"МИРАЖЪТ" НА ПРАВОТО – "ОАЗИС" ЗА НАБЛЮДЕНИЕ

Личната неприкосновеност, защитата на личните данни и наблюдението през погледа на европейското и американското законодателство

Василка Чифильонова

1. Въведение

Личната неприкосновеност се основава на идеята за лична свобода. Личната неприкосновеност е необходим компонент от демокрацията, при която индивидът и обществото са си взаимно значими. Защитата на личната неприкосновеност и на личните данни е важна, защото стига дълбоко до нашето "аз", до човешката същност и автономност, както и до способността ни да се изразим, да комуникираме с други хора и да бъдем част от колектива, от общността.

Обществото е успокоявано с погрешно чувство за сигурност по отношение на защитата на личната неприкосновеност – наблюдението става част от неговия живот: следени сме където и да отидем, каквото и да правим, и е разбираемо, че хората изискват определени мерки от правителството – актове за защита на личната неприкосновеност.

Макар и появата на законодателство в областта на личната неприкосновеност и защитата на данните да е факт, има доказателства, че всичко това е само една илюзия и тази илюзия е "оазис" за наблюдение. И единственото обяснение на управляващите е, че по този начин те се грижат и следят за благополучието на обществото, с което, разбира се, обществото се съгласява.

Поддръжниците на личната неприкосновеност твърдят, че тя е особено важна за запазването на градивно обществено взаимодействие и ще бъде критично за запазване и поддържане на разумно демократично общество в модерния свят.

Според редица анализатори[1] много често американското законодателство за защита на личната неприкосновеност търпи критика.

---

[1] **Berman, J. & Goldman, J.** (1989), "*A Federal Right of Information Privacy: The need for reform*", Washington D.C.: The Beneton Foundation; **Flaherty, D.** (1997), "*Privacy on the Internet*", www.oipcbc.org/publications/presentations/internet_privacy.html; **Onsrud, H. et all** (1994) "*Protecting Personal Privacy in Using geographical Information Systems*", Photogrammetric Engineering and Remote Sensing, Vol. 60, No. 9 , September 1994,1083-1095; **Trubow, G.** (1989), "*Watching the watchers: the coordination of federal privacy policy*", Washington , D.C.: The Beneton Foundation.

Учените Джей и Хамилтон[2] подчертават ограниченията на Закона за защита на данните във Великобритания от 1998, тъй като в него има много изключения като национална сигурност, престъпления, облагане с данъци, здравословно състояние, социална работа, сигурност, при определени обстоятелства и журналистика, изкуство, научна дейност и история. Много често компаниите не са заинтересовани да съхраняват точна информация, обаче по съвсем по друг начин стои въпросът за нейното използване. Личната неприкосновеност е неразделна част от демокрацията, индивидът и колективът са си взаимно необходими.

Повечето от националните законодателства не определят адекватно нито интереса на хората към областта на личната неприкосновеност, която трябва да бъде защитавана, нито принципите в областта на защита на данните, които трябва да бъдат заложени, за да бъде ограничено наблюдението[3].

Неконтролираното събиране и използване на лична информация от правителствени и стопански организации съществено увеличава вероятността за "конформистко, роботизирано общество, което се опитва да избегне излагането на риск, за да функционира обществото"[4] . Твърди се, че търговският сектор в Америка вече е "станал твърде натрапчив, тъй като се събира и се обменя информация за хора без да се вземат предвид вредите, които се причиняват по този начин"[5]. Лицата, които не желаят всяка тяхна покупка, всяко движение, хоби или политическо убеждение да се знаят, вече са принудени да намерят начин, за да "скрият" своя живот и убеждения.

Настоящият анализ няма за цел да опише съществуващите актове в тази област, а да обрисува илюзията, която ни се предоставя от различните законодателни мерки в областта на защитата на личните данни с основен аргумент – законодателството е само един мираж, в който вярваме, и в същото време оправдание за правителствените и стопанските институции да ни наблюдават. Поглеждайки върху наблюдението и защитата на личните данни от различен ъгъл, тази статия разисква въпроса защо и как законите не оправдават надеждите ни и кой стои зад всичко това.

2. "Миражът" на правото

---

[2] **Jay, R. & Hamilton, A**. (1999), "Data protection law and practice", Sweet& Maxwell, London.

[3] **Flaherty, D.** (1989), "*Protecting privacy in surveillance societies*", Chapel Hill, University of North Carolina Press.

[4] **Trubow, G.** (1989), "*Watching the watchers: the coordination of federal privacy policy*", Washington , D.C.: The Beneton Foundation.

[5] **Graham, J**. (1987), "Privacy, computers, and the commercial dissemination of personal information" Texas Law Review June: 1395-1439.

За един от първите актове, касаещи проблема за личната неприкосновеност, се приема Законът за мировия съдия[6] от 1361 г., с който на английските поданици се предоставя закрила от наблюдение, следене и подслушване. В по-ново време основите на съвременната правна уредба се поставят с Всеобщата декларация за правата на човека, провъзгласена от Общото събрание на ООН на 10 декември 1948 г. Член 12 на Декларацията гласи: "Никой не трябва да бъде подлаган на произволна намеса в личния му живот, семейството, жилището и кореспонденцията, нито на посегателства върху неговата чест и добро име. Всеки има право на закрила от закона срещу подобна намеса или посегателства." Значителна част от литературата относно личната неприкосновеност е свързана с контрола върху неприкосновеността. Известната фраза "правото да бъдеш оставен сам" датира от 1880 г. и остава в историята като едно от най-ранните определения за лична неприкосновеност, а една от най-пламенните статии в защита на личната неприкосновеност остава тази на Уорън и Брандеис[7], които отказват да вярват, че личната неприкосновеност трябва да умре, за да могат високите технологии да се развиват.

