Модели за защита на личните данни

Дейвид Банисар[1]

В съвременния свят има много предизвикателства пред правото на защитата на личните данни. Правителствени организации събират големи масиви лични данни при изпълнение на техните задължания. Новите технологии създават възможност за получаване на медицинска, генетична и други видове информация, каквато не се е събирала преди. Когато отделни хора сърфират из Интернет и осъществяват онлайн транзакции, те остават след себе си подробни следи от лични данни. Компютърните и мрежови технологии създават нови неподозирани проблеми, породени от събирането, разпространението и използването на информация по нови начини.

Различните правителства реагират по различни начини на тези предизвикателства. Бихме могли да отбележим четири различни модела за защита на личните данни – изчерпателно законодателство, секторно законодателство, саморегулация и технологични защити. В зависимост от тяхното приложение, тези модели биха могли да се допълват или да си противоречат, като в много страни няколко от тях се използват заедно. В държавите, които гарантират най-добре правото на защита на личните данни, всички тези модели работят едновременно и се допълват.

Определение на правото на защита на личните данни

Правото на защита на личните данни се определя от отношенията между личността и обществото, включително правителствените институции, фирми и други личности. Това право покрива широк кръг въпроси, между които тайната на лична кореспонденция, защитата на дома и семейството и неприкосновеността на личния живот. Неприкосновенността на личния живот е в основата на човешкото достойнство

[1] Авторът е гостуващ учен в Департамента по Право на Университета в Лийдс, Великобритания, стратегически консултант на Институт "Отворено общество" и заместник-директор на Privacy International. Преди това е бил гостуващ учен при Информационен Инфраструктурен Проект, Kennedy School of Government, Harvard University и основател и стратегически директор на Центъра за електронна защита на на личните данни във Вашингтон. Част от този материал е публикуван в Лични данни и човешки права (EPIC/PI 2000).

и други ценности, като свободата на изразяването и правото на свободно сдружаване и поради това е едно от най-основните човешки права в съвременността.

Правото на защита на личните данни има широко международно признание. То е оценено като основно човешко право във Всеобщата Декларация за Човешките Права и Основни Свободи, както и в други международни договори. В повечето държави правото на защита на личните данни е част от конституцията. Като минимум тези норми предвиждат право на защита на дома и защита на кореспонденцията. Повечето от по-новите конституции предвиждат право на достъп и контрол върху собствените лични данни. В много държави, чиито конституции не предвиждат отделно защитата на лични данни, съдебни решения се позовават на други правни норми, като зачитат това право. На други места международни споразумения, уреждащи това право - като Международния пакт за граждански и политически права и Европейската конвенция за защита на правата на човека и основните свободи – са част от националните законодателства.

Зашитата на неприкосновеността личния живот е дълбоко заложено в историята още от библейски времена. В по-близкото минало, в доста държави се приемат и закони, които защитават гражданите от публикуването на техни лични данни. През 1858 във Франция се забранява публикуването на факти от личния живот и се приемат строги мерки срещу евентуални нарушители.[2] През 1889 норвежкият наказателен кодекс забранява публикуването на информация, засягаща "лични или семейни дела".[3] През 1890 г. американските юристи Самюел Уорън и Луис Брандайс издават фундаментална публикация, в които описват правото на защита на личните данни като право "да бъдеш оставен намира"[4], а неспазването му - като закононарушение. След тяхната публикация, идеята, че при нарушаване на това право пострадалите могат да заведат съдебен иск, става част от американското прецедентно право.

В ерата на информацията, правото на защита на личния живот налага поставянето на ограничения върху събирането, разпространяването и използването на лична информация, която се съхранява от правителствени структури, частни фирми и други организации. Тези правила са обикновено известни като "защита на личните данни". Интересът към това право на защита се увеличава през 60-те и 70-те години на 20 век с развитието на информационните технологии. Потенциалът на мощните компютърни системи за наблюдение предизвиква искания за конкретни правила, регулиращи събирането и обработката на лични данни.

Принципи за коректност към личните данни

---

[2] The Rachel affaire. Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62. See Jeanne M. Hauch, Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris, 68 Tul. L. Rev. 1219 (May 1994).

[3] See prof. dr. juris Jon Bing, Data Protection in Norway, 1996.
<http://www.jus.uio.no/iri/rettsinfo/lib/papers/dp_norway/dp_norway.html>.

[4] Warren and Brandeis, The Right to Privacy, 4 Harvard Law Review 193 (1890).

През последните 30 години, се развива набор от правила, известни като "принципи за коректност към личните данни" (ПКЛД). Тези принципи са предложени за първи път от Американското Министерство на Здравеопазването, образованието и благосъстоянието през 1974 и по-късно стават част от законодателствата на много държави. На основата на тези принципи, през 1981 г. Организацията за икономическо сътрудничество и развитие представя разширени препоръки, които впоследствие се приемат в целия свят.[5]

Като използват тези постижения, работна група от потребители, представители на правителствени и бизнес организации към Канадската асоциация по стандартизация (КАС) разработват следните "принципи за коректност към данните", които стават част от канадския закон през 2000 г.[6]

