ЕДИН ПОГЛЕД ВЪРХУ ПОЛУЧАВАНЕТО НА ИНФОРМАЦИЯ ЧРЕЗ СПЕЦИАЛНИ ТЕХНИЧЕСКИ СРЕДСТВА И КАНАЛИ

Илин САВОВ*

The article discusses different aspects of obtaining information through dedicated technical means and channels worldwide. Specific types of means of collecting information and their use by security structures are identified and evaluated. Data retrieval from networks is analyzed, based on the application of statistical techniques and programming algorithms.

Бурното развитие на техниката и технологиите през последните десетилетия предизвика още по-бързо развитие на техническите средства и системи в разузнаването. В създаването на средства и системи за водене на разузнавателна дейност във всички развити държави се влагат огромни средства. Стотици фирми в много държави работят в тази област. Този отрасъл на бизнеса отдавна е заел своето място в общата система на западната икономика и има своята здрава законодателна основа.

Според мненията на водещи експерти стойността на информацията при използване на специални технически средства (електронно наблюдение, проследяване и подслушване и др.) при разс-

* Авторът е професор, доктор, декан на Учебно-научен център „Национална сигурност и обществен ред“ във Висше училище по сигурност и икономика – Пловдив.

ледването на някои форми на тежки престъпления или терористични актове е несъмнена. Този метод е от изключителна важност за защитата на националната сигурност в съвременните условия.

Методът „получаване на информация чрез специални технически средства и способи“ обхваща набор от възможности и практики.

Условно методът „получаване на информация чрез специални технически средства и канали“ се дели на няколко отделни групи:

- Аудионаблюдение (Audio surveillance)
- подслушване на телефони разговори
- контрол на разговори, които се осъществяват по интернет (VoIP)
- контрол на разговори в помещение
- Визуално наблюдение (Visual surveillance)
- скрити видеонаблюдаващи устройства
- вградена видеосистема в превозни средства
- наблюдение чрез дрон (Surveillance Drones)
- Проследяващо наблюдение (Tracking surveillance)
- системи за глобално позициониране (GPS systems)
- мобилни устройства (mobile devices)
- устройства за радиочестотна идентификация (RFID)
- биометрични информационни технологии (сканиране на пръстовите отпечатъци, ириса, ретината на очите и т.н.)
- Контрол върху трафичните данни (Data surveilliance)
- наблюдение върху компютърната информация
- мониторинг върху използването на компютърни системи

Естествено, че всяко такова деление се явява условно (както впрочем и всяка друга класификация), тъй като практически всеки от посочените по-горе способи може в определени случаи да се яви съставна част на общия контрол върху наблюдавания обект, дори когато става дума за едно-единствено техническо средство. Например наблюдението над един смартфон може да служи за акустичен контрол на провежданите разговори, за проследяване на маршрута на движение на неговия притежател, за контрол на трафичните му данни, за мониторинг върху посетените сайтове в интернет и т.н. Ще се спрем накратко на състоянието на някои основни способи в световен мащаб.

Акустично наблюдение. Телефонният контрол е един от най-старите оперативни способи за получаване на информация.

Показателен е фактът, че само три години след като през 1876 г. Александър Бел получава патент на САЩ № 174465, описващ „метод и апарат (…) за предаване на говор и други звуци по телеграфа (…) с помощта на електрически вълни“, т.е. става дума за телефона, в САЩ е регистриран и патент за защита на телефоните от подслушване. Аудионаблюдението е отдавна известно на обществото и за него могат да се открият много литературни източници, включително и от български автори.

Официалното и неофициалното подслушване на телефонни линии днес е широкоразпространено. В САЩ например Законът за съобщителната помощ на правоохранителните органи (Communications Assistance For Law Enforcement Act – CALEA) изисква всички телефонни и VoIP комуникации[1] да са достъпни за разговори в реално време от федералните правоохранителни и разузнавателни служби.[2] Двете най-големи телекомуникационни компании в САЩ – AT&T Inc. и Verizon, имат договори с ФБР, които изискват те да пазят и правят записите си на телефонни разговори леснодостъпни за федералните агенции в замяна на 1,8 млн. долара годишно.

