
PUBLIC
DOMAIN

Какво точно събират МВР и ДАНС за всеки един гражданин използващ мобилен телефон и/или Интернет.

Автор:
Богомил „Бого“ Шопов – http://bogomil.info
shopov.bogomil@gmail.com

Съдържание

За това издание на е-книгата....3
Дарения....3
Как държавата ни следи в Интернет и чрез мобилните ни телефони....3
Директива 2006/24/ ЕО за задържането на данни (data retention). 4
А у нас?....4
Малко повече за регулацията....4
Какво се случи през последната година?....5
Следенето на практика....6
Примери....6
Гривната....6
Досието....7
Журналистът....7
Следенето на практика: Германия....8
Следенето на практика: Примерът от Естония по Бтв....9
Още примери....10
Как да се защитим законно срещу проследяване в Интернет....10
Лични данни....10
Защита в Интернет – E-mail....11
Защита в Интернет – IP адрес....11
Добрата новина....12
Лицензи:....13
Контакти....13
Дарения....13
Ремиксиране....13

За това издание на е-книгата

Това е второ издание на тази е-книга. Тя не претендира за изчерпателност за красив дизайн или за високи технически познания от страна на автора. Опитал съм се да опиша нещата на езика на крайния потребител, а не да използвам много технически термини, които биха били интересни за професионалисти.

Част от тези материали са публикувани в списание “.net”, където се надявам да ги прочетете и на хартия.

Дарения

Ако е-книгата ви е харесала, като съдържание, защото като визия едва ли ще ви направи впечатление, можете да ми дарите няколко валутни единици чрез paypal: b@bogomil.info или bitcoin-и на 1PXw9m6Thv3hW75BjDFxzSDDxp16tU7bQi

Как държавата ни следи в Интернет и чрез мобилните ни телефони.

Сигурно сте чули, чели или видели за намеренията на Държавата да следи мобилните ни телефони и кореспонденцията ни в Интернет, което вече е факт, чрез Закона за Електронни съобщения.

За да обхвана тази огромна материя, трябва да започна доста преди събитията от последните години да започнат да се случват.

Нарушаването на цифровите права на гражданите започва много отдавна - от както в България се появяват мобилните телефони, а в последствие и Интернет. Още тогава Държавата, чрез различни формирования, едно от които е НСБОП, има директна и непроследима връзка към мобилните оператори чрез която може да вземе информация за всеки един телефонен разговор.

Това разбира се е “законно”, защото по силата на закона за МВР, приет от Народното събрание, “всички трябва да оказват съдействие на МВР”.

Доста по-късно след въвеждането на този “независим интерфейс” към всичко, което правят всички притежатели на мобилни телефони и тези ползващи Интернет се появява още еднин документ, които трябва да се спомене.

Директива 2006/24/ ЕО за задържането на данни (data retention).

Тя беше обсъждана и приета от Европейския парламент в отговор на терористичните удари в метрото в Лондон. Още тогава по-време на обсъжданията се чу мнението, че отговор на една терористична заплаха, чрез ограничаване на свободите на гражданите и чрез непрекъснатото им наблюдаване в всъщност победа на тероризма, защото реалната цел на всички подобни движения е именно подкопаване на исконните демократични ценности на обществата.

Директивата беше приета с много малко мнозинство и беше решено да се използва само в краен случай, за определен род престъпления и то допста внимателно. Като вкарването на това законодателство не беше задължително за страните членки, доста от които все още се възползват от това си право.

А у нас?

В началото 2008 година Държавната агенция за информационни технологии (ДАИТС), съвместно с работна група от МВР се опитва да прокара Наредба 40 към Закона за Електронните съобщения (ЗЕС), която има за цел безконтролното задържане на данни на всички български граждани използващи Интернет и мобилни телефони.

Разбира се, държавата в лицето на тези две агенции се беше престарала със пренасянето на евро-документа към нашето законодателство, защото тази директива беше удобен начин да се узаконят, иначе незаконните достъпи на МВР до комуникацията на всички граждани, за които говорих в началото и са удобен начин да се даде пълен достъп до данните за комуникацията на всички граждани.