- **Отчетност**: Институциите са задължават да опазват личните данни, които съхраняват и да назначат служител, или служители, които са отговорни за изпълнението на следните принципи в институцията.
- **Определяне на целта**: целите, за които се събират лични данни трябва да са определени от институцията преди или по време на на събиране на информацията
- **Съгласие**: Знанието и съгласието на лицата са задължителни при събирането, използването, или разкриването на личните им данни, освен когато това е неуместно.
- **Ограничено събиране**: Събирането на лични данни трябва да е ограничено само в рамките на неоходимото за целите, определени от организацията. Информацията трябва да се събира по законен и обективен начин.
- **Ограничено използване, разкриване и съхранение**: Лични данни не могат да се използват или разкриват за цели, различни от тези, за които са били събрани, освен със съгласието на лицето или в случаи, предвидени в закон. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели.
- **Прецизност**: Личните данни трябва да са прецизни, пълни и актуални, доколкото това е необходимо за целите, за които се използват.
- **Опазване**: Личните данни трябва да са защитени с мерки за сигурност, съответстващи на чуствителността на информацията.
- **Откритост**: Институциите трябва да осигуряват свободен достъп до информация за политиките и практиките свързани с управлението на личните данни.
- **Право на достъп**: При подаване на заявление, гражданите трябва да бъдат информирани за съществуването, използването и разкриването на техни лични данни и трябва да могат да получат достъп до тях. Гражданите трябва да имат възможността да проверят точността и пълнотата на техните лични данни и да ги поправят ако е необходимо.

[5] OECD, “Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data” Paris, 1981. < http://www1.oecd.org/publications/e-book/9302011E.PDF>.

[6] Bill C-6, Personal Information Protection and Electronic Documents Act <http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html>.

- **Възможност за контрол**: Гражданите трябва да имат възможността да проверят дали тези, които използват или събират техни лични данни, спазват горните принципи, като отправят питане към определения служител, или служители.

Модели за защита на личните данни

Изчерпателно законодателство

В над 40 държави има общи закони, които регулират събирането, използването и разпространяването на лични данни както от правителствени структури, така и от частни компании. Други около 20 държави са в процес на приемане на нови закони. Всички те възприемат принципите за коректност към личните данни, описани по-горе.[7]

Първият изчерпателен закон за защита на личните данни е приет в немската провинция Хесен през 1970 г. Впоследствие Швеция (1973г.), Германия (1977г.) и Франция приемат подобни закони.[8] В САЩ (1974г.) и Канада (1981г.) се приемат закони, които изчерпателно регулират правителствения, но не и частния сектор.

През 1981г. Съвета на Европа приема конвенция за автоматизираната обработка на лични данни.[9] Тази конвенция отразява принципите за коректност към личните данни, като определя правила за трансгранично прехвърляне на лични данни и създава механизми за международно сътрудничество. Много държави в Европа приемат закони след приемането на Конвенцията, ефективно влязла в сила през 1985г., с което осигуряват безпрепятствано прехвърляне на информация. Днес, 34 държави са подписали Конвенцията и 30 са приели закони за нейното прилагане.

Директиви за защита на личните данни на Европейския съюз

Важна стъпка в развитието на правото на защита на личните данни е приемането през 1995г. на Директивата по защита на личните данни. Целта на тази директива е да хармонизира законите в Европейския Съюз, да осигури надеждна защита на правата на гражданите и да позволи свободен пренос на лични данни в между страните на ЕС. [10] Всяка страна-членка на ЕС е задължена до Октомври 1998г. да приеме закони осигуряващи прилагането на Директивата, но до 2003г. някои държави все още не я прилагат изцяло. Някои от страните в процес на присъединяване са приели подобни закони.

---

[7] See Privacy and Human Rights 2002 (EPIC/PI) available at http://www.privacyinternational.org/survey/, Council of Europe Status of Ratifications of Treaty 108, http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=108&CM=8&DF=10/04/03

[8] Прекрасен анализ на законодателството може да бъде намерен в David Flaherty, Protecting Privacy in Surveillance Societies (University of North Carolina Press 1989).

[9] Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Strasbourg, 1981. < http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=108&CM=8&DF=10/04/03 >.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm>.

Основна промяна в Конвенцията на Съвета на Европа е разширяването на правата върху неелектронни носители. Всяка страна от ЕС трябва да създаде Комисия по защита на личните данни или агенция, която да следи за изпълнение на закона. Директивата създава задължение към страните членки да осигури еднакво ниво на защита на личните данни, когато те се прехвърлят или обработват в страни извън ЕС. Това задължение оказва голям натиск върху страните извън Европа да приемат закони за защита на личните данни. Тези държави, които отказват да приемат адекватни закони за защита на личните данни, могат да се окажат в положение на невъзможност да обменят определени видове информация с европейските страни. Това се отнася особено до някои категории чувствителна информация. След направена оценка от Комисия в няколко страни, включително Унгария, Швейцария, Аржентина и Канада, условията на защита на личните данни са оценени като адекватни. Отделно и донякаде противоречиво споразумение за сигурност е прието със САЩ, позволяващо прехвърлянето на информация към конкретни компании, които се задължават да спазват ПКД.

Европейският съюз разширява приложението на Директивата за защита на личните данни, като приема Директива за защита на личните данни свързани с телекомуникациите през 1997г.[11], която урежда конкретна защита при прехвърляне на данни по телефон, дигитална телевизия, мобилни мрежи и други комуникационни системи. Директивата въвежда обширен кръг задължения към носителите и доставчиците на услуги, за да осигури защита на личните данни на потребителите на услуги, свързани с Интернет. След двугодишен дебат, през юли 2002, Европейският съюз приема нова директива, която по-ясно покрива Интернет комуникациите и слага ограничения върху рекламните e-mail-и (спам).[12] Въпреки това, поради натиска от страна на разузнавателни и правоприлагащи организации от ЕС и американското правителство, директивата отслабва задълженията за събиране на транзакционни данни. Това от своя страна не позволява на държавите да приемат закони, задължаващи комуникационните компании да пазят информация за дейността на техните клиенти.

