СБОРНИК МАТЕРИАЛИ ПО НАЦИОНАЛНА СИГУРНОСТ, ТЕРОРИЗЪМ, КОНТРОЛИРАНЕ НА ТЕЛЕФОННА И КОМПЮТЪРНА КОМУНИКАЦИЯ

RiskMonitor
WWW.RISKMONITOR.BG

AMERICA FOR BULGARIA
FOUNDATION
Фондация Америка за България

СБОРНИК МАТЕРИАЛИ ПО НАЦИОНАЛНА СИГУРНОСТ, ТЕРОРИЗЪМ, КОНТРОЛИРАНЕ НА ТЕЛЕФОННА И КОМПЮТЪРНА КОМУНИКАЦИЯ

Настоящата публикация се осъществява
с подкрепата на Фондация „Америка за България“.
Мненията и позициите в изданието принадлежат
единствено на авторите на този материал.
Те по никакъв начин не могат да се приемат за
израз на мнение и позиции на донорската организация.

AMERICA FOR BULGARIA
FOUNDATION
Фондация Америка за България

Фондация „Америка за България” подпомага израстването и укрепването на динамична пазарна икономика и демократично общество в България и подкрепя страната в постигане на пълния ѝ потенциал на успешна и модерна европейска нация. Основана през 2008 година, Фондацията е наследник на Българо-американския инвестиционен фонд, създаден от правителството на САЩ чрез Американската агенция за международно развитие. Грантовете, които Фондация „Америка за България” предоставя, продължават отношенията на доброжелателство и приятелство между народите на САЩ и България.

СБОРНИК МАТЕРИАЛИ ПО НАЦИОНАЛНА СИГУРНОСТ, ТЕРОРИЗЪМ, КОНТРОЛИРАНЕ НА ТЕЛЕФОННА И КОМПЮТЪРНА КОМУНИКАЦИЯ

Съставители: Георги Петрунов и Радостина Михалкова
Преводач: Марианна Панова
Редакция и коректура: Евгения Мирева

Фондация РuckМонитор© ISBN 978-954-2914-46-4
София, 2016

Фондация **РuckМонитор**
България, София 1000, бул. „Цар Освободител“ 29
ел. поща: riskmonitorinfo@gmail.com
www.riskmonitor.bg

Съдържание

ПРЕДГОВОР

Настоящият сборник събира материали, които са преведени от три специализирани наръчника за разследване, предназначени за обучение на американски прокурори и представители на други агенции към Департамента по правосъдие на САЩ.

Сборникът е публикуван в рамките на проект „Специализирана прокуратура срещу организираната престъпност“, изпълняван от фондация „Risk-Монитор“ с финансовата подкрепа на фондация „Америка за България“. Основна цел на проекта беше повишаване капацитета за противодействие на организираната престъпност на българските специализирани прокуратури. В рамките на проекта бяха организирани поредица обучителни семинари за специализираните прокурори и съдии с водещи лектори от САЩ и Европейския съюз.

С последните изменения в българското законодателство, приети в средата на 2015 г., Специализираната прокуратура и Специализираният наказателен съд получиха компетенции да работят по всички случаи по Глава първа от Наказателния кодекс, която касае престъпленията против републиката, в това число и случаите на тероризъм. Първата част от сборника ще бъде полезна в подготовката и практиката на специализираните прокурори и съдии. Материалите, включени в сборника, имат много по-широко приложение и ще бъдат от полза и за представители на другите институции, ангажирани с опазване на националната сигурност и противодействие на тероризма в Република България. Заедно с потенциала за развитие на практическите знания на българските магистрати и представители на правоохранителните органи, събраните текстове могат да бъдат от полза и при разработването на подготвяните през последните месеци нормативни документи, включително и специален закон, насочени към борбата с тероризма.

Втората част от сборника е посветена на подслушването. Няколкократно през последните години в България темата за подслушването и контрола при използване на това специално разузнавателно средство беше в основата на грандиозни публични скандали, които за дълго време привличаха общественото внимание. Очевидна е необходимостта от засилване на контрола и предотвратяване на бъдещи случаи на нарушение, като в същото време се гарантират възможностите за ефективно използване на подслушването като метод за събиране на годни съдебни доказателства. Американски опит за постигане на тази цел е представен във втората част.