Не е необходимо хора да слушат повечето обаждания. Софтуер „говор към текст“ (speech-to-text) създава машинно четим текст от подслушвания разговор, който след това се обработва от автоматизирани програми за анализ на обажданията, като например тези, разработени от агенции като Office for Information Awareness или от компании като Verint и Narus, които за определени думи или фрази решават дали да се намеси човек при обработката и анализа.

Правоприлагащите и разузнавателните служби в Обединеното кралство и Съединените щати отдавна притежават технология за дистанционно активиране на микрофона в мобилните телефони,

---

[1] Voice over Internet Protocol (глас през IP, VoIP или IP телефония) е методология и група технологии за предоставяне на гласови комуникации и мултимедийни сесии чрез интернет протоколни (IP) мрежи, като например интернет. Термините „интернет телефония“ и „широколентова телефонна услуга“ се отнасят конкретно за предоставяне на комуникационни услуги (глас, факс, SMS, гласови съобщения) по обществения интернет, а не чрез обществената комутируема телефонна мрежа (PSTN).

[2] **CALEA:** The Perils of Wiretapping the Internet. *Electronic Frontier Foundation* (website). Retrieved March 14, 2009; **CALEA:** Frequently Asked Questions. *Electronic Frontier Foundation* (website). Retrieved March 14, 2009.

като използват функции за диагностика или поддръжка на телефони, за да слушат разговорите, които се провеждат близо до човека, който държи телефона.[3]

Мобилните телефони също често се използват за събиране на данни за местоположението. В САЩ този метод е известен под името „Location intelligence“ или „LOCINT“. Географското местоположение на мобилния телефон (и по този начин на лицето, което го носи) може лесно да се определи дори когато телефонът не се използва, като се използва техника, известна като „мултилатерация“ или „геолокация“, при което се изчислят разликите във времето за преминаване на сигнала от мобилния телефон към всяка от няколкото базови станции в близост до собственика на телефона. Законосъобразността на тези техники е била поставена под съмнение в САЩ, по-специално въпросът дали е необходима съдебна заповед за получаване на информацията. Записите за един телекомуникационен оператор (Sprint) показват, че за една година (между септември 2008 г. и октомври 2009 г.) федералните правоохранителни органи са поискали данни за местонахождението на клиентите 8 млн. пъти.[4]

Въпреки че CALEA изисква от телекомуникационните компании да изградят в своите системи възможността да се извършва законно подслушване, законът не е актуализиран, за да се отговори на въпроса за смарттелефоните и исканията за достъп до имейли и трафични данни (наричани още „метаданни“). Информацията, станала известна след изказвания на Сноудън, показва, че Агенцията за национална сигурност на САЩ (АНС) се възползва от това двусмислие в закона, като събира метаданни за „най-малко стотици милиони“ „случайни“ цели от целия свят. АНС използва аналитичен инструмент, известен като „CO-TRAVELER“, за да проследява хората, чиито движения се пресичат, и да открива скрити връзки с лицата, представляващи интерес.[5]

---

[3] **FBI** taps cell phone mic as eavesdropping tool. By Declan McCullagh and Anne Broache. Staff Writers, CNET News, December 1, 2006.

[4] **Zetter,** Kim. Threat Level Privacy, Crime and Security Online Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year. – In: *Wired* Magazine: Threat Level. Retrieved December 5, 2009.

[5] **Gellman,** Barton. NSA tracking cellphone locations worldwide, Snowden documents show. – In: *The* Washington Post. Retrieved November 1, 2014.