Съвместна регулация

В Канада и Австралия е приет така наречения *модел за съвместна регулация*, който е модификация на гореописания. При този подход, правилата за защита на личните данни се развиват и налагат от бизнеса, а специална агенция или комисия следи за тяхното изпълнение. Макар предимството на този подход да е в евентуалната му по-голяма гъвкавост, той поражда загриженост от възможно занижаване на стандартите и нивото на защита.

През Април 2002, федералното правителствона Канада приема Закон за защита на личната информация и електронните документи.[13] Този закон приема гореспоменатите

[11] Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997), <http://www.ispo.cec.be/legal/en/dataprot/protection.html>.

[12] Directive 2002/58/EU of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf >

[13] Bill C-6, Personal Information Protection and Electronic Documents Act

принципи на КАС и ги включва в закон за компании, които обработват лични данни "във връзка с търговската им дейност" и за държавни компании и техните служители. Този "кодекс" е разработен и приет с всеобщата подкрепа и участие на потребители, представители на бизнес и правителствени организации. За неговото изпълнение следи Комисар по личните данни.

Законът влезе в сила за федерални компании през Януари 2002. До края на следващата година Законът ще влезе в сила и за предприятия, управлявани от отделните провинции, освен ако там не се приемат "по същество еднакви" регулации, като например Закона за защита на личните данни на Квебек. В момента в Онтарио, Британ Колумбия и Алберта текат процедури по приеменете на съответстващи закони.

В Австралия усилията да се приеме закон, които едновременно да осигурява защита на правата на гражданите и да е благосклонен към бизнеса, не са толкова успешни. През Декември 2000 беше приет Законопроекта за допълнение на закона за личните данни. Промените засягат частния сектор и въвеждат Национални принципи на защита на личните данни. Първоначално те са разработени като саморегулация от Комисаря по личните данни през 1997 и 1998. Националните принципи всъщност налагат по-нисък стандарт на защита в сравнение с Директивата на ЕС.

Австралийското правителство описва Закона като "облекчен законодателен режим", въвеждащ минимален стандарт за защита на личните данни, който може да бъде заместен от утвърдени бизнес правила, покриващи минималните стандарти на Националните принципи. Законът предизвика широки дебати и спорове, като някои групи потребители изразиха загрижеността си, че той не покрива международните стандарти в областта. Законопроектът също претърпя много критики поради слабостите в уреждането на режима на изпълнението си, включително за това, че позволява частни жалби да бъдат разглеждани от упълномощени от бизнеса служители при занижен контрол от страна на Комисаря по личните данни. Европейският съюз изрази своята загриженост от големия брой изключения от Закона и в момента работна група на Австралийското правителство подготвя поправки в него.

Проблеми

Съществуването на изчерпателна правна уредба не гарантира само по себе си правото на защита на личните данни. В много държави законите не предлагат почти никаква защита, докато в други проблемите са извън режима на защита на личните данни. Не на последно място, дори и най-строгите закони за безполезни, ако не се изпълняват.

В голям брой страни изчерпателните закони не предлагат добра защита на правото на лични данни. В Русия например, Законът за информация, информираност и защита на информацията, приет през 1995г. изглежда, че няма голям ефект[14]. С някои нови закони положението е същото. През Октомври 1999г. Чили стана първата държава от Латинска

<http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html>.

[14] Федеральный закон об информации, информатизации и защите информации, 25.01.1995. <http://www.computer-museum.ru/document/gosduma1.htm>

Америка, приела закон за защита на личните данни – Законът за защита на частния живот от страните.[15] Според него обаче, само правителствените информационни системи за обработка на лични данни трябва да се регистрират. Няма институция по защитата на лични данни и изпълнението на закона се следи единствено от засегнатите лица. Друг недостатък е, че няма предвидени ограничения върху прехвърлянето на лични данни към други страни.

Дори при юрисдикции, при които има изчерпателни закони и желание за прилагането им, има някои проблеми с придържането към законовите норми. Според проучване на Международната асоциация на потребителите проведено през 2001г., повечето уеб страници в ЕС не следват основни принципи на коректност към личните данни.[16] Ирландският комисар по защита на личните данни предупреди сайтовете за електронна търговия да спазват Закона за защита на личните данни и да се регистрират към Комисията.

В други правни системи, много въпроси по опазването на личните данни остават извън законовите рамки. Много страни изключват контрола по защита на личните данни от дейностите по изпълнението на законовите им задължения, като подслушването е особено важен проблем. През последните няколко години много политически скандали възникват в Дания, Норвегия и Швеция. В тези страни в продължение на десетки години разузнавателни служби незаконно следят граждани със съмнителни цели. В някои държави, като Великобритания, Украина и Русия се приемат поправки, които позволяват практически неограничено наблюдение върху компютърните мрежи. Извън надзор са оставени шпионските мрежи, като известната система Echelon, която подслушва милиони телефонни разговори всеки ден по цял свят.[17]

В много държави видео камерите за наблюдение също създават проблеми. Напоследък, системите за видеонаблюдение (също известни като Closed Circuit Television или CCTV), които се използват на обществени и частни места се разпространяват до безпрецендентни нива. Най-широко тази тенденция е застъпена във Великобритания, където годишно се използват между 150 и 300 милиона паунда за закупуването на около 200 000 камери за наблюдение на обществени места.[18] Много закони за защита на личните данни не покриват такъв вид наблюдение, понеже то не включва създаване на бази данни с идентифицируема информация. Много комисари по защита на личните данни са се намесвали активно в случаи, когато поради развитие на тези технологии, е възможно да се създадат информационни системи с информация, достатъчна за идентифициране на отделни личности.