Третата част от сборника е посветена на друга особено актуална тема – събирането на доказателства от компютърни и електронни из-

точници. Някои от разглежданите въпроси в тази част от сборника все още не са публично поставяни в България, докато в САЩ е натрупан огромен опит със значителна съдебна практика. Например, съдебните заповеди с точно описана информация, за която има разрешение да бъде иззета, без да се изземва целият компютър. Тази практика гарантира, че лица и фирми, които осъществяват със същия компютър легална дейност, няма да търпят неправомерни загуби.

Всяка от трите части на сборника акцентира върху изключително актуален проблем с оглед на съвременния български контекст. Надяваме се идеите от публикуваните материали да провокират съответните законодателни и организационни промени, за да реализират своя потенциал за разрешаване на очертаните проблеми.

Радостина Михалкова

Правен съветник
Посолство на САЩ в София

Георги Петрунов

Ръководител на проект
„Специализирана прокуратура срещу организираната престъпност“

ПЪРВА ЧАСТ: ТЕРОРИЗЪМ И ДРУГИ ЗАПЛАХИ ЗА НАЦИОНАЛНАТА СИГУРНОСТ

1. ИНСТИТУЦИИ В НАКАЗАТЕЛНОПРАВНАТА СИСТЕМА НА САЩ

Наказателноправната система е само едно от средствата в арсенала на САЩ в борбата срещу тероризма. Международният тероризъм може да бъде и е бил третиран като военен и дипломатически проблем, основен обект на тайни операции и специални икономически санкции. Тъй като националната сигурност по същество е отговорност на върховния главнокомандващ, различните агенции в изпълнителната власт имат задачата да разработят програми и протоколи, които да възпрепятстват тероризма и в най-лошия случай същите тези агенции ще трябва да отговорят на терористичните акции. Идеалният апарат за борба срещу тероризма е онзи, при който различните федерални служби, отговарящи за мерките за борба срещу тероризма, схващат както общата картина, така и уникалната си роля в нея, а всяка една от тях се стреми да представя алтернативи пред президента, който е върховната инстанция за вземане на решения в страната. Важно е федералните прокурори, чиято роля в борбата срещу тероризма непрекъснато нараства, да разберат тази динамика. Тази глава разглежда институциите на САЩ за борба срещу тероризма, както и уникалната роля на Департамента по правосъдие.

ДЕПАРТАМЕНТА ПО ПРАВОСЪДИЕ И ФЕДЕРАЛНОТО БЮРО ЗА РАЗСЛЕДВАНЕ

Департамента по правосъдие посредством различните си компоненти участва в събирането, производството и потреблението на разузнавателни данни. Въпреки че федералните прокурори обикновено са потребители на разузнавателна информация, промените, приети след гласуването на PATRIOT Act на САЩ, допускат обмен на известна информация между Голямото жури и органите на правоприлагането, от една страна, и разузнавателната общност на САЩ. Важно е федералните прокурори да разберат как ФБР събира разузнавателните данни и това са данните, които ще бъдат най-адекватни при прилагането на мерки за борба срещу тероризма. Законът и указите на президента вменяват на ФБР първостепенната роля

за провеждането на разследвания на територията на САЩ, свързани със заплахи за националната сигурност. Това включва водеща роля в рамките на страната при разследването на международни терористични заплахи срещу САЩ и при провеждането на контраразузнавателни дейности за посрещане на разузнавателни и шпионски усилия на чуждестранни организации, насочени срещу Съединените щати. ФБР изпълнява също така важни функции в събирането на чуждестранни разузнавателни данни като агенция, член на разузнавателната общност на САЩ. В съответствие с това ФБР играе ключова роля при прилагането на федералния закон и правилното правораздаване в САЩ, при защитата на националната сигурност и при получаването на информация, нужна на САЩ за провеждане на външната политика. Тези роли отразяват широкия спектър от настоящите отговорности на ФБР, което изисква от ФБР да бъде както агенция, която ефективно открива, разследва и предотвратява престъпления, така и агенция, която ефективно защитава национална сигурност и събира разузнавателни данни. Звеното за национална сигурност на ФБР, създадено през 2005 г. с директива на президента, обединява мисиите и ресурсите на елементите, свързани с борбата срещу тероризма, контраразузнаването, оръжията за масово унищожение и разузнаването под егидата на висш служител на Бюрото. Звеното за национална сигурност се ръководи от изпълнителен заместник-директор и помощник изпълнителен заместник-директор. Звеното за национална сигурност се състои от Отдел за борба с тероризма, Отдел за контраразузнаване, Дирекция „Разузнаване", Дирекция за оръжия за масово поразяване и Център за изследване на тероризма. Центърът за изследване на тероризма играе ключова роля за набавянето на актуални разузнавателни данни на държавните и местни правоприлагащи органи. Изпълнителният помощник-директор на Звеното за национална сигурност е основната свръзка на ФБР с Офиса на директора на националното разузнаване и останалата част от разузнавателната общност. В Звеното за национална сигурност работят и служители, които наблюдават администрирането на проекти, свързани с националната сигурност, и координират въпроси по националната сигурност между петте компонента на Звеното за национална сигурност и други подразделения на ФБР.

