05.03.2014
http://computerworld.bg

Правни аспекти при управление на данни в Облака и Големи данни

Анализ на доц. д-р Георги Димитров и адв. Десислава Кръстева от адвокатско дружество „Димитров, Петров и Ко.", специализиращо в защитата на личните данни и авторските права

„Димитров, Петров и Ко." е адвокатско дружество със седалище в гр. София, България. От основаването си през 1997 г. на името на съдружниците д-р Георги Димитров и адв. Богдан Петров, кантората се специализира главно в областта на търговското право, право на информационните и комуникационни технологии, право на интелектуална собственост, недвижими имоти и процесуално представителство.

Доц. д-р Георги Димитров е основател и съдружник на адвокатско дружество „Димитров, Петров и Ко.". Ръководи Отдела по право на информационните и комуникационни технологии (ИКТ) и Отдела по защита на интелектуалната собственост. Той е и учредител и старши експерт във Фондация „Право и Интернет" и понастоящем е председател на УС на организацията.

Адв. Десислава Кръстева е старши адвокат в адвокатско дружество „Димитров, Петров и Ко.", към което се присъединява през 2005 г. Член е на Управителния съвет на Фондация „Право и Интернет" от ноември 2004 г. Специализира в електронна търговия и Интернет право, телекомуникационно право, защита на личните данни, договорно право, дружествено и търговско право.

доц. д-р Георги Димитров, адвокатско дружество „Димитров, Петров и Ко."

адв. Десислава Кръстева, адвокатско дружество „Димитров, Петров и Ко."

- Какви са най-често срещаните юридически казуси, свързани с управлението на Големи данни и съхранение на данни в облака? Има ли юридически специфики при частния и публичния облак?

При навлизането и използването на нови технологии е трудно да бъдат предвидени всички казуси, които могат да възникнат. Технологиите и възможностите, които те предлагат, се развиват с много по-голяма бързина от правото. При все това, на този етап правните въпроси, които възникват пред управлението на Големи данни, са свързани приоритетно със защитата на личните данни. Така например, се поставят въпроси, свързани с т. нар. профилиране. Не е ясно дали и колко често се извършва такова профилиране, а и възможността да се контролира и проверява дали са налице такива дейности, е силно ограничена. И все пак, все по-често ставаме свидетели на явления, които сочат за наличието на подобни практики – напр. таргетираната реклама. Големите данни представляват огромни масиви от информация. В тях може да се включват всевъзможни данни като колко и за какво харчим, какви търсения и интереси имаме, с кого общуваме, какво работим, какво ядем и пием, спортуваме ли, къде, какво, през какви маршрути, дали искаме да отслабнем и колко, от какви заболявания се интересуваме, какво четем, дали и къде пътуваме, наши физиологични и здравни показатели и т.н., и т.н. Например, можем да се замислим за информацията, която става известна за нас, когато използваме комплексни услуги като тези предлагани от Google (привързване на социална мрежа, с е-поща, търсачка и ред. др. приложения), Amazon.com, Facebook, iPhone с цялата съвкупност от услуги и приложения, включващи и iCloud, iTunes и т.н., и редица други. На базата на такъв набор от информация могат да се изграждат профили, т.е. „картина" (комплексна представа) за личността, характера и личните ни предпочитания, за склонността ни към радикални действия, за адаптивността ни в обществото и прочие. Нещо повече, чрез автоматизирано обработване на Големи данни и с използването на предварително зададени алгоритми могат да се предвиждат и предстоящи събития в нашия живот (раздели, бременност, здравословни проблеми и т.н.). Профилирането само по себе си почти никога не се осъществява с пълното знание на лицата, за които се отнася, което само по себе в голяма част от случаите може да се разглежда като накърняване на нашето право на неприкосновен личен живот. То често е свързано и с вземане на автоматизирани решения (т. е. само на базата на автоматизирана обработка на данните), които са съществени за нашите права или интереси, а това е дейност, която в ЕС е забранена и се допуска само по изключение в много ограничен брой случаи.

Възникват и редица въпроси относно контрола върху обработването на Големите данни и върху осъществявания до тях достъп, тъй като често т.нар. Големи данни се обработват и достъпват от лица, които са разположени на територията на различни държави. По-конкретно, със значителна сложност, но често срещани, са въпроси като правилата на коя държава се прилагат при положение, че информацията се събира, достъпва или обработва от лица, които са разположени в различни държави, кои от тези лица отговарят за сигурността и законосъобразното обработване на данните, как да защитят правата си лица, чиито данни се обработват по такъв начин в случаите, когато лицата, които извършват обработването са в друга/и държава/и т. н.