Личната неприкосновеност винаги е била трудно дефинирана, което е довело до възникването на няколко сродни определения: информационна лична неприкосновеност и комуникационна лична неприкосновеност. Де Кю[8] извежда три вида лична неприкосновеност: "информационна" (контрол върху информация), "достъпна" (получаване на достъп) и "изразителна" (право да се изразиш). Тенденцията за приемане на законодателство относно личната неприкосновеност и защитата на данните продължава и до наши дни. Редица от Централноевропейските държави, както и Нова Зеландия, Австралия и Хонг Конг приемат т. нар. "всеобхватни" закони за защита на данните. Три десетилетия от развитието на усилията на Европейския съюз в тази област са отразени в Директива 95/46/ЕС за защита на индивидите по отношение на обработката на лични данни и движението на такъв вид данни. Една от особеностите на тази Директива е възможността да се прекрати прехвърлянето на данни от която и да е държава на Европейския Съюз, ако законодателството на държавата, към която данните се прехвърлят, няма адекватен закон за защита на личните данни. Американските компании, които развиват търговски отношения с Европа, трябваше да се съобразяват със законодателството на

---

[6] Законът за мировия съдия (Justice of the Peace Act) е приет от Парламента на Едуард III през 1361 г. Част от неговото предназначение е разгледано от **Henderson, S & Snyder, C.** (1999), "*Personal information privacy: implications for MIS managers*", Information and Management 36, 213-220.

[7] **Warren, B. & Brandeis, L.** (1890), "The Right to Privacy", Harvard Law Review article.

[8] **DeCwe, J. W.** (1997), "*In pursuit of privacy: law, ethics, and the rise of technology*", Cornell University Press, United States.

съответната държава, тъй като в противен случай щяха да загубят важни бизнес-партньори. Иронията е, че самите тези компании могат и да не предоставят същата тази защита на своите сънародници или на индивиди от трети страни, където няма такова изискване[9].

Най-общо, концепцията за информационна лична неприкосновеност възниква през 60-те и 70-те години на XX век, по същото време, когато защитата на данните (data protection – произлиза от немската дума "Datenschutz") влиза в речника на европейските експерти и се свързва с възможностите на компютрите да обработват информация. Създадените групи от експерти в различни държави като САЩ, Великобритания, Канада и Швеция полагат основите на първите законодателни актове за защита на данните и информационната лична неприкосновеност.

Част от тази проблематика е склонността на човека да наруши личната неприкосновеност на другите, а обществото да се заеме с наблюдение, за да следи различни видове антисоциално поведение. Правото на индивидите и юридическите лица да решат кога и как да навлязат в публичното пространство им е отнето. Някои дори твърдят, че правото да се събира и да се "търгува" информация само връща обществото в социалния сценарий на малкия град, където всеки знае какво прави другия.

Същността на наблюдението може да бъде разгледана от различни страни. Изключително интересно е твърдението, че наблюдението е необходимо за създаване на репутацията на даден човек. В едно общество "личната неприкосновеност затруднява изграждането на надеждно мнение един за друг"[10]. Затова може да се заключи, че общество от непознати се характеризира с лична неприкосновеност и наблюдението е цената, която трябва да се плати за тази лична неприкосновеност. При липса на репутация човек е считан за чужд. Този аргумент може би е в полза на дейността по наблюдението, но не определя кой е отговорен за това и дали има право да се прави.

От друга страна се твърди, че общество, в което всеки по някакъв начин трябва да разкрие всичко за себе си, би било психологически нетърпимо за неговите членове[11]. В резултат на това хората няма да имат възможност да установят или да поддържат чувство за идентичност и граници – откъде започват и къде завършват техните собствени и тези на другите индивиди. Технологията ни "превзема" и възможностите за

---

[9] **Hurley, D.** (2001), "*A whole world in a glance: privacy as a key enabler of individual participation in democratic governance*", Harvard Infrastructure Project, Harvard, http://www.pco.org.hk/english/infocentre/conference.html

[10] **Nock, S.** (1993), "The cost of privacy – Surveillance and Reputation in America", Aldine De Gruyter, New York.

[11] **Steele, F.** (1975), "The open organization – The impact of secrecy and disclosure on people and organisations", Addison-Wesley Publishing Company.

нежелано разкриване, например чрез електронното наблюдение, са много по-големи, отколкото са били само преди няколко години.

И още една, трета гледна точка – да бъдеш под наблюдение означава да получиш максимално клиентско обслужване. Това може да се стори доста противоречиво твърдение, но показва и другата страна на основната теза. Например когато използваме "бисквитки" – малък файл с информация, който се записва на компютъра и записва настройките ни, има възможност да ни бъде предоставена доброволно информация, която търсим, а това е вид удобство. Освен това самият живот налага други начини на електронно удобство, като например мобилните телефони, използването на Интернет за пазаруване, които в същото време улесняват онези, които искат да научат повече за нашия живот.