Малко повече за регулацията

Предложението за следене на информационния трафик имаше за цел да разкрие кой на кого се е обаждал и изпращал имейли, какви сайтове са посещавали хората и дори къде са били на всяко едно време, чрез техническите средства вградени в мобилните телефони, чрез които става възможно техническото функциониране на GSM мрежата.

На телефонните компании и доставчиците на Интернет услуги беше наредено да запазват цялата информация за трафика на клиентите си. Достъп до тези данни беше даден на полицейските власти и разузнавателните агенции в Европа.

Задържането на данни е агресивен метод, който се намесва в личния живот на 450 милиона души в Европейския съюз и безпрецедентно разширява правата на полицейско наблюдение. В същото време нарушава много от инструментите, гарантиращи човешките права в Европа, като Директивите за защита на данните и Европейската конвенция за правата на човека.

Задържането на данни означава, че управляващите могат да се намесват в частния ви живот и личната ви кореспонденция, без значение дали сте заподозрян извършител на престъпление или не.

Какво се случи през последната година?

След множество гласувания, промени, протести и смяна на правителства, финалния вид на закона беше приет и влезе в сила през пролетта на 2010 година. По неговата сила МВР, ДАНС и още няколко служби ще могат да използват данните събирани за всички граждани, само ако има разрешение на прокурор и ако тези данни биха могли да се отнасят за определени групи престъпления.

Може би всичко изглежда нормално, но всъщност не е. Основен проблем, както и в самото начало е това, че се събират данни за всички български граждани, без да има правно основание за това и се нарушава принципа за невинност.

Всеки е невинен до доказваме на противното, нали?

Макар, че законодателят твърди, че информацията, която се събира за всеки един гражданин не е лична, то беше показано с едно просто уеб приложение, че макар и да не се събират лични данни, все пак тези данни биха разкрили много неща за всеки един и чрез използването им, може да бъде проследен всеки един човек, къде се е намирал, какво е правил и с кого е контактувал, както и може информацията може да бъде използвана за направата на профил, което е нарушение на правото на неприкосновеност и на повечето от човешките права в конвенцията за защитата им.

От друга страна всеки ден ставаме свидетели за толкова злоупотреби с данни на високо ниво и се усеща чувството за недоверие и в службите, които трябва да защитават демокрацията и в държавата като цяло, а за да поверим данните с в ръцете на някого, трябва да му имаме доверие – нали?

Следенето на практика

След като по-горе бях писал за законовата страна на нещата и за евро-директивите, и се бях засилил да пиша следващата част, която да покаже теоретично какво точно може да се прави с данните, който държавата събира за всеки един от нас, когато в Германия се появи много интересен случаи как точно може да се използват данните в практиката, а дори след публикуването на този текст в списание „.НЕТ“ по Бтв излезе чуден репортаж, за това как с данните събирани по електронен път може да си види ВСИЧКО за вас, и то без дори да дадете разрешението си.

Примери

Преди да започна обаче искам да споделя два от любимите си примери какво точно може да се прави със тези, уж невинно изглеждащи данни за нашия електронен живот, съдържащи трафични данни, към които всеки нормален човек би погледнал с неразбиране.

Станахме свидетели в последно време на хиляди начини секретни данни да изтекат в публичното пространство, както и да се появяват флашки с всичко с което ви е нужно за да навредите на някого.

Ето три реални примера, който могат да опишат какво само може да се прави с тези данни, които ние доброволно предоставяме на МВР, ДАНС и други служби, най-често без да знаем:

Гривната

Гледали сме по филмите как на престъпниците им слагат гривна на ръката или на крака за да може да ги следят къде ходят или да не се отдалечават на 100 метра от жилището си. Всеки един от нас, близо 99% от населението, разполага с мобилен телефон, някой с два или три.

За да може да работи той, периодично, без да говорите по него, съобщава на мобилния оператор къде се намира и мобилния оператор записва това местоположение, нещо повече, чрез ЗЕС ще се събира информация, която да може да локализира човека с точност до 60 метра за голям град и 200 за извън града.

Без да знаете, вие бивате следен, доброволно и всеки, който би искал да знае къде се намирате, може да направи справка.

Разбира се веднага можете да сметнете това за добра идея, но ви съветвам да помислите пак. Искате ли ВСИЧКИ да знаят къде ходите? Не цените ли собствената си неприкосновеност?