Секторно законодателство

---

[15] Law for the Protection of Private Life (Ley Sobre Proteccion de la Vida Privada), Law No.19628 of August 30, 1999, published in the Official Journal in August 28, 1999.

[16] Consumers International, Privacy@net: An international comparative study of consumer privacy on the internet January 20001, <http://www.consumersinternational.org/news/pressreleases/fprivreport.pdf>

[17] Published by STOA (Science and Technology Options Assessment). Ref : project no. IV/STOA/RSCH/LP/politicon.1

[18] House of Lords, Science and Technology Committee, Fifth report, "Digital images as evidence", 3 February 1998, London.

Вторият важен начин за защита на правото на лични данни е чрез приемане на закони, които дават защита за тесен кръг информация или за ограничен кръг компании. Почти всички държави, които нямат изчерпателни закони са приели някои секторни закони или конституционни норми, защитаващи личните данни в някои области. САЩ и някои други страни, например, нямат общо законодателство за защита на личните данни, но имат конкретни закони. Дори страни, в които действат изчерпателни закони, приемат и секторни такива. Често те покриват области от особена сложност, като например телекомуникациите (пример за това е Европейската директива спомената по-горе), медицинска или генетична информация, кредитна история, или документи на бившите разузнавателни служби в Източна Европа. В други страни като Южна Корея и Мексико, са приети конкретни закони за електронната търговия, които защитават личните данни.

Закони понякога се приемат и за области извън традиционната юрисдикция на защитата на личните данни. Пример за това са законите за електронно наблюдение и законите за свобода на информацията, които дават право на гражданите за достъп до правителствени документи, но също съдържат общи разпоредби за защита от разкриване без съгласие на личните данни, съхрънявани от правителствени организации. Над 50 страни в света са приели закони за свобода на информацията.

Секторни закони, налагащи строги ограничения върху използването и разкриването на лични данни се приемат и в други области, в които се събира информация. Пример за това са данните от преброяване на населението, които в много държави могат да се използват само за статистически цели и не могат могат да се разкриват в никакви случаи за дълги периоди от време. Ограничения се налагат и върху данни от данъчните декларации.

Недостатъци на секторното законодателсвто

Основен недостатък на секторните закони е, че с развитието на технологиите конкретни разпоредби могат да станат неприложими. С въвеждането на нова технология, при която защитата се отслабва трябва да се направят поправки в съществуващите разпоредби или да се приемат нови. В САЩ такава практика за приемане на закони с въвеждането на нови технологии вече съществува. Това включва защита на личните данни на потребителите на кабелна телевизия, електронна поща и телефони. Въпреки това, тези промени са непоследователни. Например, те не осигуряват защита на Интернет потребителите, освен ако не са под 13 години, или не попадат в някоя друга защитена категория. Потребителите на сателитна телевизия също не са защитени. Компютърни и комуникационни компании яростно се борят против приемането на подобни регулации, твърдейки, че са ненужни, понеже бизнес организациите полагат достатъчни усилия за защита на личните данни.

Проблемът с контрола също е сериозен. Ако в една страна има комисия по защита на личните данни, нейната юрисдикция може да не се простира върху секторните закони, особено тези, които са извън традиционните сфери на защита (като например подслушването). В страни без общ орган по личните данни, юрисдикцията може да

бъде разпределена върху много правителствени агенции и да бъде осъществана некоординирано. В някои области, като разузнаването или изпълнението на закони, контрола се осъществява от самата правителствена агенция, което води до намаляването или изчезването му.

Пример за това са САЩ, където няма независима надзорна агенция занимаваща се със защита на правото на личен живот. По Закона за Защита на Правото на Личен Живот (Privacy Act), Бюрото за Управление и Бюджет (Office of Management and Budget) има ограничена власт да определя донякъде политиката на федералните агенции по въпроса със защита на правото на личен живот, но то не е особено активно или ефективно. В началото на 1999 към Бюрото за Управление и Бюджет беше създаден специален отдел, който да се занимава с координацията на политиките на федералните агенции по въпроса на защита на защита на правото на личен живот. Беше определен и Главен Съветник по въпросите на неприкосновеността на личния живот. Съветникът имаше единствено консултативна роля, при това ограничена, поради което преобладаващото мнение е, че подобен орган е неефективен. Когато новата администрация дойде на власт, Съветникът не беше сменен.