Контролът на разговорите в помещения или на открито предполага използването на микрофони с последващ запис на информацията. Този запис винаги се прави тайно и без съгласието или знанието на субекта. Микрофоните могат да са по-малки от една монета и да са тайно, незабележимо носени или монтирани. Независимо от затихването на звуковите вълни, микрофонът може да осигури ясен запис дори когато той е достатъчно далеч от разговарящите. Технологиите за аудионаблюдение често се използват за допълване на други технологии, като например определяне на местоположението и видеонаблюдение, като предоставят информация за контекста и подробности за разговорите. Все по-често тези устройства са разположени в публични зони за целите на мониторинга. Те могат да бъдат използвани по този начин за предотвратяване на престъпления, обаче приложението им според доста автори е лишено от балансирано отчитане на правото на личен живот и на ефективността на технологията за постигане на желаната цел. Това поражда сериозни опасения в обществото и може да има възпиращ ефект върху свободата на изразяване.

Визуално наблюдение. Визуалното наблюдение се използва от правителствата за събиране на разузнавателни данни, предотвратяване или разследване на престъпления, защита на процеси, на лица, група лица или обект. То се използва и от престъпни организации за планиране и извършване на престъпления, като грабежи и отвличания, от страна на бизнеса – за събиране на разузнавателна информация за конкуренти, а така също и от частни детективи. Може да се изпълнява с помощта на хора, но най-често чрез телевизионни системи за наблюдение и документиране на събитията.

Визуалното наблюдение се използва за наблюдение на помещения (частни или обществени), на открити площи (в обекти или населени места). При наблюдение на помещение камерите са камуфлирани в някакъв предмет в него и сигналът се предава по кабел или чрез радиосигнал. През последните години създаването на т.нар. „затворени телевизионни системи“ (Closed Circuit Television – CCTV) особено в градовете добива все по-широки размери. Те се наричат „затворени“, тъй като получаваната чрез тях информация не е за обществено ползване, а може да се ползва само от правоохранителните органи или от охранителните структури. Във всички случаи една от съществените им части са камерите за видеонаблюдение.

Камерите за наблюдение се използват за наблюдение на дадена зона (област). Те най-често са свързани със записващо устройство или IP мрежа и могат да бъдат наблюдавани от охраната на обекта или от полицейски служител. Камерите и апаратурите за запис бяха сравнително скъпи и изискваха в миналото човешки персонал да следи видеоинформацията. Днес анализът на кадрите е улеснен от автоматизиран софтуер, който организира цифровите видеозаписи в база данни с възможност за търсене и от софтуер за видеоанализ. Количеството на записаните кадри също се намалява драстично от т.нар. „сензори за движение“, които позволяват да се прави запис само когато се установи движение в наблюдаваната зона. За по-елементарни системи камерите за наблюдение са прости и евтини и могат да бъдат използвани в системите за домашна охрана и малки системи за ежедневно наблюдение.

В САЩ Министерството на вътрешната сигурност предоставя милиарди долари годишно безвъзмездни средства за национална сигурност на местни, държавни и федерални агенции за инсталиране на модерно оборудване за видеонаблюдение. Например град Чикаго, Илинойс, е използвал субсидия за вътрешна сигурност от 5,1 млн. долара, за да инсталира допълнително 250 камери за наблюдение към съществуващата мрежа от над 2000 камери и да ги свърже с централизиран мониторингов център. Говорейки още през 2009 г., кметът на Чикаго Ричард Далей обявява, че Чикаго ще разполага с камера за наблюдение на всеки уличен ъгъл до 2016 г. Но това изглежда твърде скромна цел в сравнение с плановете на Китай.

Като част от проекта „Златен щит“ (Golden Shield Project) на Китай няколко американски корпорации, включително IBM, General Electric и Honeywell, работят в тясно сътрудничество с китайското правителство, за да инсталират милиони камери за наблюдение в цял Китай заедно с усъвършенствани видеоанализи и софтуер за разпознаване на лица, да идентифицират и проследяват хората навсякъде, където отиват. Те ще бъдат свързани с централизирана база данни и станция за мониторинг, която след завършване на проекта ще съдържа снимка на лицето на всеки човек в Китай – на над 1,3 млрд. души.[6] Лин Джианг Хуай (Lin Jiang Huai) – ръководител на китайския офис „Технологии за информационна

[6] **Klein,** Naomi. China's All-Seeing Eye. Rolling Stone. Retrieved March 20, 2009.