Досието

По старите от нас, знаят за досиетата. Ако не сте чували за тях - прочетете някъде, защото това е една срамна част от историята на Европа.

Половината българи доносничеха за другата половина на специалните служби, за да могат да си купят луканка, такъв беше живота. Тези досиета се използваха за мръсни цели - за изнудване, за изтребване на хора в лагери, за натиск, за политически и граждански шантаж и за какво ли не.

Сега "благодарение" на технологиите този тип информация се събира автоматично - кого познаваш, къде се намираш, с кого си говорил, колко често, какви услуги използваш и още много неща, за да се направи едно ново електронно досие за теб.

Чрез тези данни, които разбира се, не включват съдържанието на съобщенията, може да се проследи какво си правил през последната една година, с кого и колко пъти. Могат да се направят много пресечки на тази статистическа информация, която е свободно достъпна за всеки един гражданин.

Не бяхме ли невинни до доказване на противното? Защо ни следят тогава? Наистина, тази мярка ми се струва на аналогична, всеки един гражданин да бъде съпровождан от полицай докато се движи и си върши работата.

Журналистът

Приемаме, че имаме двама герои - един журналист и един източник, който има важна информация за това, че в МВР има голяма корупционна сделка.

Всеки един журналист има конституционно гарантирано право да пази тайната на източника си, ако това застрашава неговата свобода, неприкосновеност или по други съображения. Това е начинът по който (трябва да) работи един демократичен процес.

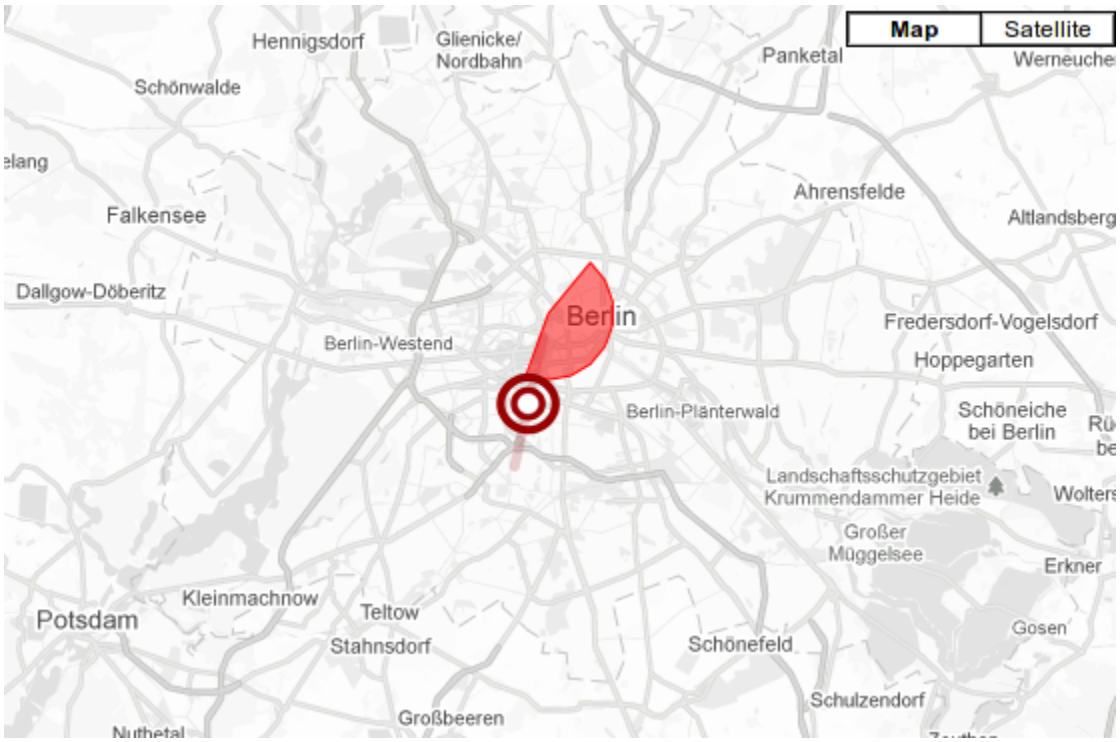
След въвеждането на директивата за задържане на данни, вече е достатъчно един от двамата да проведе разговор или да напише email и тайната на източника,

остава само имагинерна измислица във волята на законодателя преди .. доста години.