В други области различни департаменти имат контролна функция. Федералната Комисия по Търговия има надзорни и правоналагащи функции по законите защитаващи личната неприкосновеност на децата в Интернет, информацията за потребителските кредити и уреждаща правилата за честна търговия, но Комисията няма общо право да налага принудителни решения, ако няма опит за измама или подвеждане на клиента[19]. Департамента за Защита на Здравето и Хуманитарните Услуги се занимава с медицинските записи и наскоро приетите правила за защита на медицинските записи. Департамента по Правосъдие регулира както себе си така и други правителствени агенции по въпроси свързани с наблюдение над граждани и организации. Департамента по Образование регулира защитата на записите на образователните институции, но често е подкрепял и мерки за по-широко събиране и разпространяване на информация за учащи.

Понякога приемането на секторни закони може да доведе до орязване на защитата предоставяна от общите закони. В Исландия например, през 1998 парламента одобри проектозакон за създаване на национална централизирана база-данни със здравна информация, която да се използва за генетични изследвания[20]. Правителството даде лиценз за базата-данни на американска компания (deCODE Genetics) занимаваща се с биотехнологични разработки за срок от 12 години. Тази компания ще включи в базата-данни генетична информация за цялото население на Исландия на основата на предоставените й национални медицински данни за последните 30 години. Последваха основателни протести от страна на лекари и обикновени граждани. В отговор на тези протести правителството прие Акта за Биобанките на 13 май 2000[21]. Актът определя правилата за "събиране, съхраняване, обработване и използване на човешки биологични образци" с цел осигуряване на конфиденциалност и предотвратяване на

[19] Виж страницата на FTC http://www.ftc.gov/privacy/index.html

[20] Закон за База-данни на Здравния Сектор (Act on a Health Sector Database no. 139/1998, 17 December 1998)

[21] Act on Biobanks no. 110/2000, May 13, 2000

дискриминация. В същото време обаче, "ако образци са събрани с цел да се използват в клинични тестове или лечение, то съгласието на пациента за включване на образците му в биобанка се предполага за дадено" при положение, че лекарят му е дал обща информация. Подобно на това, новата Директива на ЕС по Въпросите на Защита на Правото на Личен Живот в Интернет ограничава Директивата за Защита на Личните Данни от 1995 като позволява задържане на данните.

Саморегулация

Друг метод за защита на правото на личен живот е посредством саморегулация от страна на самите компании и фирми, при което те сами си определят ограничения. Този подход има някои положителни страни, но като цяло по-често защитата става жертва на желанието за максимизиране на печалбата.

Самоналагането на ограничения има сериозна роля в защита на правото на личен живот. Компаниите са най-добре осведомени каква точно лична информация събират и как я използват. За да може защитата на личните данни да е ефективна в една система, компаниите трябва да са склонни да сътрудничат, защото има финансови и политически ограничения пред правителствата и другите надзорни органи да налагат принудително сътрудничество.

Саморегулацията има различно значение в САЩ и в Европа. В САЩ където няма общ закон за защита на неприкосновеността на личния живот, индустриалния сектор не е задължен да спазва някакви минимални стандарти и има малко доказателства, че целите на кодексите за саморегулация са постигани. Съществува също така и сериозен проблем с прилагането на такива правила. В случая с ЕС, саморегулирането обикновено значи, че индустрията създава правила, основани на националните стандарти при защита на данни, а прилагането се осигурява от националните агенции за защита на данни.

Типично прилагане на саморегулация е създаването на политики за защита на правото на личен живот от страна на компании, които после "обещават", че ще ги спазват. Те варират широко от политики базирани на Насоките на Организацията за Икономическо Сътрудничество и Развитие, до такива гарантиращи слаба или почти никаква защита.

Друг вариант на самоограничение е свързан със създаване на индустриални кодекси. Това са споразумения между голям брой компании в даден индустриален бранш, с които те се съгласяват да следват определени правила изготвени от индустриални асоциации или от орган(и) на правителството. В зависимост от правната система, правилата могат да бъдат доброволни или задължителни. Търговските асоциации понякога поддържат и общи база-данни. Американската Асоциация за Директна Търговия например има правила за нежелана поща (спам) и от 20 години поддържа списък с потребители, които не желаят да получават рекламна поща.

Надзор и Налагане на Правила

Надзорът при саморегулирането обикновено е в ръцете на самите компании или на търговски групи в които те участват. В някои случаи има трети страни, които приемат оплаквания и осигуряват ограничен надзор и проверки.

В някои случаи индустриални органи могат да налагат прилагане на правилата. В САЩ има единични случаи на такова налагане. Американската Асоциация за Директна Търговия едва наскоро въведе изискване членовете й да следват правилата за защита на личния живот и да дават на потребителите възможност да избират дали да бъдат включвани в списъците за реклама по пощата. Същата асоциация до момент не е изключила нито един свой член при неспазване на правилата за защита на личния живот на потребителите.

Широко разпространена практика сред компаниите опериращи в Интернет е да позволяват на клиентите да се ползват регистрирани програми с цел потребителите да имат чувството, че техните лични данни са защитени. Тези програми са наследници на традиционните затворени програми, които задават известни приемливи стандарти (правила), които компаниите трябва да следват, за да получат съгласието на клиента.

Регистрираните програми като цяло не дават сериозна защита. На първо място те поставят много ниски изисквания за получаване на сертификат. Основните програми не изискват от компаниите да следват изцяло правилата за честна информация. За някои сертификати се изисква само да се заяви дадена политика, без значение колко агресивна е тя. Обхватът на някои програми е ограничен. Сертификатите като цяло са ограничени само до трафика от и до сайтовете в Интернет. Когато беше открито, че Майкрософт и RealNetworks тайно следят активността на потребителите чрез специален софтуер, TRUSTe отказа да постанови, че това е извън правата на двете компании. Други като BBBOnline са давали сертификати на компании с дългогодишна история на незачитане на личния живот и данни. Оправданието за издаването на тези сертификати е, че те покриват само Интернет страниците, така че не е необходимо да се взема в предвид практиките на дадена фирма в други области.