Обяснимо е, че когато изискваме повече удобства, трябва да се откажем от част от своята лична неприкосновеност. Например, когато използваме кредитна карта, това е един вид стимул за пазаруване. Тя се приема като индикатор за доверие и е удобство, но за да имаме кредитна карта, първо трябва да има установено доверие между индивида и банката, което се създава чрез събиране, съхраняване и обработване на различна информация. Макар че този аргумент е в полза на наблюдението, въпросът е каква степен на наблюдение се осъществява и дали законодателството е в състояние да наложи известни ограничения.

Инспекторите на лични данни твърдят, че наблюдението е необходимо, за да се поддържа общественият ред и да се създаде икономическа продуктивност, а личните права трябва да останат подчинени на ограничения от фискален и обществен характер[12].

Но личната неприкосновеност не се отнася само за неразкриване на факти и обстоятелства. Тя е свързана с автономия, почтеност и самоопределение. Знаем, че личната ни неприкосновеност е застрашена, но проблемът е, че не знаем как да отвърнем на този удар. Някога експертите са смятали, че единственото разрешение на този проблем е прокарването на закон за личната неприкосновеност и защита на данните, който се базира на редица сходни информационни принципи. Много от сегашните актове са били приети под натиска на международната регламентация на търговията, особено тези данни, които се движат от / към Европейския Съюз[13].

---

[12] **Davies, S.** (2001), *"Unprincipled privacy: why the foundations of data protection are failing us"*, University of New South Wales Law Journal, http://www/austlii.edu.au/au/journals/ UNSWLJ/2001/7.html; **Davies, S.** (1999), "*Big Brother at the box office*", 21st International Conference on Privacy and Personal Data Protection, http://www.pco.org.hk/english/infocentre/ conference.html; **Davies, S.** (2002), "*Database, marketing, tracking and surveillance on the Internet*", LSE Privacy and Data Protection Lecture Notes.

[13] **Bennett, C.** (1992), "Regulating Privacy-data protection and public policy in Europe and the United States", Cornell University Press, USA

Затова може да се твърди, че има определени граници в процеса на предоставяне на лична информация и само когато тези граници са престъпени, може да се говори за нарушаване на личната неприкосновеност. Но тогава трябва да си зададем следния въпрос: ако съществува законодателство, което да защитава информацията извън тези граници, защо тези граници не са достатъчно стабилни? Само ако информацията, която се съдържа в една система, е предоставена или придобита без съгласието на лицето, бихме могли да говорим за нарушаване на личната неприкосновеност[14]. На пръв поглед това изглежда обяснимо, но в повечето случаи ние дори не знаем в колко бази-данни има информация за нас, кога и по какъв начин е била събрана.

Докато европейските страни продължават да развиват и да усъвършенстват всеобхватни закони за защита на данните, които покриват събирането на данни от правителствата и представителите на частния сектор, американското законодателство ги следва само с допълнения в различните видове закони, които се отнасят за специфични случаи, и то при самото им възникване (напр. Закона за вярното и точно предоставяне на информация за кредитите от 1970 г., Закона за защита на личната неприкосновеност от видеозаснемане от 1988 г., Закона за семейното възпитание и личната неприкосновеност от 1994 г.). Макар че предимствата на Закона за вярното и точно предоставяне на информация за кредитите от 1970 г.[15] върху личната неприкосновеност са очевидни, едва ли може да се приеме, че прокарването на нови закони, които да допълват категории на лична информация, е най-ефективният и ефикасен подход да се защити информационната лична неприкосновеност.

В Съединените щати съдебни мерки и въпроси, свързани с кредитните отдели, могат да бъдат предприети именно въз основа на този закон, който задължава отделите да предоставят точна и пълна информация за кредитите на индивидите. Законодателството обаче е било критикувано заради факта, че всеки със "законни стопански нужди" може да получи достъп до съответното кредитно досие, а терминът "законни" или действията, които представляват "бизнес-транзакция", не са ясно дефинирани в закона. Накратко, повечето закони са пълни с изключения, които позволяват "рутинна употреба" и разкриване на защитена информация за "законни бизнес-нужди". Ситуацията може да бъде обощена по следния начин: "Както дори част от законите в областта на личната неприкосновеност показва, обръща се смесено внимание на

---

[14] Вж. 10.

[15] Законът за вярното и точно предоставяне на информация за кредитите (The Fair Credit Reporting Act) е приет в САЩ през 1970 г.

личните притеснения. Федералната програма, установена със закон, прилича най-вече на пъзел, в който частите не си пасват"[16].

Освен това, с влизането в сила на Директива 95/46/ЕС вече не е достатъчно да се обяви и декларира събирането на данни – тя също така задължава всички служители / организации, които събират данни, да получат изричното съгласие на индивида, а хората биха могли да откажат да дадат съгласие. В действителност съгласието се е превърнало в механизъм, който позволява пренасянето на обем от данни, отколкото да представлява средство за защита на индивидуалните права[17]. Най-често срещаното съгласие си остава писмената форма. В света на електронните транзакции обаче не е толкова лесно да се стигне до такова. Няма всеобхватна рамка за защита на интересите, свързани с личната неприкосновеност, от новопоявяващите се технологични изобретения. Хората са объркани в сложните и нарастващи неефикасни системи за защита на техните лични интереси, включващи международното и националното право, различни професионални и индустриални кодекси, указания и етични норми. Съществуващите източници за защита на личната неприкосновеност са твърде сложни и различни и едва ли могат ефективно да се справят с възникващите технологии.