СЪВМЕСТНИТЕ ЕКИПИ СРЕЩУ ТЕРОРИЗМА НА ФБР

Съвместните екипи срещу тероризма, ръководени от ФБР, са огневата линия на борбата срещу тероризма и се състоят от малки клетки от специално обучени, внедрени по места предани следователи, анализатори, лингвисти, експерти по специални оръжия и тактики и други специалисти от редица американски правоприлагащи и разузнавателни агенции. Съвместните екипи срещу тероризма са разположени в 103 града из цялата страна, включително най-малко по един във всяка една от 56-те служби на ФБР по места. Когато се разследва тероризъм, съвместните екипи проследяват подозрения, събират улики, осъществяват арести, осигуряват охрана за специални събития, провеждат обучения, събират и споде-

лят разузнавателни данни и отвръщат незабавно на заплахи и инциденти. Съвместните екипи имат основна роля при разбиването на терористични клетки и при проследяването на източниците на финансирането на терористите. Съвместните екипи се координират от междуведомствения Национален съвместен екип срещу тероризма, което гарантира, че информационният и разузнавателен поток протича свободно между съвместните отряди по места. Съвместните екипи работят в тясно сътрудничество с федералните прокурори при разследването и преследването на терористични актове.

ОТДЕЛЪТ ЗА НАЦИОНАЛНА СИГУРНОСТ (ОНС) В ДЕПАРТАМЕНТА ПО ПРАВОСЪДИЕ

Отделът за национална сигурност (ОНС) бе създаден през 2006 г. и се ръководи от предложен от президента и одобрен от Сената помощник главен прокурор за национална сигурност. Трима заместник-помощник главни прокурори наблюдават всекидневната работа на Отдела и докладват на помощник главен прокурор. ОНС се състои от четири сектора: Сектор за борба срещу тероризма (СБТ), Сектор „Контраразузнаване“ (СК), Сектор „Разузнаване“ (СР) и Правно и политическо бюро. Един заместник-помощник главен прокурор наблюдава работата на прокурорите от ОНС в секторите СБТ и СР и се фокусира върху усилията на Отдела да осуети терористичните заплахи и заплахите за националната сигурност посредством разследвания и възбуждане на съдебни дела. Вторият заместник-помощник главен прокурор наблюдава дейността на СР и неговите усилия да осигури на изпълнителите необходимите разузнавателни средства, особено онези, предоставени от Закона за наблюдение на външното разузнаване (ЗНВР). Третият заместник-помощник главен прокурор наблюдава работата на Правното и политическото бюро, като дава правни съвети по въпроси, които възникват по време на разузнавателни и разследващи дейности, и разработва политики, стратегии и законодателни инициативи, свързани с въпроси на националната сигурност. Отделът за национална сигурност (ОНС) има също така Правно бюро за жертви на терористични актове в чужбина и Бюро за преглед на чуждестранните инвестиции. Първостепенните цели на ОНС са: (1) Централизация на управлението на програмата за национална сигурност на Департамента по правосъдие; (2) Координация на операции и политики в целия спектър на националната сигурност; (3) Осъществяване на последователно наблюдение на националната сигурност и (4) По-нататъшно обучение и експертиза по въпросите на националната сигурност.

Отделът за национална сигурност е отговорен за осигуряване на координация по всички въпроси, свързани с националната сигурност, между различните компоненти на ДП; всички федерални агенции, включително ФБР, Отдела за вътрешна сигурност, Държавния департамент, Министерство-

то на финансите, Министерството на отбраната, членове на разузнавателната общност и 94-те щатски прокуратури.