Сигурно ще се запитате, кой би го направил това? Кое правителство или кой човек, не би ИСКАЛ да знае, кой има уличаващи данни за него? Все още ли мислите, че всичките ни тайни са наша собственост?

Следенето на практика: Германия

Ако посетите този адрес: http://opendata.zeit.de/widgets/dataretention/ можете да видите какви данни са събрани с течение на времето за един германски политик и как точно може да се използват те.



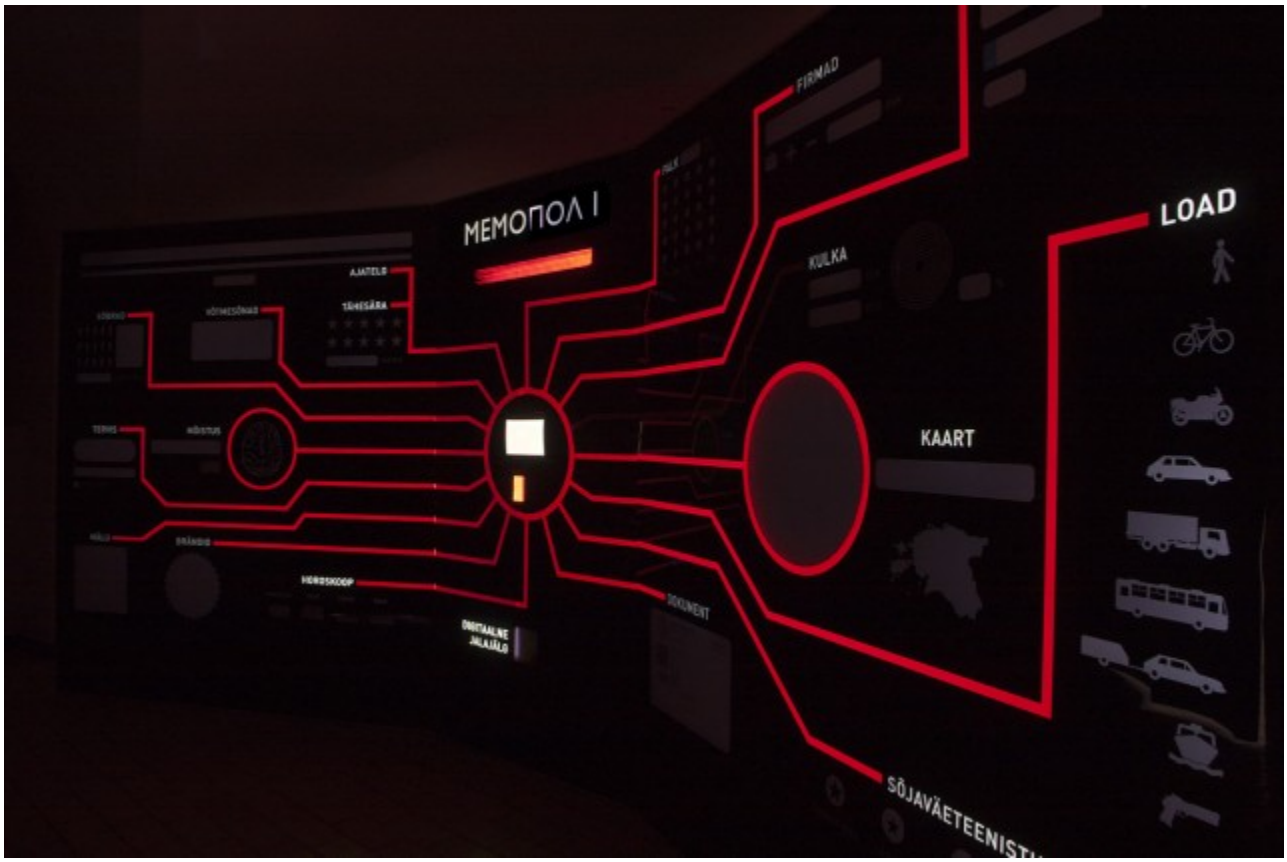
Обърнете внимание на картата, която е показана на сайта. Тя показва местоположението на този човек, който в случая може и да сте вие, защото за пореден път напомням, че данни се събират за всеки един човек, намиращ се на територията на Европа.