Що се касае до съхранението на информация „в облака", то въпросите, които се поставят понастоящем са преди всичко относно сигурността на информацията, контрола върху нея или съответно върху спазването на приложимите изисквания за нейната защита (в случаите, когато има такива), както с отговорността при нарушение на сигурността на информацията и др. под. Когато говорим за съхранение на информация „в облака" е от изключителна важност да се подчертае, че потребителят обичайно не знае къде физически се съхранява информацията. Тя би могла да бъде разпръсната в различни центрове за данни, разположени в различни държави – факт, който затруднява изключително много определянето на приложимите правила относно сигурността на информацията, контрола върху дейността на доставчика и т. н. Освен това, доставчиците на „облачни" услуги имат достъп по всяко време до информацията и потребителите не биха могли да осъществяват контрол върху този достъп – те не знаят дали, кой, кога или защо е достъпвал тяхната информация. Поради това се счита, че съществуват сериозни рискове за неоторизиран достъп до информацията, за нерегламентираното й разпространение – било инцидентно, било умишлено и дори за загубата или унищожението й.

Интересни въпроси възникват и в ситуации, при които европейска компания (т.е. компания, задължена да спазва строгото европейско законодателство относно защитата на личните данни) използва такъв тип услуги, за да съхранява обработваните от нея лични данни. В тези случаи администратор на данните е и си остава единствено европейската компания и тя е тази, която отговаря за осигуряване сигурността на данните и за съобразяване на обработването им с всички изисквания на ЕС. Така при евентуален инцидент или разкриване на данните компанията може да понесе сериозни санкции, докато възможността й да потърси след това възстановяване на вредите от страна на доставчика ще е под въпрос и ще зависи от конкретните уговорки в договора между тях. И това не е всичко - в подобна ситуация възникват и далеч по-сложни правни въпроси, свързани с ограничителния режим в ЕС относно предоставянето на данни към трети държави. Ако доставчикът на услугата е извън ЕС, то европейската компания е нужно да предприеме специални мерки, за да осигури адекватна защита на данните, докато се обработват извън ЕС. Къде е разположен доставчикът на услугата, обаче, както стана ясно, съвсем не е показателно за това къде са самите данни – те биха могли и вероятно са разпръснати в различни държави. В тази връзка е доста съмнително дали е обективно възможно да се осигури адекватна защита, дали и доставчикът би могъл да гарантира такава, след като данните ще се обработват на оборудване, което е разпръснато в различни държави с напълно различно законодателство, а от там е доста съмнително и дали предприетото от европейската компания предоставяне на данните е съобразено с изискванията в ЕС. Неясен е и въпросът как следва да се процедира, ако самият доставчик е в ЕС, но пък използва оборудване, което е разположено извън ЕС.

Възникват и в бъдеще ще възникват и все повече договорни казуси (с оглед ангажиране отговорността на доставчиците), конкурентно-правни казуси, казуси, свързани със защитата на права на интелектуална собственост и т. н. Така например, един от ключовите моменти, свързани с осигуряването на

лоялна конкуренция, е да не бъде обменяна между и да не бъде достъпвана от конкуренти чувствителна бизнес информация. С прости думи, ако една компания по някакъв начин получи ключова информация относно бизнес плановете, резултатите и други подобни на неин конкурент, тя може да вземе решения за собствения си бизнес, които да повлияят на пазара – напр. ако едната компания планира да увеличи или намали своите цени, другата компания също ще промени ценовата си политика и то в момент, съгласуван с плановете на конкурента й; ако едната компания планира пускането на нов непредлаган преди продукт, другата компания би могла да откраднe идеята и да изпревари конкурента си и т.н.

Основната разлика при публичния и частния облак е свързана с това кой „притежава" облака, т.е. дали за да съхраняваме информация в облака използваме услугите на външен доставчик или определено лице (обикновено голяма компания) изгражда собствена облачна структура, която използва за съхраняване на своя собствена информация. При т. нар. публичен облак възникват повече въпроси, свързани с уреждане на отношенията между доставчика на услугата и лицата, които желаят да я използват. Разгледаните конкретни примери и проблеми са свързани именно със случаи на използване на т.нар. публичен облак. Такива въпроси, обаче, не е изключено да възникнат и при т. нар. частен облак – напр. ако се използва оборудване разпръснато в различни държави; ако този „частен" облак всъщност не е предназначен да се използва само от една компания, а от цяла група свързани компании, което е обичайна практика и т.н.

- Какви са регулациите в ЕС относно защитата на авторските права и лицензирането при изграждането на частен облак, хармонизирано ли е националното законодателство с европейското?

Към настоящия момент липсват специални правила, които да касаят защитата на авторските права „в облака". По отношение на защитата на авторските права в контекста на „облачните" услуги, подобно и на защитата на авторските права в Интернет, се прилагат общите правила, които са неутрални по отношение на използваните технологии. Непозволеното използване или разпространение на определено авторско произведение би било нарушение независимо дали при извършването са използвани такива технологии или е извършено без използването на каквито и да е технологии. Що се отнася до българското законодателство в тази сфера, то също като цяло е хармонизирано с европейското.