КОНСУЛТАТИВНИТЕ СЪВЕТИ ЗА БОРБА СРЕЩУ ТЕРОРИЗМА НА ДЕПАРТАМЕНТА ПО ПРАВОСЪДИЕ

На 17 септември главният прокурор нареди всеки прокурор на САЩ да определи опитен помощник-прокурор на САЩ за координатор на Консултативния съвет за борба срещу тероризма (КСБТ) във всеки окръг. Отговорностите на щатския прокурор и на координатора на КСБТ във всеки щатски прокурорски офис са следните: (1) да свиква и провежда срещи на федерални, щатски и местни правоприлагащи служби за обмен на информация и обучение; (2) да гарантира, че участващите федерални, щатски и местни агенции работят координирано и свободно споделят информация; (3) да осигури консенсус сред отделните членове на координатора на КСБТ за проактивни инициативи с цел защита на критична инфраструктура в окръга; (4) да бъде свръзка между регионалните КСБТ координатори на СБТ и Националния КСБТ координатор по дела, приоритети и стратегии и (5) да гарантира дългосрочния фокус на членуващите агенции върху борбата срещу тероризма. Колкото до основните оперативни аспекти на разследванията за тероризъм, КСБТ работи в партньорство със Съвместните групи срещу тероризма, които носят основна отговорност за терористичните разследвания и които координират бюрата на ФБР по места с техните партньори във федералните, щатски и местни правоприлагащи агенции при провеждането на международни и вътрешни разследвания. КСБТ координаторът е главното лице за контакт в своя офис за всички разследвания и съдебни дела, както и за всички КСБТ дейности. Секторът за борба срещу тероризма (СБТ) има шест регионални КСБТ координатори и национален КСБТ координатор, който е основна контактна точка в ДП за КСБТ координаторите в щатските прокурорски офиси.

ОТГОВОР ПРИ КРИТИЧНИ ТЕРОРИСТИЧНИ ИНЦИДЕНТИ

Регионалните КСБТ координатори и националният КСБТ координатор играят важна роля за отговор на потенциални критични терористични инциденти. Ако регионалният КСБТ координатор научи за някакъв инцидент или въпрос в даден окръг, който би могъл да има някаква връзка с тероризма, или за инцидент, в който тероризмът не е отхвърлен изцяло като възможна причина, този координатор веднага се свързва с КСБТ координатора в Офиса на щатския прокурор, за да го уведоми и за да се увери, че Офисът е запознат с инцидента. По същия начин КСБТ координаторът в Офиса на щатския прокурор е длъжен да уведоми регионалния КСБТ координатор на СБТ или националния КСБТ координатор, в случай че научи за потенциален терористичен инцидент, засягащ неговия/нейния окръг. Щом СБТ научи за някакъв инцидент, веднага определя регионалния КСБТ координатор, нацио-

налния КСБТ координатор или друг прокурор от СБТ за контактна точка във връзка с конкретния инцидент, който продължава да работи заедно с КСБТ координатора в Офиса на щатския прокурор. Контактна точка на СБТ е единственото лице за контакт за инцидента и дава възможност на окръжния КСБТ координатор да комуникира с един-единствен източник от ДП, вместо да отправя поредица запитвания из цялото ДП. Контактната точка на СБТ отговаря за обмена на цялата свързана с инцидента информация с Отдела за национална сигурност и Департамента по правосъдие, които следва да бъдат запознати със случая. Регионалните КСБТ координатори на СБТ също така координират инциденти, които могат да засегнат няколко окръга. При тези инциденти, свързани с повече от един окръг, регионалните КСБТ координатори определят възможно най-бързо кои са засегнатите окръзи и влизат във връзка с КСБТ координатора в тези окръзи, за да го информират кой щатски прокурорски офис на ФБР ръководи следствието и за да гарантират, че всички засегнати окръзи работят координирано и разполагат с необходимата им информация. Тези регионални и национални КСБТ координатори на СБТ са на разположение 24 часа в денонощието, седем дни седмично по телефона или имейла, а с тях може да се осъществи връзка и посредством Правосъдния команден център.