Можете да видите, колко телефонни разговора са проведени, по кое време, с кого (макар, че в примера тези данни са скрити), колко кратки съобщения са получени (също може да се разбере от кого и кога), както и Интернет активността през мобилния телефон.

Ако сте маниаци на тема данни, можете да видите данните в суров вид ето тук: https://spreadsheets.google.com/ccc?key=0An0YnoiCbFHGdGp3WnJkbE4xWTdDTVV0ZDlQeWZmSXc&hl=en_GB&authkey=COCjw-kG#gid=0

Следенето на практика: Примерът от Естония по Бтв.

Ето тук можете да видите, какво например може да се направи с данните съхранявани за вас от държавата в Естония.



(c) http://timo.dart.ee/works/memopol/

Репортажът представа една “арт-инсталация”, която показва всичко, което е правил един гражданин през почти целия си живот: http://www.btv.bg/shows/btv-reporterite/videos/video/857871299-bTV_Reporterite_Estoniya.html (вижте след 14:38 минута). Проектът се казва „Memopol“ и повече за него, може да се види тук: http://timo.dart.ee/works/memopol/

Още примери

Вижте ето това малко приложение: http://bogomil.info/dr/ То показва, повечето категории събирани данни, както и тяхната комбинация, така, че да се проследи движението и поведението на човек в рамките на цяла година, дори и повече.

Ако пък имате малко време, можете да прегледате малкото филмче, което се намира тук, което е правено преди няколко години, но все още е актуално за ситуацията в момента.
http://www.efb.bg/flv/naredba40.html

Как да се защитим законно срещу проследяване в Интернет.

Това е третата и последна част от поредицата за закона за задържане на данни на теория и на практика. Ако не сте прочели предните 2 материала ви съветвам да го направите.

Искам да отворя една голяма скоба и да кажа, че това което ще представя тук е написано за широката публика и ще изпусна доста от специфичните технически детайли, който можете свободно да намерите в Интернет, ако пожелаете.

Лични данни

Преди да започна с техническите средства за защита, бих искал да се спра на едно много важно условие – да пазите личните и чувствителните си данни.

Ако имате практика да публикувате личните си данни навсякъде, както и да споделяте всички със всички дори и най-доброто технически средство няма да ви помогне.

Пример:
Преди няколко дни получих следния e-mail, по повод на едно събитие, което организирам.

“Здравейте,
Казвам се Петър Петров, журналист съм в ... с ЕГН 9999999999 и искам да се регистрирам за събитието, което организирате”

Ето за това говоря – всеки обича да споделя с идеята, че това което напише, ще се чете само от подателя. За съжаление в Интернет не е така. Електронната поща преминава през различни сървъри, на различни места в мрежата и дори през различни континенти докато достигне до вас и всеки има възможност с безплатни програми и начини да прочете какво има в съобщението.

Ето точно заради това, смешно звучат опитите на държавата да ни обясни, как тя ще взема

само част от съобщенията, а другата част ще е “защитена”. Бабини деветини, като определение би подхождало най-много на случая.

От друга страна, много популярно е да използваме програми, които постоянно показват къде се намираме – като twitter, foursquare и т.н и всеки би могъл да влезе и да види къде сте се намирали в рамките на 2-3 месеца назада, че дори и повече, без да е нужно използването на специални разузнавателни средства дори :)

Първата стъпка към защитата в Интернет е да внимаваме какво данни публикуваме, къде и най-вече с кого, като все пак не забравяйте, че собствениците на сайта могат лесно да видят цялата ви информация и дори да я предоставят на трети страни, почти без никакви условия (пише го с малки бели букви на бял фон в условията на повечето сайтове).

Защита в Интернет – E-mail

Ако използвате български доставчик на електронна поща като abv.bg, mail.bg, email.bg и други подобни – спасение няма. Те пазят информация за всяко изпратено/получено писмо от вас и могат да го предоставят на всеки, които има “законен” начин да го изисква.