По отношение на лицензирането при изграждането на „частен" облак, ако се има предвид лицензирането на софтуерните приложения, необходими за изграждането на такъв облак, не възникват специфични въпроси. Всеки, който желае да използва определен софтуерен продукт следва да се съобрази с лицензионните изисквания, които се поставят от носителя на правата върху този софтуер. Това важи включително и за случаи, при които софтуерът, който се използва е предоставен за безплатно ползване. В тези случаи лицата, които желаят да го използват отново следва да се съобразят с лицензионните ограничения, поставени от притежателя му – напр. забрана да се използва за търговски цели, забрана да се преработва, забрана да се препродава на трети лица и т.н.

- Как се регулират и регламентират управлението, и съхранението, както и правата върху данни, когато доставчикът е в една държава, а центърът за обработка на данни – в друга?

Както вече отбелязахме, това е обичайната ситуация при съхранение на данни в облака, а именно – възниква необходимост да се определи кои са приложимите правила, т.е. законите на коя държава се прилагат, за да се регламентира съответната дейност. Нещо повече, при казуси, свързани с Големи данни или със съхранение на данни в облак, в повечето случаи въпросът за приложимите правила може да касае законодателството на много повече от две държави. Поради това, за да се определи как се регулират управлението, съхранението и правата върху данните са от значение редица фактори. В общия случай режимът, който се прилага по отношение на данните зависи от това в коя държава е лицето, чиято собственост са данните, а не от това коя е държавата на доставчика или къде чисто технически се извършва обработването на данните. Въпреки това, в държавата на доставчика може да са налице определени специални правила, които да създават задължения за същия във връзка с предоставяната от него услуга (напр. задължение на доставчика да предоставя достъп на държавни органи от неговата държава до информация, която не е негова, но е съхранена на негово оборудване при ползване на услугата). В зависимост от това къде се извършва техническите обработването на данните, къде е разположено оборудването или къде са разположени лицата, които достъпват и обработват данните, за лицето, което ползва услугата може да възникнат специфични задължения, напр. да е необходимо да се съобразят допълнителни изисквания относно обработването и предоставянето на лични данни в трети страни. Това касае напр. разгледания по-горе случай, при който европейска компания използва такъв тип услуга. На следващо място, в контекста на защита на личните данни, приложимо би могло да бъде и правото на държавата, в която пребивава лицето, чиито права са нарушени и което търси закрила. Ако български гражданин е претърпял вреди поради злоупотреба с негови лични данни, той би могъл да предяви иск в България, независимо че злоупотребата се е осъществила извън България. Ако се касае пък за казус, свързан със защита на права на интелектуална собственост ще е от значение и в коя държава търси защита автора и т.н., и т. н.

- Мнозинството Интернет потребителите са на мнение, че предоставят твърде много лични данни, без да имат възможност да упражняват контрол над предоставената лична информация. Как се гарантира защитата на личните данни в публичния облак в България, в ЕС и по света?

Не може да се говори общо за гарантиране защитата на личните данни в публичния облак в България, в ЕС и по света, тъй като липсва обща и еднаква регулация, която да е валидна и приложима за цял свят. Хармонизиране и относително еднакви правила и гаранции има единствено в рамките на ЕС, като дори и в тези случаи прилагането на иначе еднаквите правила в различните държави-членки разкрива някои различия. Основният и най-ефективен механизъм, за да си гарантират Интернет потребителите защитата на техните лични данни, е тяхната внимателна преценка дали да предоставят и разкрият своя лична информация. Ако някой потребител счита, че му се изискват твърде много лични данни, би могъл да откаже да ги предостави. При предоставянето на лични данни в Интернет обикновено говорим за доброволно предоставяне, а последиците от отказа да предоставим нашите лични данни в най-лошия случай биха били свързани с невъзможност да се използва определена услуга. Важно е да обръщаме внимание и дали доставчикът, на който предоставяме личните си данни, действително ги изисква или предоставянето им е само опция. Предварителното запознаване с това на кого предоставяме информацията си, къде е позиционирано това лице, за какво ще бъде използвана тази информация, какви политики по отношение на личната информация прилагат, която предоставяме е основният начин да се предпазим от нежелано навлизане в личното ни пространство. Важно е също така да се знае, че повечето държави извън ЕС са възприели значително по-либерални правила относно защитата на личните данни в сравнение с ЕС, а в редица държави дори напълно липсва уредба в тази сфера. Поради това доставчиците на услуги, които са извън ЕС, често нямат задължението да осигуряват съществени гаранции за защита на личните данни, разполагат с доста гъвкави възможности да променят политиките си относно защитата на личните данни и др. подобни.

Въпросите зададе Константа Григорова