По данни на Саймън Дейвис – директор на неправителствената организация Privacy International, към 2002 г. средностатистически индивид от развитите западноевропейски страни се появява в около 400 бази-данни[18]. Това може да бъде достатъчно за съставянето на кратък справочник за всеки човек. Освен това, тъй като само една малка част от данните са събрани директно от индивида, малко е вероятно човек да може да разбере кои организации разполагат с данни за него. Привържениците на по-голяма защита на личната неприкосновеност твърдят, че представители на правителствения и частния сектор взимат решения за техния живот на базата на информация, за която засегнатите индивиди дори не подозират. Случаят със събирането на информация за нашите навици за пазаруване е ярък пример за това. Ако, например, човек купува цигари не за себе си, а за друг член от семейството, информацията може да бъде предадена на застрахователната компания и това съответно да доведе до неблагоприятни последици върху застрахователната му полица.

По същество комисарите (с тази длъжност са по-известни висшите служителите за защита на личната неприкосновеност и данни например в Австралия, Нова Зеландия, Хонг Конг, Канада, Швейцария и

---

[16] **Brin, D.** (1998), "*The transparent society*", Perseus Books, New York; **Ellen, A. & Kennedy K.** (1997), The right to privacy, Baltimore Sun.
[17] Вж. 12.
[18] Вж. 12.

ФРГ) или държавните агенции са тези, които служат като алармена система за защитата на личната неприкосновеност. Затова тяхната ефективност бива измервана по способноста им да служат като "спирачка" при нарушаване на личната неприкосновеност. Поставя се въпросът дали контролните органи, които неминуемо ограничават възможността за намеса в личната неприкосновеност, са по-скоро в полза на законното наблюдение, отколкото на неговото ограничаване. Канада и Франция, съответно канадският комисар за личната неприкосновеност и френският орган за защита на данните, трябваше да положат огромни усилия, за да напомнят на правителството и неговите отдели за своето съществуване. В тази насока бе и изводът на Дейвид Флахерти, който прекара седем години като комисар на Британска Колумбия по въпросите на информационната и личната неприкосновеност.

Дали съществуването на контролни органи за защита на данните в Европа, в някои случаи вече повече от 20 години, е ограничило значително нарастването на наблюдението в правителствения и частния сектор? В действителност липсата на контролни органи явно не пречи на САЩ да предприемат множество инициативи за намеса в личната неприкосновеност. Реакцията през 2000 г. спрямо потенциала за наблюдение на чипа за идентифициране Pentium 3 е само друг пример за ефективна и в основата си успешна "народна" акция. Особено във връзка с банковия мониторинг, съмнително е дали служителите, назначени от управляващите, са се чувствали по-способни да помогнат с повече от пределно стореното. Много държави със законодателство в областта на личната неприкосновеност приеха "любезно" нива за финансово наблюдение доста над това, което е било предложено в САЩ[19]. Съдейки от европейския и австралийски опит, това, което може най-много да се очаква, е подчертаване на опасността за личната неприкосновеност, но и съобразяване с други обществени интереси. Твърде рядко комисарите за лична неприкосновеност са се чувствали способни да вземат страната на обществото и твърдо да се противопоставят на правителствените инициативи.

Законът за свобода на информацията е приет от Конгреса на САЩ още през далечната 1964 г., но на практика никога не е изпълняван от правителството, тъй като позицията на управляващите е, че тежестта на доказване за достъп до информация трябва да бъде върху гражданите. Много е трудно да се докаже и предположението, че информацията е придобита безплатно[20]. Освен това държавните представители ревниво пазят информацията, с която разполагат. Независимо от приемането на

---

[19] **Waters, N.** (1999), "*Re-thinking information privacy-a third way in data protection?*", 21st International Conference on Privacy and Personal Data Protection http://www.pco.org.hk/english/ infocentre/conference.html

[20] **Steele, F.** (1975), "The open organization-The impact of secrecy and disclosure on people and organisations", Addison-Wesley Publishing Company.

Закона за свобода на информацията в САЩ, задължаващ служителите да предоставят информация на всеки гражданин, който я поиска, имаше случаи, когато поисканата информация попадаше в няколкото освободени от това задължение категории, сред които и "националната сигурност"[21].

Повечето от законите в областта на личната неприкосновеност защитават само "лични данни" или "лична информация", като изискват информацията да може да бъде свързана с индивид, чиято самоличност може да бъде установена[22]. Все пак законодателството обикновено позволява данните, които са предмет на дискусия, да бъдат обединени с други данни, за да се установи самоличността, както и показва как може да се постигне подобно обединяване. Например в австралийския Закон за личната неприкосновеност от 1996 г. "лична информация" означава всякакъв тип информация за индивида, чиято самоличност е явна.

По делото "Пол срещу Дейвис" (1976)[23] Върховният съд на САЩ решава, че "области на лична неприкосновеност" се създават от действието на специфични гаранции и тези зони налагат граници върху правителствените органи. Към дейностите в рамките на тази "зони" се отнасят "въпросите, свързани с брака, създаването на потомство, семейни отношения, отглеждането на деца и образованието". По друго дело – „Уален срещу Рое"[24] съдът приема, че индивидите се ползват с предимство при определяне на разкриването на лична информация от правителството. По този начин се показва, че докато индивидите имат значителен интерес да защитават разкриването на лична информация, то този интерес може да бъде превишен по значение от интереса на правителството към информацията. Освен това в доклада на Кендал е заложена тезата, че конституционно защитената лична неприкосновеност не включва повечето данни за арести и осъждания, както и повечето други категории публично достъпна информация.