2. РАЗСЛЕДВАНИЯ, СВЪРЗАНИ С ТЕРОРИЗЪМ

Изисквания за уведомяване, консултация и разрешение при дела, свързани с тероризъм

След терористичните атаки на 11 септември 2001 г. главният прокурор разработи различни инициативи, за да осигури агресивна, последователна и координирана национална изпълнителна програма за предотвратяване, осуетяване и наказване на действията на международните терористи. Департамента по правосъдие и Конгресът също така подчертаха нуждата от широк обмен на информация, свързана с тероризма, между и сред различните компоненти на ДП и други изпълнителни агенции, включително необходимостта подходящата информация, събрана в централата, да се сведе по места, както и да се осигури приток от долу към централата. С оглед широките правомощия на федералното правосъдие по въпроси, свързани с международен тероризъм, и очевидната необходимост да се осигури добре координиран федерален отговор по такива дела бяха постановени изисквания за уведомяване, консултация и одобрения във връзка с дела, свързани както с международния, така и с вътрешния тероризъм. Координацията се осъществява от Отдела за национална сигурност (ОНС) и в частност от неговия Сектор за борба с тероризма (СБТ). Изискванията за уведомяване, консултация и одобрение при дела, свързани с тероризъм, са записани в Наръчника на прокурорите на САЩ. Наръчникът на прокурорите на САЩ определя делата по закон или като Първа категория дела, включващи основни обвинения в тероризъм като записаните в Глава 18 от Кодекса на САЩ,

параграф 2339А (Предоставяне на финансова подкрепа на терористи), или като Втора категория дела, повдигнати въз основа на традиционни не-терористични обвинения, използвани в терористични казуси, описани в Глава 18 от Кодекса на САЩ, параграф 1001 („Неверни показания").

Закони за международен тероризъм (Първа категория)

Федералните закони, изброени в този подраздел, олицетворяват намерението на Конгреса да разшири юрисдикцията на Съединените щати да разследват и преследват международния тероризъм или които редовно се използват при дела, свързани с международен тероризъм. Ако Първа категория закон се използва при разследване на тероризъм, който не е изцяло вътрешен – тоест разследване на тероризъм, в което участват чужди граждани, места в чужбина или връзки с чужди страни или групи – делото следва да бъде разглеждано като дело за международен тероризъм. Това включва използването на описан закон като обект на конспирация, предикат за RICO (Закон за рекета и корупцията), или друго престъпление.

Други международни терористични дела (Втора категория)

Различни други федерални закони могат да бъдат използвани, за да се предотвратят действията, да се разкъсат клетките и да се накажат международните терористи. В тях са включени описаните по-долу закони, както и много други федерални престъпления включително, но не само измами, имиграционни нарушения, незаконно притежаване на оръжие, престъпления, свързани с наркотици и неверни показания, в някои от които изобщо няма елементи на тероризъм, а в други – само на вътрешен тероризъм.

Въпреки това обаче, ако разследването, в което се използва законът, потвърди наличието на връзка с международния тероризъм, включително, но не само каквато и да е връзка или позоваване на конкретна чуждестранна терористична организация, то се включва в политиката, разглеждана в този раздел.

Уведомяване: Уведомяването на Сектора за борба с тероризма (СБТ) е задължително при всички въпроси, свързани с международен тероризъм или с вътрешен тероризъм. Това първоначално уведомяване обикновено се осъществява, когато помощник-прокурор на САЩ научи за терористично дело, възбудено от ръководения от ФБР Съвместен екип срещу тероризма, и започва да го наблюдава. Това уведомяване трябва да бъде осъществено от регионалния координатор на Консултативния съвет за борба срещу тероризма (КСБТ) на Сектора за борба срещу тероризма (СБТ) или националния КСБТ координатор и може да бъде направено по електронната поща или по телефона или, когато е необходимо за защита на класифицирана и чувствителна информация, по защитен факс, защитен телефон или защитен имейл. Щом получи уведомяването, СБТ ще реши дали регионалният координатор на СБТ ще проследи делото, или ще назначи друг СБТ прокурор.

Одобрения: Одобрението от помощник-прокурора по национална сигурност е задължително, когато настъпи „значителен развой“ в дело от Първа категория. Одобренията не са задължителни при дела от Втора категория, освен ако не се изискат изрично от помощник-прокурора за национала сигурност. „Значителен развой“, изискващ одобрение от ОНС, включва попълване на съдебна заповед за обиск, призоваване на материални свидетели, обвинения, важни съдебни пледоарии, споразумения, отхвърляне на обвиненията/параграфи и обжалвания.