сигурност“ (който отговаря за проекта), е кредитирал подобни системи за наблюдение в САЩ и Великобритания като благодарност за това, че те подпомагат неговата работа по проекта „Златен щит“.

Правителствата най-често първоначално твърдят, че камерите са предназначени да бъдат използвани за контрол на трафика, но много от тях в крайна сметка ги използват за общо наблюдение. Например във Вашингтон имаше 5000 „камери за трафик“, а след като всички са били монтирани на местата си, обединили всички заедно в една система и след това предоставили достъп към нея на столичния полицейски участък, за да могат да изпълняват „денонощен мониторинг“ (day-to-day monitoring).[7]

Разработването на централизирани мрежи от камери за видеонаблюдение, които наблюдават обществени места, свързани с компютърни бази данни със снимки и системи за идентифициране на хората (биометрични данни), дават възможност да се проследяват движенията на хората в целия град и да идентифицират с кого са били.[8],[9]

Авиационното наблюдение е извършване на наблюдение, обикновено визуално изображение или видео, от въздушно транспортно средство, като безпилотен летателен апарат (БПЛА), хеликоптер или шпионски самолет. Военните авиационни средства за наблюдение са известни много отдавна. Естествено, че подобни средства могат да се използват и при задачи от значение за националната сигурност и охрана на обществения ред. Но тук ще обърнем внимание на някои по-нови технологии.

Технологията за цифрови изображения, миниатюрните компютри и много други технологични постижения през последните две десетилетия допринесоха за бързия напредък на хардуера за наблюдение от въздуха, като например миниатюрните въздушните апарати, инфрачервената светлина и изображенията с висока разделителна способност, способни да идентифицират обекти на изключително големи разстояния. Например MQ-9 Reaper[10] – американски самолет, използван и за вътрешни операции от Минис-

---

[7] ***WIKILEAKS:*** Surveillance Cameras Around The Country Are Being Used In A Huge Spy Network. 2016-10-05.

[8] **EPIC** Video Surveillance Information Page. EPIC. March 13, 2009.

[9] **Hedgecock,** Sarah. TrapWire: The Less-Than-Advertised System To Spy On Americans. The Daily Beast. 2012-09-13.

[10] **Boyd,** Ryan. MQ-9 Reaper. Retrieved 2016-10-05.

терството на вътрешната сигурност, носи камери, които са в състояние да идентифицират обект с размери на картонена кутия мляко, летейки на надморска височина 60 000 фута (над 18 000 м), и има инфрачервени устройства, които могат да открият топлината на човешкото тяло на разстояния до 60 км.[11]

Министерството на вътрешната сигурност на Съединените щати е в процес на тестване на БПЛА за патрулиране на небето над Съединените щати за целите на защитата на критичната инфраструктура, граничния патрул, „транзитния мониторинг" и общото наблюдение на населението на САЩ.[12] БПЛА се използват и в операции на екипите на SWAT (Special Weapons And Tactics).[13]

Проследяващо наблюдение. Проследяващото наблюдение се различава от визуалното по това, че се проследява маршрутът на движение на човек, кола, предмет, без те да са в зоната на пряката видимост, или се отчита преминаването им през определени контролни пунктове. Много често в последните случаи това се използва в системите за контрол на достъп. Методите на извършване на проследяващо наблюдение са много и почиват на използването на различни физически принципи.

Устройството за GPS проследяване е устройство, което обикновено се носи от движещо се превозно средство или човек и което използва глобалната система за позициониране, за да определя и проследява периодично точното местоположение и оттам това на носителя. Записаните данни за местоположението могат да се съхраняват в структурата, която извършва проследяване, или да се

---

[11] **Friedersdorf,** Conor. The Rapid Rise of Federal Surveillance Drones Over America. Retrieved 2016-10-05.

[12] **McCullagh,** Declan. Drone aircraft may prowl U.S. skies. – In: *CNet* News. Retrieved March 14, 2009.