Политиката за ограничение на данните в частния сектор е неефективна, за да се избегне злоупотребата с информацията. Не е ефективна, не само защото законодателството на Европейския съюз не се прилага върху много от правителствените дейности и предоставя широк кръг от изключения за използването на данни "в името на обществото", например от правителствата, но също така, защото е малко вероятно, че може да се предотврати едно злонамерено управление посредством вече

---

[21] **Theoharis, A.** (1998), "*A culture of secrecy*", University Press of Kansas, USA; **Wiener, J.** (1998), "A culture of secrecy", edited by A. Theoharis, University Press of Kansas, USA.

[22] **Greenleaf, G.** (2001), *"IP, Phone Home"*, Information Technology and People, Emerald, vol. 14, issue 2, 206-231.

[23] **Paul-v-Davis** (1976), 424 U.S., 693, 713, http://www.oyez.org/oyez/resource/case/297/

[24] **Whalen-v-Roe** (1977), 429 U.S., 589, 599-600, http://www.law.cornell.edu/supct/html/historics/USSC_CR_0429_0589_ZS.html

съществуващи закони за защита на данните[25]. То би премахнало и заобиколило тези закони. Ако сме загрижени, че "големият брат ни гледа", ние би трябвало да наложим подходящи ограничения и на самия него.

Дори и да има законодателство, което да защитава личната ни неприкосновеност, разработени и усъвършенствани методи за наблюдение винаги могат да бъдат използвани за нейното нарушаване. Подобни техники могат да бъдат използвани незаконно от безскрупулни работодатели, детективи, търговци или обществени медии. Организацията "Международни потребители", която публикува резултатите от изследване на международните практики по отношение на личната неприкосновеност в Интернет, стига до извода, че на потребителите едва ли се предоставя право на избор дали искат да принадлежат към списък на адресати на съответната страница и дали имената им да се предоставят на трети лица.

В повечето случаи наблюдението на обществени места е напълно явно и се предприемат мерки за осведомяване за неговото съществуване, за да се увеличи ефективността за разкриване на престъпления. Но и срещу наблюдението на обществени места са изказани подозрения, че нарушава личната неприкосновеност. Първо, може да унижи хората като ги накара да се чувстват заподозрени, престъпници или граждани втора класа. Вторият довод срещу наблюдението на публични места е свързан с използването на информацията, събрана по този начин. Освен това може да бъде прието, че задължение на държавата е да се въздържа от извършването на наблюдение върху гражданите по начин, несъвместим със съответното ниво на уважение към личния им живот. Въпреки това има много малко законен контрол върху наблюдението на лични зони посредством технически средства, но няма никакъв законодателен контрол върху използването на агенти под прикритие[26]. Все повече и повече предоставяме доброволно личните си карти (ID), въпреки че по този начин не се удовлетворява основната потребност на обществото, а именно, всички хора да се идентифицират, когато служителите на службите за защита на обществения ред изискват това[27].

Все пак обществото е загрижено за личната неприкосновеност. Над четвърт милион жалби бяха подадени, след като в САЩ бе прокаран закон, който принуди банките да докладват за всяка съмнителна транзакция[28]. Поставени са основите на ENFOPOL 98 – система, която може да подслушва всички мобилни телефони, комуникацията по Интернет, факс-съобщения и пейджъри навсякъде в Европа. Защо тогава

---

[25] **Bergkamp, L. et al** (2002), "*EU Data Protection Policy*", Computer Law and Security Report, Vol. 18/1, 2002.
[26] **Birks, P.** (1997), "*Privacy and Loyalty*", Clarendon Press, Oxford.
[27] **Etzioni, A.** (1999), "*The limits of privacy*", Basic Books, USA.
[28] Вж. 21.

правителствата приемат закони в защита на личната неприкосновеност, след като обратни действия и без това биват предприемани? Когато през 1985 г. във Великобритания е приет Законът за подслушване на комуникациите, става очевидно, че той е предназначен да се погрижи за функционирането на системата ECHELON[29], контролираща всички международни комуникации към и от Великобритания. Специален параграф в закона – § 3 (2), позволява да бъдат издавани съдебни заповеди за подслушване на всякакъв тип информация към и от Британия, ако тя е "в интерес на националната сигурност" или "за нуждите на опазването на икономическото благосъстояние на Обединеното кралство". Без значение дали съдебната заповед позволява на американски агенти да подслушват частни британски комуникации, няма и съмнение, че британското законодателство е изготвено по начин, който повече насърчава, отколкото забранява развиващата се индустрия в комуникационното подслушване.

3. Правителствата и "другият начин"

Повечето защитници на личната неприкосновеност и обществените движения търсят трети вариант за разрешаване на проблема при съществуването на т. нар. "парадокс на личната неприкосновеност".

Всичко извън обхвата на файловете и записите, които са резултат от нашето взаимодействие с правителствените ведомства, изненадва доста хора. Човек не трябва да е известен, за да бъде обект на интерес. Когато ведомствата са по следите на шпиони, терористи или имат подозрения за организирана престъпност, десетки хиляди "обикновени граждани" са обхванати в мрежата от данни.