3. РАЗСЛЕДВАНИЯ, СВЪРЗАНИ С НАЦИОНАЛНАТА СИГУРНОСТ

Указанията на главния прокурор за вътрешни операции на ФБР дават насока за всички разследващи дейности на ФБР на територията на САЩ. Наръчникът на ФБР за вътрешни разследвания и операции, който всъщност прилага Указанията, стандартизира политиката на ФБР по отношение на всички криминални дела, свързани с националната сигурност и разследващи дейности на чуждестранни разузнавателни служби, провеждани в Съединените щати.

Разследванията на ФБР попадат в пет основни категории: (1) Преценки; (2) Предварителни разследвания; (3) Пълни разследвания; (4) Разследване на начинания и (5) Позитивни разследвания на чужди разузнавания. Както се вижда от заглавията, дълбочината и обхватът на методите на разследване нарастват с нивото на разследването. С изключение на обиските, които изискват съдебна заповед, и електронното наблюдение под Раздел III на Закона за наблюдение на чуждо разузнаване, което изисква пълно разследване, всички законни следователски методи са на разположение на етапа на предварителното и пълното разследване, въпреки че е възможно да изискват някаква степен на одобрение от наблюдаващ орган. Освен че дават насоки за обмена на информация, тези политически документи задължават ФБР да уведомява ОНС за всички пълни разследвания, свързани със събиране на данни от чужди разузнавания или разследвания на граждани на САЩ, когато събирането на данни и разследването е свързано със заплаха за националната сигурност. По-нататък ФБР трябва да уведомява ОНС, когато започва пълно разследване на група или организация (разследване на начинание), в случай че има връзка с тероризъм или друга заплаха за националната сигурност. Указанията на главния прокурор за вътрешни операции на ФБР и Наръчникът на ФБР за вътрешни разследвания и операции също поставят върху ФБР изисквания за допълнително одобрение и наблюдение в случаите, когато има чувствителна следствена тема, която е определена в Указанията на главния прокурор за вътрешни операции на ФБР като: разследване относно дейностите на висш държавен служител или кандидат на политическа партия (свързани с корупция или заплаха за националната сигурност), религиозна или политическа организация, или

лице на ръководен пост в такава организация, или новинарска медия, или всяка друга тема, която по преценка на висшия служител, дал разрешение за провеждането на разследването, следва да бъде сведена до вниманието на Централата на ФБР и други високопоставени служители на Департамента по правосъдие.

Преценки

Според Наръчника на ФБР за вътрешни разследвания и операции преценката по същество е първоначално и ограничено разследване, основано върху твърдение. За провеждането на преценка не се изискват факти. Обикновено преценките са рутинна следователска дейност, за да се определи дали се налага по-нататъшно разследване.

Предикатни разследвания

Следващото ниво е предикатното разследване, което означава, че е налице известна информация, която полага основата за по-нататъшно разследване. Предикатните разследвания се разделят на предварителни разследвания и пълни разследвания. Предварителните разследвания могат да бъдат възбудени, когато е налице „твърдение или информация“, която сочи за евентуална престъпна дейност или за заплаха за националната сигурност. Пълно разследване може да бъде възбудено, когато съществува „формулирана фактическа основа“ за криминална дейност или за заплаха за националната сигурност. Пълните разследвания се разпределят в три категории: (1) един/повече от един субект; (2) начинание и (3) позитивно събиране на чужди разузнавателни данни.

4. ЗАКОН ЗА НАБЛЮДЕНИЕ НА ЧУЖДО РАЗУЗНАВАНЕ

Законът за наблюдение на чуждо разузнаване (ЗНЧР) от 1978 г., с направените поправки, оторизира освен всичко останало четири типа следователска дейност, разгледани по-нататък: (1) електронно наблюдение; (2) физически претърсвания; (3) проследяване на входящи и изходящи телефонни обаждания и (4) изискване на бизнес документация (принудително представяне на материални вещи). По закон власт да одобрява исканията във връзка със ЗНЧР има Съдът за наблюдение на чуждото разузнаване (СНЧР). „Законът за наблюдение на чуждото разузнаване се прилага само във връзка с електронното наблюдение и физическото претърсване на лица или общности на чужди държави или агенти на чужди държави, или проследяването на входящи и изходящи телефонни обаждания и принудителното представяне на материални вещи само в контекста на разследване във връзка с националната сигурност.“ Съдът за преглед на наблюдението на чуждото разузнаване е апелативният съд на СНЧР. И двата са съставени от федерални съдии, назначени от председателя на Върховния съд на САЩ.