[13] В Съединените щати екипът на SWAT (Специални оръжия и тактики) е правоохранителна единица, която използва специализирано или военно оборудване и тактики. Първоначално са създадени през 60-те години на XX век, за да се справят с контрола на бунтовете или с въоръжени конфронтации с престъпници. Броят и употребата на екипите на SWAT се увеличават през 80-те и 90-те години, по време на акциите срещу наркотиците, а по-късно, след нападенията от 11 септември – в борбата с тероризма. В САЩ от 2005 г. насам екипите на SWAT са разгръщани 50 000 пъти всяка година, в почти 80 % от случаите за да обслужват заповеди за разследване, най-често за наркотици. Екипите на SWAT са все по-добре оборудвани с военни хардуерни устройства и са обучени да противодействат срещу заплахи от тероризъм, за контрол на тълпата и в ситуации, извън възможностите на обикновеното правоприлагане, считани за „високорискови".

предават в централна база данни или компютър, свързан с интернет, като се използва мобилен (GPRS или SMS) радио- или сателитен модем, вграден в устройството. Това позволява местоположението на обекта да се показва на фона на картата в реално време или при по-късен анализ на маршрута, като се използва софтуер за проследяване на GPS. Софтуерът за проследяване на данни е налице за смартфони с възможности за GPS.[14]

Мобилните телефони също често се използват за събиране на геолокационни данни. Географското разположение на мобилния телефон (и по този начин на лицето, което го носи) може лесно да се определи (независимо дали телефонът се използва или не), като може да се използва твърде различна техника, за да се изчислят например разликите във времето за преминаване на сигнала от мобилния телефон към всяка от няколкото базови станции в близост до собственика на телефона.[15],[16] През 2013 г. от 321 545 заявки за правоприлагане, направени от Verizon, 54 200 от тези искания са били за информация за „съдържание“ или „местоположение“, т.е. не само данни за клетъчни телефонни номера или IP адреси.[17] Информацията за съдържанието е включвала действителния текст на съобщенията, имейлите и подслушването на гласово съдържание или съобщения в реално време.

Обозначаването с радиочестотна идентификация (на англ. ез. RFID – Radio-Frequency IDentification) е използването на много малки електронни устройства (наричани „RFID тагове“), които се прилагат или се включват в предмет, животно или човек с цел идентифициране и проследяване чрез използване на радиовълни. Маркерите могат да бъдат прочетени от няколко метра разстояние. Те са изключително малки, така че могат да бъдат вложени в много видове ежедневни предмети и да бъдат използвани за проследяване и идентифициране на тези обекти за различни цели.

Един пример. Verichip е RFID устройство, произведено от фирмата Applied Digital Solutions (ADS). Verichip е малко по-голям от зърно ориз и може да се имплантира под кожата. Чипът е обвит в стъкло и съхранява VeriChip Subscriber Number, който скенерът

---

[14] **GPS** Cycle Computer v3. Axivo Inc. 22 April 2014.

[15] **Tracking** a suspect by mobile phone. – In: *BBC* News. March 14, 2009.

[16] **Miller,** Joshua. Cell Phone Tracking Can Locate Terrorists – But Only Where It's Legal. – In: *FOX* News. March 14, 2009.

[17] **Kappeler,** Victor. Forget the NSA: Police May be a Greater Threat to Privacy.

използва за достъп до личната ви информация чрез интернет от базата данни на Verichip Inc. „Global VeriChip Subscriber Registry". В Мексико например 160 работници в канцеларията на главния прокурор са били задължени да вкарат чип за проверка на самоличността и контрол на достъпа.[18]

Биометричното наблюдение е технология, която измерва и анализира физическите и/или поведенческите характеристики на човека за удостоверяване, разпознаване или скрининг.[19] Примерите за физически характеристики включват пръстови отпечатъци, ДНК и модели на лицето. Примери за предимно поведенчески характеристики включват движението (начина на ходене на човек) или гласа (начина на изразяване, бързината на говорене и т.н.).