Ако използвате подобни услуги базирани извън България – gmail.com, hotmail.com, mail.yahoo.com или подобни, имайте предвид, че агенцията към МВР, която разследва престъпления, може да изиска от доставчика – да речем Google за gmail.com да направи копие на вашата пощенска кутия и други услуги, които ползвате и да ги предостави с допълнителна информация на тази агенция. Това може да се случи, само ако сте извършили престъпление, защото тази процедура минава през различна правова рамка от тази в България, което е една малка и добра новина.

Ако искате да имате пълен контрол върху вашата поща, можете да си купите домейн и хостинг (за 30-40 лева на година) и да обслужвате сам пощата си – като триете и съхранявате, каквото вие счетете за добре. Имайте предвид, че това което в момента се намира на сървъра на доставчика (този от когото сте си купили хостинга) също подлежи на задължението да предостави данните срещу лист хартия и печат.

Затова внимателно избирайте държавата и компанията от която да си купите хостинг.

Да, точно така – ако искате да повишите сигурността си, трябва да отделите време. Най-лесно е да се абонирате за някаква уеб-базирана услуга (отнема 30 сек) и след това да не бъдете защитени по никакъв начин

Защита в Интернет – IP адрес

Вашето IP е начин да бъдете идентифициран в Интернет. По силата на Закона за електронните

съобщения, доставчика ви на Интернет е длъжен да знае, за всеки акаунт, в определено време, кой IP адрес отговаря и кой е собственика на този акаунт.

Тоест, ако ползвате Интернет от доставчик XXX.bg той е длъжен, ако бъде попитан на кого е бил определен IP адрес в 8.10 сутринта, той трябва да даде реален човек.

Това, разбира се понякога е трудно да стане, но не трябва да разчитаме на това. След въвеждането на директивата за задържане на данни – се появи чудесен бизнес модел в по-свободните страни, а именно да се предлага използването на VPN от където поискате по света до тях.

Една от тези фирми например е https://www.relakks.com/. Те предоставят възможността да се абонирате за тяхната услуга, срещу определена сума, която не е никак висока и да използвате техен IP адрес, за който те НЕ съхраняват никаква информация, освен тази която вие сте въвели при регистрацията (а тя съвсем не трябва да отговаря на истинските ви данни :)).

По силата на шведското законодателство, то може да изиска тази информация при доста сериозни нарушения. Разгледайте сайта и вижте какво точно се предлага. Впечатление прави едно послание, което продава доста добре тази услуга:

“For security reasons RELAKKS do not use any American software neither for encryption nor for any other part (we anticipate that most users will in spite of that use an American OS),”

Повече за законодателната рамка и за това какво се пази за вас и за какво не се пази, можете да видите тук: https://www.relakks.com/faq/security/?cid=gb&lang=en

Много внимавайте в коя държава се намира компанията, която предоставя подобни услуги, защото, ако например си вземете подобна услуга в Швейцария и свалите един торент, доставчика ви ще получи предупредително писмо, което е вероятно и вие да получите със страшни думи – но не се връзвайте много.

Добрата новина

Добрата новина, че цялата тази простотия отива към своя край. Преди няколко месеца беше поръчано проучване от страна на европейските институции за ефективността на тази мярка и резултатът според блогът на Нели Огнянова (http://nellyo.wordpress.com/2011/06/09/200624/) е, повече от интересен и очакван.

Европейският надзорен орган по защита на личните данни публикува официална позиция относно ефективността на Директива 2006/24/ЕО за запазване на трафични данни.

Според прессъобщението, количествената и качествена информация, предоставена от държавите, не е достатъчна да обоснове положително становище относно необходимостта от запазването на данни, регламентирано в директивата.

Лицензи:

Контакти

Можете да ми пишете на shopov.bogomil@gmail.com или да посетите блога ми http;//bogomil.info

Дарения

Ако книгата ви е харесала, можете да ми дарите няколко валутни единици чрез paypal: b@bogomil.info или bitcoin-и на 1PXw9m6Thv3hW75BjDFxzSDDxp16tU7bQi

Ремиксиране

Ако мислите, че можете да направите по-добра визия на тази е-книга или имате по-интересна идея за представяне на проблема, сте свободни да ремиксирате съдържанието, както желаете. Ще ми е любопитно да видя все пак резултата :)