Искания за прилагането на ЗНЧР обикновено произтичат от ФБР, което подава формална молба до Разузнавателната служба на Отдела за национална сигурност (ОНС). След получаването на такава молба прокурор от разузнавателната служба започва да работи заедно с агент от ФБР, за да се проверят фактите, необходими в подкрепа на искането по ЗНЧР. След това прокурорът от РС подготвя комплект документи за кандидатстване, който се състои от заверена апликационна форма, положителна резолюция от високопоставен правителствен служител (обикновено директора на ФБР или заместник-директора) и предложени първични и вторични заповеди на вниманието на СНВР. Всяка апликация трябва да бъде одобрена от главния прокурор, преди да бъде подадена в СНЧР. За нуждите на ЗНЧР терминът главен прокурор означава „главния прокурор на САЩ (или действащ главен прокурор), заместник главния прокурор (на САЩ) или по преценка на главния прокурор – помощник главния прокурор, определен като помощник главен прокурор за националната сигурност...“. Освен това преди подаване пред СНЧР документите минават през разработени от ФБР процедури, за да се провери достоверността на фактическата информация, съдържаща се в тях.

„Международен тероризъм“

Този термин е още един белег, който подчертава международната връзка, изисквана от ЗНЧР.

Глава 50 от Кодекса на САЩ, параграф 1801 (с) определя „международен тероризъм“ като дейности, които –

(1) са свързани с насилствени действия или действия, опасни за човешкия живот, които са в нарушение на наказателните закони на САЩ или на отделния щат или които биха представлявали престъпно нарушение, в случай че бъдат извършени на територията на САЩ или на всеки щат;

(2) вероятно имат за цел –

(А) да сплашат или упражнят принуда върху цивилно население;

(Б) да повлияят върху политиката на дадено правителство посредством принуда или сплашване или

(В) да променят позицията на дадено правителство чрез извършване на убийство или отвличане и

(3) се случват извън територията на САЩ или преодоляват националните граници в смисъл на средствата, с които са осъществени, лицата, които трябва да бъдат сплашени или принудени, или мястото, където извършителите действат или търсят убежище.

Третата точка е ключова за установяването на международното естество на тероризма и за да се изключи вътрешният тероризъм. Въпреки

това обаче самите терористични актове (или планирани актове) могат да бъдат замислени да се случат в Съединените щати, доколкото има международна връзка, която отговаря на тази точка в закона, като терористичен акт, планиран да бъде осъществен на територията на САЩ от международна терористична групировка.

„Информация от чуждо разузнаване“

Терминът „информация от чуждо разузнаване“ също така често се среща в ЗНЧР. Например, както се разисква по-долу, за прилагане на електронно наблюдение и физическо претърсване ЗНЧР изисква определеният висш чиновник от съответния изпълнителен орган да гарантира пред Съда за наблюдение на чуждо разузнаване (СНЧР), че информацията, която се търси чрез прилагането на ЗНЧР, е информация от чуждо разузнаване; че „първостепенно основание“ за наблюдението или обиска е да се получи информация от чуждо разузнаване и че такава информация не може да бъде получена чрез обикновени следователски техники. Според този стандарт информацията от чуждо разузнаване трябва да бъде първостепенното основание за наблюдението или обиска под ЗНЧР, а „единствената цел“ може да не се ограничава само до „да се докаже престъпно поведение в миналото“, за да се накаже агентът. Според Глава 50 от Кодекса на САЩ, параграф 1801(е) „информация от чуждо разузнаване“ означава:

(1) информация, която има връзка със, а ако засяга американски гражданин, е необходима за способността на САЩ да се защитават срещу – (А) действителна или евентуална атака или други сериозни враждебни действия на чужда държава или на агент на чужда държава; (Б) саботаж, международен тероризъм или международното разпространение на оръжия за масово унищожение от чужда държава или агент на чужда държава; или (В) подривни разузнавателни дейности на разузнавателна служба или мрежа на чужда държава или от агент на чужда държава; или

(2) информация във връзка със, а ако засяга американски гражданин, е необходима за – (А) националната отбрана или сигурността на САЩ; или (Б) провеждането на външната политика на САЩ.

Стандартът за дефинициите на информация от чуждо разузнаване зависи от това дали информацията засяга гражданин на САЩ. Ако търсената информация не засяга американски гражданин, информацията трябва само „да има връзка с“ описаните по-горе дейности. Ако обаче търсената информация засяга американски гражданин, информацията трябва да бъде „необходима за“ описаните по-горе дейности.