Разпознаването на лицето е използването на уникалната конфигурация на лицевите черти на лицето, за да ги идентифицира точно, обикновено от видеонаблюдение. В много държави по света се финансират сериозни изследвания в областта на системите за разпознаване на лица. Службата за технологична обработка на информацията (Information Processing Technology Office) в САЩ например изпълни програма, позната като „идентификация на човек на разстояние", чрез която разработи технологии, които са способни да идентифицират хора на разстояние до 500 фута (150 м) по техните характеристики на лицето.

Друга форма на поведенчески биометрични данни, основаваща се на ефективни изчисления, включва компютрите, които разпознават емоционалното състояние на човека въз основа на анализ на израженията на лицето: колко бързо говорят, тон и стъпка на гласа, поза и други поведенчески черти. Това може да се използва например, за да се види дали поведението на дадено лице е подозрително.[20]

---

[18] **Gardener,** W. David (July 15, 2004). RFID Chips Implanted In Mexican Law-Enforcement Workers. Information Week. March 17, 2009.

[19] Скрининг (от англ. ез. *screening – пресяване, селектиране*) е систематичен изследователски метод, чиято цел е извършване на предварителен подбор чрез най-общо класифициране в предварително избрана област за изследване (проби или личности). Предварителният подбор или разслояването на извадката служи за намиране на обектите, които са носители на определени признаци и по-късно ще бъдат подложени на специално изследване.

[20] **Vlahos,** James. Surveillance Society: New High-Tech Cameras Are Watching You. – In: *Popular* Mechanics, March 14, 2009.

Перспективно направление е и профилирането и съхранението на данните от ДНК. ФБР изразходва 1 млрд. долара за изграждането на нова биометрична база данни, която ще съхранява ДНК, данни за разпознаване на лицето, данни за ириса или ретината на очите, отпечатъци от пръсти, отпечатъци от дланите и други биометрични данни за хората, живеещи в Съединените щати. Компютрите, които управляват базата данни, се намират в подземно помещение с размери около две американски футболни игрища.[21]

По-голямата част от компютърното наблюдение включва мониторинг на данни и трафик в интернет. В Съединените щати например съгласно Закона за съобщителната помощ на правоохранителните органи (Communications Assistance For Law Enforcement Act – CALEA) всички телефонни разговори и широколентов интернет трафик (имейли, уебтрафик, мигновени съобщения и т.н.) трябва да бъдат достъпни за безпрепятствен мониторинг в реално време от федералните правоприлагащи органи и агенции.[22]

В интернет има твърде много данни, за да могат хора да преровят ръчно всичко. Следователно автоматизираните системи за интернет наблюдение пресяват огромното количество трафик от интернет, за да идентифицират и докладват на анализаторите за трафика, какво се смята за интересно или подозрително. Този процес се регулира чрез насочване към определени „задействащи“ думи или фрази, посещаване на определени видове уебсайтове или комуникация чрез електронна поща или онлайн чат с подозрителни лица или групи.[23] Милиарди долари годишно се изразходват от агенции като АНС, ФБР и вече липсващата Служба за оценка на информацията (Information Awareness Office) за разработване, закупуване, внедряване и експлоатация на системи като Carnivore, NarusInsight и ECHELON, за да осъществяват прихващане и анализ на всички тези данни и да извличат само информацията, полезна за правоприлагащите и разузнавателните служби.[24]

---

[21] **Nakashima,** Ellen. FBI Prepares Vast Database Of Biometrics: $1 Billion Project to Include Images of Irises and Faces.– In: *Washington* Post, pp. A01, May 6, 2009.

[22] **CALEA** Archive – Electronic Frontier Foundation. *Electronic Frontier Foundation* (website). March 14, 2009.

[23] **Hill,** Michael. Government funds chat room surveillance research. – In: *USA* Today, Associated Press, March 19, 2009.

[24] **McCullagh,** Declan. FBI turns to broad new wiretap method.– In: *ZDNet* News, September 26, 2014.