Друг проблем е налагането на правилата. Често пъти регистратори на програми като TRUSTe не са склонни да прилагат наказателни мерки срещу техни членове, сред които е и Майкрософт. В доклада на Форестър от 1999 е отбелязано, че "благодарение на факта, че независимите групи за защита на личния живот като TRUSTe и BBBOnline печелят парите си от компании рекламиращи и продаващи в Интернет, те се превръщат по-скоро в защитници на бизнес конфиденциалността в Интернет, отколкото в защитници на правата на личен живот на потребителите[22].

Съществуват някои независими проверяващи компании, най-вече счетоводни фирми, които в определени случаи са били наемани за независима проверка на дейността на определена компания. Въпреки това, в много случаи проверките са били повърхностни

[22] Forrester Research Inc, "Privacy Wake-Up Call," September 1, 1999.

или техните резултати никога не са били публично огласявани. След като в Hotmail на Майкрософт бяха открити сериозни пробиви в сигурността, от Майкрософт се съгласиха системата им да бъда проверена. След края на проверката те отказаха да огласят резултатите й и дори името на автора, подозрително оправдаващи се с правни ограничения. Други, подобно на IRSG, търговска асоциация на агенции за потребителски кредити, поставиха ниски критерии за проверка, а после се поздравиха, че са я минали.

Друг проблем със саморегулацията е, че при отсъствието на законова рамка, компаниите, които предоставят сериозна защита на личната неприкосновеност на клиентите си, често пъти се поставят в неизгодна позиция спрямо конкурентите си, които не се съобразяват с никакви правила за защита на личната информация. В повечето индустрии, отделните компании не са задължени да следват правилата изработени от самата индустрия. По-агресивните компании се възползват от добрата воля и вярата на потребителят създадени от индустриалните правила, но после разрушават тази вяра като не следват тези правила, което често пъти води до загуба на доверие от страна на потребителите дори и в компании, които са добросъвестни при опазване неприкосновеността на личните данни.

Тези проблеми си проличаха в наскорошния дебат в САЩ по въпроса за защитата на правото на личен живот. Основен проблем е, че в нерегулирана бизнес среда (каквато съществува в САЩ) няма минимален задължителен стандарт за защита на това право. Много от политиките в тази област просто заявяват, че те (дадена частна компания например) събират голямо количество подробна информация на клиенти, която смятат да използват за незнайни цели по тяхна преценка и да предоставят същата информация на незнаен брой външни организации, за да я използват по незнаен начин. Досега няколко изследвания на американската Федерална Комисия по Търговия и на независими групи като EPIC показаха, че повечето политики за защита на личните данни не са ефективни.

Дори и при положение, че дадена компания има добра политика, поради липсата на правна рамка, във всеки момент съществува реалната опасност тази политика да бъде променена от самата компания. Много Интернет компании промениха политиката си в следствие на срива на Интернет индустрията, с цел да използват наличната им информация за повече печалби.

Проблеми се появяват и при промяна в правния статут на дадена компания. Ако дадена компания фалира или е закупена от друга компания, то е съмнително, че придържането към политика за защита на личната информация на клиентите й ще продължи. Интернет компанията Toysmart.com се опита да продаде базата-данни с информация за клиентите си, въпреки че във фирмената политика изрично бе обещано, че компанията никога няма да предостави тази база-данни на трета страна. Информацията също така може да бъде разкрита публично, защото често тя е единствения актив на компанията. Когато Living.com подаде иск за банкрут, попечителите публикуваха в Интернет имената и адресите на хиляди нейни клиенти.

Накрая, (принудителното) налагането на политики за защита на правото на личен живот в страни без специални закони по въпроса като САЩ е възможно само при обвинения, че компанията действа с измама или подвеждане на клиентите си. В най-добрия случай (който не се наблюдава често) потърпевшите могат да се обърнат към Федералната Комисия по Търговия или щатския Главен Прокурор да наложат изпълнение на "обещанието" за конфиденциалност. Както вече бе отбелязано, Федералната Комисия по Търговия е получила досега хиляди оплаквания, но е изразила становище само по няколко от тях. По принцип Комисията не е задължена да провежда разследвания по оплакване на потребители.

Саморегулацията също така пропуска проблеми свързани с правителството. Без обща система и надзорен орган, много от дейностите на правителството остават без наблюдение и тяхната промяна налага скъпоструващи съдебни битки.

Технологии за Защита на Личните Данни

С развитието на Интернет, защитата на личните данни частично премина в ръцете на самите индивидуални потребители. Технологиите позволяващи това са познати като "Технологии за повишаване защитата на личната информация" (Privacy Enhancing Technologies – PET). Потребителите на Интернет могат да използват набор от програми и системи даващи различни степени на защита на комуникацията и личните данни. Сред тях са кодиране, прокси сървъри, препращане на съобщенията, електронни пари и смарт карти. Въпреки това остават някои въпроси касаещи сигурността и надеждността на тези системи.