В самото начало инспекторите не знаят кой точно е обектът, замесен в конкретния случай или точно кои хора имат информация за него. Анализатори дори твърдят, че понякога наблюдението на американски граждани е неконституционно и / или противозаконно[30]. Причините за събиране на информация от правителството са безброй. По принцип повечето индивиди не биха се противопоставили при

---

[29] Терминът **ЕШЕЛОН (ECHELON)** се отнася до глобалната мрежа от компютри, която автоматично претърсва милиони съобщения по предварително дефинирани думи, факсове, телекси или електронни адреси. Анализи за предназначението на мрежата могат да бъдат открити в докладите на следните автори: **Campbell, D.** (1988) "Somebody's listening", New Statesman , 12/08/98, p. 10-12; **Lyon, D.** (2001), "Surveillance society: monitoring everyday life", Open University Press, Buckingham; **Davies, S.** (2001),*"Unprincipled privacy: why the foundations of data protection are failing us"*, University of New South Wales Law Journal, http://www/austlii.edu.au/au/journals/UNSWLJ/2001/7.html

[30] **Melanson, P.** (1984), " *The politics of protection*", Praeger Publishing, USA; **Melanson, P.** (2001), "*Secrecy Wars*", Brassey's Inc., Washington, D.C.

прилагането на законите и в системата за наказателното правосъдие да се използват технологии за провеждане на подходящи разследвания с оглед разрешаването на проблема с нарастващата престъпност. Но по-голямата част от гражданите би се отнесла резервирано относно това, дали прилагането на законите трябва да е свързано с неограничена възможност за събиране, натрупване, анализиране и разкриване на интимна лична информация, засягаща индивиди, които не са заподозрени в извършване на престъпна дейност. Този аргумент се допълва от социологическа гледна точка от неуспеха на законодателството да защити данните, както и от основателни съмнения доколко това е за благото на обществото. Вярно е, че ако Федералното бюро за разследване на САЩ може да декриптира тайни електронни съобщения, ще може по-добре да предотвратява планирането на операции от терористи, но това повдига въпроса за повече доверие в правителството. При достатъчно демократични гаранции всички жители имат полза от правителствения контрол, тъй като представителите на правителството знаят кое е добро за обществото и не биха злоупотребили с дадената им власт [31].

От друга страна се счита, че ние можем да изберем засилено наблюдение на обществени места и сгради като условие за по-голяма свобода[32]. Много често сме свидетели на противоречиви опити, като например на Европейския съюз, който прокарва своя собствена директива за защита на данните и в същото време заявява вниманието си върху проблеми като ЕНФОПОЛ[33]. Правителството като институция твърди, че сигурността на обществото е основна негова грижа, но това за съжаление може да се превърне в посегателство върху защитата на личната неприкосновеност[34]. На гражданите се представя едно просто уравнение: повече наблюдение означава повече сигурност. Въпреки това може да се твърди, че повече наблюдение не означава повече сигурност и това се доказва от актовете от 11 септември 2001 г.[35].

Колкото повече толерираме наблюдението, толкова повече се насочваме към т. нар. "пан-оптично общество"[36]. Наивно е да се вярва, че общества, в които се осъществява наблюдение, не биха просперирали поради съществуването на институция и законодателство за защита на

---

[31] **Etzioni, A.** (1999), "*The limits of privacy*", Basic Books, USA.

[32] **Brin, D.** (1998), "*The transparent society*", Perseus Books, New York.

[33] **ЕНФОПОЛ** (ENFOPOL съкратено от Enforcement Police) е обозначение на поредица от работни документи за наблюдение на телекомуникациите в Европейския съюз.

[34] **Pounder, C.** (2001), "The September 11th Terrorist Atrocity: Implication for Individual Privacy", Data protection and Privacy Practice.

[35] **Peissl, W.** (2002), "*Surveillance and Security-A Dodgy Relationship*", Institute of Technology Assessment, Austria , http://www.oeaw.ac.at/ita/pdf/ita_02_02.pdf

[36] "Пан-оптично общество" ("panoptic-society") – Гръцката дума "panoptos" означава "напълно видим".

данните: всъщност, една непредумишлена последица за тяхното съществуване е просперитетът на обществата под наблюдение, тъй като обществото има погрешно разбиране за сигурността, а институциите за защита на данните имат или са използвали ограничена власт[37]. Очевидно е, че политическата система (механизъм) във всяко общество е основна сила, която формира баланса на личната неприкосновеност, тъй като определени модели на лична неприкосновеност, разкриване и наблюдение са служебна необходимост за конкретния вид политически режим[38]. Затова наблюдението очевидно е основен начин за социален контрол и законодателството едва ли би могло да направи нещо повече по този въпрос. Може би то предлага доста добра правна рамка, но определено не е средство за постигане на определена цел.

