването на една електронна поща с "Г.Д." или "Георги Димитров" по смисъла на директивата ще се третира като електронен подпис във всички случаи. Според нашия закон това не винаги ще е така. В повечето случаи подобно подписване въобще няма да се квалифицира като подпис.

---

[3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures
[4] Вж. Чл.2, 1. от Директивата – "electronic signature"
[5] Вж. Чл.2, 2. от Директивата – "advanced electronic signature"
[6] Вж. Чл.5, ал. 1. от Директивата
[7] Арг. от чл.3, ал.2 във връзка с (11) от Преамбюла на Директивата
[8] Чл.5 от Директивата
[9] Чл.13, ал.2 и 3 от ЗЕДЕП

Обикновеният електронен подпис по нашия закон се третира много по-стриктно. Ако трябва да се направи някаква аналогия, то обикновеният електронен подпис е приравнен като изисквания с усъвършенстваният електронен подпис по смисъла на Директивата.

Електронен подпис съгласно чл.13 от Закона е само тази информация, която е свързана с електронното изявление по начин, съгласуван между автора и адресата, достатъчно сигурен с оглед нуждите на оборота, който: а) разкрива самоличността на автора; б) разкрива съгласието на автора с електронното изявление, и в) защитава съдържанието на електронното изявление от последващи промени.

Доколкото нашият закон почива на доброволността на използването на електронната форма за размяна на волеизявления между субектите[10], то и използването на електронния подпис следва да бъде обусловено от съгласуваната воля на страните. За електронен подпис ще се счита само тази информация, която страните са определили *предварително* или *последващо* като начин за идентификация при размяна на електронните изявления. Така например, ако с колегата ми приемем, че ще използваме нашите инициали положени под разменяните по електронна поща изявления за идентифицирането ни (напр. "Г.Д." и "Б.П"), то тяхното полагане ще се счита за електронен подпис в нашите отношения. От използването на законовия термин "съгласуване" може да се остане с погрешно впечатление че е необходимо страните предварително да са определили начина на идентифициране. Такова тълкуване е погрешно. Няма пречка и след размяната на волеизявленията страните да определят, че използваният начин следва да се счита за електронен подпис.

Само съгласуването, разбира се, не е достатъчно. Като елемент от фактическия състав на нормата е въведен относителен обективен критерий – начинът на свързване на идентифициращата информация (електронния подпис) следва да е "*достатъчно сигурен с оглед нуждите на оборота"*. Поставя се въпрос: за нуждите на кой оборот следва да се преценява "достатъчната сигурност" – въобще за нуждите на оборота на съответните стоки или услуги или на оборота конкретно между субектите (напр. между мен и колегата ми)? Смятам следва да се приеме за правилна втората постановка. Един е оборотът и нуждите от сигурност на търговците на стомана на едро, други са между хлебаря и редовния му клиент. Ясно е че първите ще наложат по-високи изисквания за сигурност, а вторите – по-ниска.

Критерият е обективен, защото необходимостта от сигурността на конкретния оборот е факт от обективната действителност, съществуващ извън съзнанието на субектите. От друга страна, обаче, той е и относителен, доколкото степента на сигурност следва да се преценява в зависимост от правните качествата на различните субекти (напр. дали са търговци или не) и правоотношенията, по повод на които разменят волеизявления.

За да се определи степента на "достатъчна сигурност" на начина на свързване на идентифициращата информация с електронното изявление, законът предпоставя три кумулативно дадени условия.

На първо място е необходимо идентифициращата информация да разкрива самоличността на автора. Това е разбираемо. Средството за идентификация изпълнява ролята си само тогава, когато носи информация, по силата на която адресатът може да изгради пълна увереност, че изявлението изхожда от точно определен автор. Ползването на инициали, псевдоним, галено име, пълно име, фамилно име, особен символ, често

[10] Арг. от чл.5 от ЗЕДЕП

ползуван от автора, прякор и т.н. са все възможни начини за идентифициране, разкриващи самоличността на автора.