Компютрите могат да бъдат и са цел за наблюдение. Ако някой може да инсталира софтуер от типа на Magic Lantern и CIPAV на ФБР, той лесно може да получи неоторизиран достъп до тези данни. Такъв софтуер може да бъде инсталиран физически или дистанционно. Друга форма на компютърно наблюдение, известно като „Van Eck phreaking“[25], обхваща четене на електромагнитни излъчвания от компютърни устройства, за да извлича данни от тях на разстояния стотици метри.[26] АНС поддържа база данни, наречена „Pinwale“, която съхранява и индексира голям брой имейли както на американски граждани, така и на чужденци. Освен това АНС изпълнява програма, известна като „PRISM“, която е система за извличане на данни, даваща на правителството на Съединените щати директен достъп до информация от технологични компании. Чрез достъп до тази информация правителството може да получи историята на търсене, имейли, съхранявана информация, чат на живо, прехвърляне на файлове и др.

Извличането на данни от мрежите се базира на прилагането на статистически техники и програмни алгоритми, за да се открият преди това незабележими взаимоотношения в данните. Профилирането на данни в този контекст е процес на събиране на информация за конкретен индивид или група, за да се генерира профил – това е картина на техните модели и поведение. Профилирането на данни може да бъде изключително мощен инструмент за анализ на психологическата и социалната мрежа.

Икономически трансакции (като например покупки с кредитни карти) и социални трансакции (като телефонни обаждания и имейли) в съвременното общество създават големи количества съхранявани данни и записи. Днес много от тези записи са електронни, което води до създаването на т.нар. „електронна пътека“.

---

[25] Van Eck phreaking е форма на подслушване, при която се използва специално оборудване за събиране на страничните радиочестотни електромагнитни излъчвания от електронни устройства, които са свързани със скрити сигнали или данни с цел да се пресъздадат тези сигнали или данни, за да се шпионира електронното устройство. Излъчванията от страничните радиочестотни ленти съществуват и с подходящото оборудване могат да бъдат заснети от клавиатури, компютърни дисплеи, принтери и други електронни устройства. Носи името на холандски инженер, открил метода и направил демонстрации пред журналисти.

[26] **Van Eck,** Wim. (1985). Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? (PDF). – In: *Computers* & Security, 4 (4): 269 – 286. doi:10.1016/0167-4048(85)90046-X.

Всяко използване на банкова машина, плащане с кредитна карта, използване на телефонна карта, обаждане от дома, проверка на библиотека, нает видео или друга завършена записана трансакция генерира електронен запис. Обществените записи, като раждане, съд, данъци и други документи, все повече се цифровизират и се предоставят онлайн. Електронното водене на данни прави данните лесносъбираеми, съхранявани и достъпни, така че е възможно обемно и ефективно събиране и анализ при значително по-ниски разходи.

Друга обща форма на наблюдение е и създаването на карти на социалните мрежи, базирани на данни от сайтове за социални контакти, като Facebook, MySpace, Twitter, както и от информация за анализ на трафика от записи на телефонни обаждания и др. След това тези „карти“ на социалната мрежа се анализират, за да предоставят полезна информация, като лични интереси, приятелства и връзки, желания, убеждения, мисли и дейности.[27]

Литература

1. **CALEA:** The Perils of Wiretapping the Internet. *Electronic Frontier Foundation* (website). Retrieved March 14, 2009.

2. **Zetter,** Kim. Threat Level Privacy, Crime and Security Online Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year. – In: *Wired* Magazine: Threat Level. Retrieved December 5, 2009.

3. **Gellman,** Barton. NSA tracking cellphone locations worldwide, Snowden documents show. – In: *The* Washington Post. Retrieved November 1, 2014.

4. **Friedersdorf,** Conor. The Rapid Rise of Federal Surveillance Drones Over America.

5. **Nakashima,** Ellen. FBI Prepares Vast Database Of Biometrics: $1 Billion Project to Include Images of Irises and Faces.– In: *Washington* Post, pp. A01, May 6, 2009.

[27] **Ethier,** Jason. Current Research in Social Network Theory. Northeastern University College of Computer and Information Science. Archived from the original on February 26, 2015. Retrieved March 15, 2009.