Именно защото законодателството не предоставя сигурна защита на личната неприкосновеност, учените търсят и други начини за нейната защита. Ограничаването на наблюдението чрез артефакти, които съобщават обратно чрез дигитални мрежи до някакъв централен пункт за наблюдение, ще бъде ключов момент за неприкосновеността на личността през XXI век, а дигиталният механизъм ще бъде един от най-противоречивите примери[39]. Съвременното законодателство за защита на данните е създадено така, че по-скоро да управлява обработването на данните, отколкото да го ограничава. С други думи, политиката за информационна неприкосновеност на личността може да доведе до по-ефективен начин за управляване на употребата на личната информация, но тя не може да контролира нарастващата нужда от такава информация[40]. Действащото законодателство, което предотвратява подслушването, например Наказателните кодекси на някои държави, обявяват за престъпление незаконосъобразното подслушване на телефонните разговори. Същевременно е регламентирано, че на служителите на реда е позволено подслушване на телефонни разговори в определени случаи с разрешение от съдебен орган.

Може би използването на псевдоними би било възможно всеки път, когато е възможно да се предотврати злоупотреба с лична информация за двойна употреба, както и да се предотврати "охлаждащият ефект" върху свободата да четем, мислим и говорим, ако законът не може да справи с това. Все пак анонимността и псевдонимите

---

[37] Вж. 3.

[38] **Westin, A.** (1967), "*Privacy and Freedom*", The Bodley Head.

[39] **Greenleaf, G.** (2001), *"IP, Phone Home*", Information Technology and People, Emerald, vol. 14, issue 2, 206-231.

[40] **Bennett, C**. (2001), "*The western approach to privacy protection and the limits to its global diffusion*", Paper prepared for workshop on IT in China, http://web.uvic.ca/polisci; **Lyon, D.** (1994), *" The electronic eye: The rise of surveillance society*", University of Minnesota Press.

имат своите недостатъци[41]. Правните рамки като директивите на Европейския съюз в областта на защитата на данните не поставят ограничения върху събирането на анонимни данни (или псевдоними). Да се определи дали конкретен тип информация може обратно да бъде свързана с човека, много често е обект на дебат – дори произволно създаден псевдоним при определени обстоятелства може да бъде свързан с лицето.

Или може би трябва да уравновесим установените практики за лична неприкосновеност с удобството или неудобството, свързани с тях – ако хората трябва да стигнат докрай, за да защитят своята лична неприкосновеност, те няма да го направят[42], дори ако бъде въведена PKI (Инфраструктура на публичните ключове – йерархична система за ключове и сертификати, съставена от сертифициращи органи, които електронно подписват и публикуват в публичното пространство списъци със сертификатите на публичните ключове на всеки потребител) като основен способ да се защити начинът, по който комуникираме. Правителството също иска достъп до базата, в която се съхраняват личните ключове. Счита се, че PKI клони по-скоро към приемане, че всичко трябва да се върти около идентичността на притежателя на личния ключ, а тази негова идентичност е свързана с определена база-данни. Разчитането на самоличността като фокална точка или индекс би разкрило твърде много лична информация[43].

В някои страни комисарите по въпросите на личната неприкосновеност признават, че техните опити могат само да се плъзгат по повърхността на съгласието за упражняване на индивидуалните права и защита срещу други посегателства върху личната неприкосновеност. Личният самоконтрол трябва да бъде придружаван от регулиращи действия, ако целта е да постигнем "еднопосочност към лична неприкосновеност". Ако на индивидите се предложи да управляват собствената си неприкосновеност, това може да бъде доста съблазнително и никой няма да желае да спре този развой[44]. Както отбелязва Дайсън[45] "[клиентите] са твърде заети да консумират, да работят или просто да живеят живота си", за да защитават добре интереса си. Нереалистично е да се очаква, че хората ще водят преговори за всяка една транзакция, да превъзмогнат силната липса на равновесие на икономическите подбуди, които им се предлагат.

---

[41] **Langheinrich, M.** (1999), "*Privacy by Design*", ETH, www.inf.ethz.ch/~langhein/, Zurich.
[42] Пак там.
[43] **Hill, A & Hosein, G.** (1999), "*The privacy risks of public key infrastructure*", 21st International Conference on Privacy and Personal Data Protection http://www.pco.org.hk/english/infocentre/ conference.html
[44] Вж. 19.
[45] **Dyson,E.** (1998), "*Release 2.1*", Penguin.

Същността на личната неприкосновеност, защитавана от законодателството, трябва ясно да бъде определена от гледна точка на вреда и лек. Към "въображаемата вреда" трябва да се отнесем с комуникация и образованост, а не със законодателство или наредби[46]. След като хората разберат механизма на комерсиалното използване на информацията, предимството от потоците информация и цената на личната неприкосновеност, може да се окаже, че техните предпочитания към личната им неприкосновеност не са онези, в които са вярвали.

4. Заключение

Хората усещат, че губят контрол върху защитата на личната си неприкосновеност и вече не вярват в грандиозни обещания за конфиденциалност в свят, в който компютрите доминират, а повечето хора към момента едва осъзнават истинската обществена цена и влиянието на досиетата ни върху всеки от нас[47]. С колко точно от нашата лична неприкосновеност трябва да се разделим в името на удобството, преди обществото да се намеси и да ни попречи да продадем душите си[48]? А може би трябва да следваме съвета на Дейвид Флахерти "най-малкото да проявим ексцентричност" по отношение на т. нар. от американския експерт в областта на личната неприкосновеност Алан Уестин "фундаментализъм на личната неприкосновеност в някои области от нашия живот"[49]?