На второ място е необходимо идентифициращата информация да е свързана с електронното изявление по такъв начин, че да разкрива съгласието на автора с електронното изявление. Докато при традиционните писмени документи полагането на саморъчния подпис под писменото изявление изпълнява успешно тази функция (с някои изключения), то при електронния подпис това не е задължително. Ако информацията за автора, съдържаща се в служебния идентификатор на изпратената електронна поща носи достатъчно индивидуализиращи белези за самоличността му, а изявлението е ясно и недвусмислено, то условието да се разкрива съгласието на автора с електронното изявление ще бъде изпълнено. Страните могат да уговорят всякакъв начин на свързване, за да се постигне тази увереност.

Много въпроси поставя третата предпоставка за начина на свързване на идентифициращата информация за да се приеме, че е налице валиден електронен подпис. Законът установява, че свързването следва да става по начин, защитаващ съдържанието на електронното изявление от последващи промени. Разглеждането на нормата през призмата на най-съвременните способи и методи за сигурна защита на съдържанието на предавани електронни пакети с информация може да доведе до неправилното й тълкуване. Правилото не следва да се абсолютизира. При обикновените електронни подписи не е необходимо прилагането за такива методи за защита на съдържанието, както при усъвършенстваните електронни подписи. Достатъчно е ползуването на методи чрез алгоритми на симетрична криптография (с един и същ ключ се криптира и декриптира съдържанието), използуване на по-малко сигурни методи на асиметрична криптография (с различни ключове се извършва защитата и проверката)[11], стандартизирани методи за защита, използувани при традиционните клиентски софтуерни приложения за размяна на електронни изявления и т.н. Идеята на законодателя е била да има някакво ниво на сигурност и защита на съдържанието. Достатъчно е страните да го приемат за сигурно.

При наличието на всички предпоставки на чл.13, ал.1 идентифициращата информация ще се счита за електронен подпис с всички произтичащи от това правни последици.

Могат да се приведат някои практически примери за това кога ще се счита, че е налице полагане на обикновен подпис. Това ще са всички случаи на използуване на PGP[12] криптографски ключове, на усъвършенствани подписи, удостоверенията за които са издадени от чуждестранни доставчици и не е призната правната им сила на територията на Република България[13], генерирани симетрични и асиметрични ключове от клиентски софтуери за обикновена електронна поща, генерирани псевдослучайни ключове за временна свързаност по различни протоколи[14] и т.н.

Интерес представлява въпросът какви ще са последиците от използуването на подписи, удостоверенията за които не отговарят на изискванията на чл. 24. Така, ако доставчик на удостоверителни услуги по нашия закон издаде удостоверение с липсващи задължителни реквизити по чл.24, то изявлението няма да се счита подписано с усъвършенстван електронен подпис. Това не означава, обаче, че ще изявлението ще се счита неподписано с електронен подпис въобще. Ако от тълкуване волята на страните може да се установи, че

---

[11] Напр. шифровани със сложност по-малка от 64 бита.
[12] Pretty Good Privacy
[13] Понастоящем някои от по-известните са: Thawte, VeriSign, GlobalSign, Belgacon, Microsoft и др.
[14] Напр. по https

са приели да считат за подписани разменените електронни съобщения независимо от вида на електронния подпис – усъвършенстван или универсален, то подписаният, но придружен с невалидно удостоверение документ ще се счита подписан с обикновен подпис и ще обвърже титуляра по същия начин, както ако би бил използуван усъвършенстван подпис. Ще е налице конверсия на електронния подпис.

В общия случай изпращаните съобщения по електронна поща при липса на изрична и ясна воля на автора и адресата и при липса на някоя от предпоставките по чл.13 няма да се считат подписани с електронен подпис. Това, обаче, не лишава заинтересованата страна да докаже авторството на неподписания електронен документ в рамките на гражданския процес.

Следва …