Такива системи могат да се използват в ограничаване на предаването на лични данни, като дават достъп на потребителя до неговите данни и осигуряват конфиденциалност. През 1998 Европейската Комисия разгледа някои от тези средства и заключи, че те не могат да заменят една правна рамка, но биха могли да подпомогнат прилагането на съществуващите закони[23].

Повечето от тези средства възникнаха благодарение на опасенията, възникнали в много потребители за сигурността на личните им данни с развитието на Интернет и на електронната търговия. Опитите да се създават закони позволяващи по-прецизно следене в мрежата на Интернет също така допринесоха за повишаване на интереса в средства предотвратяващи следенето на дейността. Като цяло тези средства са създавани от потребители от САЩ и Европа загрижени за правото си на защита на личния живот.

Кодирането е едно от най-ефективните средства за защита от следене на комуникациите. Дадено съобщение или предаване се разбърква по начин, който (на теория) само желания получател е в състояние да сглоби правилно отново и да го прочете. Повечето Интернет браузъри имат вградено кодифициране за защита на

[23] Мнение 1/98: Platform for Privacy Preferences (P3P) и Open Profiling Standard (OPS)
http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp11en.htm

номерата на кредитните карти и лична информация прехвърляна по мрежата от потребителя до сървъра. Друг софтуер предпазва електронната поща между индивидуалните потребители и малки групи. PGP (Pretty Good Privacy) е най-известната кодираща програма със стотици хиляди потребители, които я използват, включително групи за защита на човешките права[24]. GNU Privacy Guard е кодираща програма с отворен код, създадена като безплатен заместител на PGP. GNU позволява на потребителите да имат достъп до пълния код на системата за да са сигурни, че няма тайно подслушване и следене на комуникацията[25].

Препращането на съобщенията премахва идентификационната информация от електронната поща и може да спира анализа на трафика. Създадени са и по-усъвършенствани средства, които съчетават функциите кодиране и препращане на съобщенията.

Друго полезно средство позволява на потребителя да влиза в уеб сайтове, така че идентичността му да не бъде разкрита. Много от тези услуги също предпазват от т.нар. "cookies", представляващи програми, които веднъж поставени на компютъра на потребителя, могат да се използват за следенето му.

Смарт картите, базирани понякога на биометрични показатели за идентификация, са полезни както за покупки в Интернет така и извън него. Те са ефективни за запазване на неприкосновеността на личния живот, защото в тях се използват добри системи за запазване на анонимност. Въпреки това понякога техните ползи се преувеличават, а те самите са изготвяни по начин улесняващ следенето на данните.

Границите на Технологията и Системи Не-гарантиращи Защита на Правото на Личен Живот

Не всички средства попадащи под названието PETS са ефективни за защита правото на личен живот. Сериозен недостатък е, че почти всички средства не следят за защита на информацията след като веднъж е дадена. Кодирането се използва за защита на информацията докато е в процес на предаване, но не помага ако компаниите на които тази информация е дадена решат да злоупотребят с нея.

В последните няколко години известен брой от най-обещаващите технологии включително дигиталните разплащания и някои Интернет браузъри, даващи висока степен на анонимност, не успяха да се наложат на пазара поради факта, че на потребителите им беше трудно да свикнат с тях.

Има и много системи предлагани от индустрията, които не защитават специално правото на личен живот на потребителите. Много от тези системи като P3P на Световния Мрежов Консорциум (W3C) са по-скоро създадени с цел да улесняват

[24] PGP International Page: http://www.pgpi.com

[25] Homepage: http://www.gnupg.org

размяната на данни, отколкото да опазват тайните на потребителите[26]. Често пъти широкото разпространение на такива системи се използва като оправдание от страна на американската индустрия за противопоставяне на приемането на актове за защита на личния живот и личната информация в Интернет.

Други компании предлагат да станат "брокери на информация". При използването на много от тези системи, като например Microsoft's Passport потребителите дават информация на компанията (често пъти неволно, както е положението при създаване на Hotmail account), която след това е предоставяна на уеб сайт на трета страна. Такива сайтове изваждат на преден план въпроса, доколко може да се доверяваме на компаниите в опериращи в Интернет. Много от тези сайтове са подържани от същите Интернет компании, които са сред основните нарушители на правото на личен живот на потребителите и които се занимават и с рекламиране в Интернет. При това положение за потребителите е хубаво да се замислят дали да трябва доброволно да предоставят информация на такива компании. Майкрософт се съгласи да направи промени в системата си през 2002 и 2003, след като компанията беше разследвана и от Американската Комисия за Свободна Търговия и от Европейската комисия.

Компаниите често преставят програмите си като защитаващи личния живот на потребителите. Много пъти това изобщо не е така. Американ Експрес обяви през октомври 2000 своята програма Private Payments, която щяла да позволява създаване на уникални еднократни номера на кредитната карта за покупки по Интернет. Номерът на картата щял да предотврати злоупотребата при евентуална нейна кражба или загуба. Въпреки това при трансфера на лична информация между продавача и потребителя AmEx също получава информация за покупката.

Съществуват и опасения за защитата на личните данни. Ако дадена компания реши да промени политиката си и да започне да разкрива лична информация, потребителите може да се окажат в състояние да направят много малко ако, както е в САЩ, липсва правна защита, регулираща използването на лични данни. Подобен случай се получава и когато дадена компания фалира или се слее с друга. В тези случаи често пъти се наблюдава промяна на фирмената политика по отношение на защита на личните данни и личния живот, като е неясно какво точно могат да направят потребителите срещу това.