Точно липсата на доверие води до по-голямо наблюдение, тъй като наблюдението ни позволява да се доверим на другите, че то е необходимо, за да създадем репутация един спрямо друг. Макар че този аргумент е отново в полза на наблюдението, все пак са необходими граници, за които законодателството може да се погрижи[50]. Видно е, че повечето закони са безпомощни и правителствата едва се справят със скоростта, с която се развиват информационните технологии. Държавните граници явно са друго основно ограничение, тъй като всяка страна има собствено законодателство. В днешно време съществуват редица актове в областта на личната неприкосновеност, но може би само един малък процент от тях се изпълняват. Изследователят Агре[51] ни

---

[46] **Bergkamp, L.** (2001), "*Liability and environment: Private and Public Law Aspects of Environmental Harm in an International Context*", Kluwer Law International, The Hague; **Litan, R.** (1999), "*Balancing Costs and Benefits of New Privacy Mandates*", AEI-Brookings Joint Canter for Regulatory Studies, working paper 99-3, April 1999.

[47] **Laudon, K.** (1986), *"Dossier Society: Value Choices in the Design of National IS*", New York; Вж. 3.

[48] Вж. 41.

[49] Вж. 3.

[50] Вж. 10.

[51] **Agre, P. & Rotenberg, M.** (1997), "Technology and privacy: the new landscape", MIT Press, Cambridge. Mass.

убеждава: "и най-добрият закон в света е без стойност, ако не се изпълнява". Защо тогава да приемаме закони? Логично е да си зададем този въпрос.

Политиките за наблюдение са "очарователни". Правителствата привидно трябва да подкрепят наблюдението за законосъобразни цели, но също така искат да запазят индивидуалната лична неприкосновеност. Обаче според Дейвид Флахерти[52] малко вероятно е правителството или законодателната власт да предприеме обратна линия на поведение, т.е. към антинаблюдение, или да се въздържи от мерки без значително подтикване към тях. Ако наблюдението може да бъде възприето или оправдано в интерес на обществото, в този смисъл защитата на личната неприкосновеност би трябвало да остане предимно незаконодателна дейност в повечето сфери на човешкото съществуване, което означава, че, дори когато съществува законодателство за защита на личната неприкосновеност, индивидите ще трябва да разчитат на значителни усилия от тяхна страна, като например да откажат да предоставят лична информация, за да ограничат нежелано наблюдение. Освен това защитниците на данни трябва да бъдат активни и ангажирани, както и независими в упражняването на власт, за да служат като антинаблюдателна или уравновесяваща сила срещу прекалената и обезпокоителна практика за наблюдение.

Дори ако послушаме съвета на Дейвид Брин[53] за повече прозрачност и отговорност, няма начин да направим отговорността реалност в дългосрочен план без предприемане на официални контакти между правителствените представители и обществото. Въпрос на време е, преди "законът" да окаже натиск за поставяне на камери в домовете ни[54]. Бихме могли да твърдим, че според "закона" всички сме престъпници. Или може би не е икономически изгодно да се придържаме към законодателството и е по-лесно да прокараме нови закони, отколкото да позволим прозрачност. Въпроси, на които всички ние – индивид, общество и държава, трябва да намерим отговор.

Използвана литература:

Bing, J. (1999), *"Data protection, jurisdiction and the choice of law"*, University of Oslo, 21st International Conference on Privacy and Personal Data Protection, http://www.pco.org.hk/english/infocentre/conference.html

Bowden, C. (2002), *"CCTV inside your head"*, Computer and Telecommunications Law Review, Issue2.

[52] Вж. 3.
[53] Вж. 32.
[54] Вж. 12.

Bradford DeLong, J. (1998), "*The Transparent Society – a sociological forecast by David Brin*", www.j-bradford-delong.net/econ_articles/reviews/transparent. html
Consumers International, *Privacy@net: An international comparative study of consumer privacy on the internet* (2001), http://www.consumersinternational.org/ news/pressreleases/fprivreport.pdf May.
Effross, W. (1999), "*Commercial Profiles vs. Suspect Classification: Preparing, Preventing, and Parrying Public and Private Profiling*", Washington College of Law
Kendall, P. et al (1999), "*Gathering, analysis, and sharing of criminal justice information by justice agencies: the need for principles of responsible use*", US Department of Justice, Office of justice Programs, 21st International Conference on Privacy and Personal Data Protection http://www.pco.org.hk/english/ infocentre/conference.html
McChesney, J. (1997), An interview with David Brin, www.amazon.co.uk
Michael, J. (1994), "*Privacy and Human Rights*", Unesco Publishing
Mohammed, A. (1999), "*An Examination of Surveillance Technology and their Implications for privacy and related issues-the philosophical legal perspective*", Journal of Information, Law and Technology, 30 June 1999.
Neill, E. (2001), "*Rites of privacy and the privacy trade*", McGill-Queen's University Press 2001, Canada.
Nesson, C. (2001), *"Online privacy*", Harvard Law School, as seen at http://eon. law.harvard.edu/ilaw/privacy
Nixon-v-Administration of Gen. Serv., 433, U.S. at 457.
Norris, C. et all (1998), *"Surveillance, Closed Circuit Television and Social control*", Ashgate, Aldershot.
Paul-v-Davis (1976), 424 U.S., 693, 713.
Perri6 (1998), "*The Future of Privacy*", Vol 1, Donos, London.
Phillips, B., "*The concept of privacy*", www.rightoprivacy.com **Post, R.** (1989), "*The social foundations of privacy: community and self in the common law tort*", California Law Review 77.5, 957-1010.