Накрая, много средства не са сигурни. Някои са лошо направени, докато други са направени с цел по-лесен достъп за аторизираните органи[27].

Надзор

[26] EPIC and Junkbusters, 'Pretty Poor Privacy: An Assessment of P3P and Internet Privacy', June 2000, http://www.epic.org/reports/prettypoorprivacy.html

[27] EPIC maintains a list of tools at http://www.epic.org/privacy

Ключов аспект от добрия режим за защита на личния живот (както и на всеки друг режим) е надзора. В повечето държави в който е приет общ закон за защита на личните данни или на правото на личен живот, съществува и независим орган, който надзирава прилагането на този закон. Властта и отговорностите на този орган – Комисар, Омбудсман или Регистратор – варира широко в различните държави. Някои държави като Германия и Канада имат подобни надзорни органи и на провинциално ниво. В момента има над 50 правни режима (включително на под-национално ниво) предвиждащи надзорен орган.

Според член 28 на Директивата на ЕС за Защита на Данните, всички страни от ЕС трябва да имат независим орган, следящ за прилагането на съответните национални закони за защита на данните. Според Директивата, тези органи трябва да имат достатъчно сериозни правомощия: националните правителства трябва да се консултират с тези органи, когато изготвят правни норми свързани с обработването на лична информация; органите имат правомощия да провеждат разследвания и да получават достъп до информация свързана с тези разследвания; органите имат право да налагат поправителни мерки като например да наложат унищожаване на информацията или забрана за нейното обработване, както и да инициират съдебни процедури, приемат жалби и издават доклади. Тези органи са отговорни по принцип за образоване на широката общественост по закона/законите и международното взаимодействие в прехвърлянето и защитата на личните данни. Много от органите поддържат регистър на организациите събиращи информация и техните бази-данни. Често пъти органът издава лицензите за дейността на такива организации. Някои страни като Тайланд, които нямат общ закон за защита на правото на личен живот, въпреки това имат надзорен орган. В допълнение, няколко страни като Канада, Австралия и Нова Зеландия бяха определили комисари по личните данни преди да приемат общ закон.

Друга основно задължение на тези органи е да насочват общественото внимание към проблемните въпроси, дори и в случаите когато самите органи не са овластени да решават тези проблеми. Те постигат това чрез изготвяне на кодекси за действие и окуражаване на приемането на тези кодекси от индустриалните съюзи и браншови организации. За представяне на проблемите пред обществото се използват и годишните доклади на органите. В Канада например, Федералния Комисар по Личните Данни обяви в своя доклад за 2000-та година за съществуването на голяма база-данни поддържана от федералното правителство. След обявяването на тази информация правителството разтури тази база-данни.

В някои държави като Унгария, Естония, Тайланд, Великобритания и в някои провинциални комисии в Канада и Германия, органът има юрисдикция върху законодателството, касаещо достъпа до правителствени архиви (свобода на информацията).

Основен проблем пред много от агенциите е липсата на достатъчно ресурси за адекватен надзор и налагане на мерки. Много от тях са затруднени от извършването на лицензионна дейност, която поглъща голяма част от ресурсите им. Повечето са затрупани от жалби и оплаквания или не са в състояние да провеждат сериозен брой

разследвания. Много от тези агенции първоначално започват дейността си с адекватен бюджет, но след няколко години той е сериозно редуциран. Бюджетът на Австралийската Комисия по Личните Данни за 1997 беше драстично орязан, въпреки че Комисията беше натоварена с нови задължения.
Накрая в някои държави в които няма отделен орган, разследванията и налагането на мерки се осъществява от Омбудсман или от орган към парламента.

Ролята на Гражданското Общество

Важна предпоставка за ефективна система, освен добри правителствени органи, е и наличието на дейно гражданско общество, което се бори за защита на правото на личен живот. Както вече отбелязахме, независимите обществени групи имат достъп до медиите и могат да разкриват пред обществото случаи на нарушения, когато правителството или дори надзорния орган не желаят да разкриват тези случаи публично.

Най-силния орган за надзор в САЩ е самото общество. Групи с нестопанска цел като Electronic Privacy Information Center, Junkbusters и ACLU редовно представят на общественото внимание проблемите по защитата на правото на личен живот и водят кампании срещу компании-нарушители на това право. Въпреки това те са възпрепятствани от ресурсни ограничения, така че те са в състояние да водят малък брой кампании по едно и също време.

Неправителствените организации в над дузина държави организират годишни т.нар. “Награди Големия Брат” (Big Brother Awards) за “награждаване” на най-големите нарушители на правото на личен живот[28]. Тези анти-награди насочват общественото внимание към нарушенията и често пъти са предизвиквали промяна в политиката на организациите.

Заключение

Нито една система за защита на правото на личен живот не е адекватна, поради бързото развитие на технологиите и големия спектър от въпроси свързани с това правото. Повечето развити държави са приели или са в процес на приемане на общи закони, определящи правната рамка, като в същото време са в процес на приемане и на секторни закони, притискайки индустрията да зачита правото на личен живот, включително и чрез налагане на технологии защитаващи това право. Във всички системи обаче е необходим и адекватен механизъм за надзор. Гражданското общество също играе важна роля в излагането на нарушенията и предизвикване на реакция от страна на властта.

[28] Виж http://www.privacyinternational.org/bigbrother