ЗАПОВЕДИ ЗА НАБЛЮДЕНИЕ ПО ЗНЧР

Основание за провеждане на електронно наблюдение е дадено в Глава 50 от Кодекса на САЩ, параграфи 1801-1812. (Електронно наблюдение на територията на САЩ във връзка с чуждо разузнаване.)

Примерни стандартни основания за електронно наблюдение по ЗНЧР

Заявка за провеждане на електронно наблюдение по ЗНЧР трябва да съдържа:

(1) самоличността на федералния служител, който подава заявката;

(2) самоличността (ако е известна) или описание на конкретния обект на електронно наблюдение;

(3) изложение на фактите и обстоятелствата, на които се основава заявителят в подкрепа на своето убеждение, че:

(А) обектът на електронното наблюдение е чужда държава или агент на чужда държава и

(Б) всички устройства или места, към които е насочено електронното наблюдение, са използвани или предстои да бъдат използвани от чужда държава или агент на чужда държава;

(4) изложение на предложените процедури за свеждане до минимум на щетите;

(5) описание на естеството на търсената информация и типа комуникации и дейности, които ще бъдат обекти на наблюдение;

(6) удостоверение или удостоверения от съветника на президента по въпросите на националната сигурност, висш чиновник от изпълнителната власт или висши чиновници, посочени от президента от онези изпълнителни длъжностни лица, работещи в сферата на националната сигурност или отбраната и назначени от президента по предложение и одобрение на Сената или на заместник-директора на Федералното бюро за разследване, в случай че е посочен от президента като удостоверяващо длъжностно лице –

(А) че удостоверяващото лице смята, че търсената информация е информация от чуждо разузнаване;

(Б) че първостепенно основание на наблюдението е получаването на информация от чуждо разузнаване;

(В) че такава информация не може да се получи посредством обикновени техники за разследване;

(Г) че обозначава типа информация, която се търси според категориите, описани в раздел 101(е), и

(Д) включително изявление за основанието за удостоверяване, че – (а) търсената информация е от типа информация от чуждо разузнаване, който е посочен, и (б) такава информация не може да бъде получена с обикновени техники за разследване;

(7) кратко изложение на средствата, чрез които ще бъде осъществено наблюдението, и изложение дали се налага физическо проникване за осъществяване на наблюдението;

(8) изложение на фактите, свързани с всички предишни заявки, които са били отправени към други съдии по този закон, касаещи всяко едно от лицата, устройства или места, посочени в заявката, и мерките, предприети при всяка предишна заявка, и

(9) изложение за периода от време, през който наблюдението трябва да се провежда, и дали естеството на събиране на разузнавателни данни е такова, че разрешението за използване на електронното наблюдение по този закон не трябва автоматично да се прекъсва, когато описаният тип информация се получи, описание на фактите в подкрепа на убеждението, че впоследствие ще бъде получена допълнителна информация от същия тип. Глава 50, Кодекс на САЩ, параграф 1804(а)(1)-(9).

За да одобри електронно наблюдение по ЗНЧР, Съдът за наблюдение на чуждо разузнаване (СНЧР) трябва освен всичко останало да представи основателно предположение че:

(1) обектът на електронно наблюдение е чужда държава или агент на чужда държава и

(2) всяко устройство или място, към което е насочено електронното наблюдение, е използвано или се очаква да бъде използвано от чужда държава или агент на чужда държава.

При определяне дали съществува основателно предположение, съдията може да вземе под внимание минали действия на обекта.

Времетраене на правомощията

Правомощието на ЗНЧР за електронно наблюдение на американски гражданин не може да надхвърля 90 дни. Глава 50, Кодекс на САЩ, параграф 1805 (g)(1). За да се продължи това правомощие отвъд периода от 90 дни, правителството трябва да получи разрешение от СНЧР посредством пълна заявка до съда за допълнителен период, който не трябва да надвишава 90 дни. За агенти на чужди държави, които не са американски граждани, ЗНЧР може да даде правомощия за електронно наблюдение за срок за 120 дни и до една година след подновяване на заявката. Няма ограничение за броя на

подновяванията, на които заявка по ЗНЧР може да бъде подложена, обаче правителството трябва да продължава да представя пред СНЧР основателни предположения, че обектът е агент на чужда държава и още използва или предстои да използва устройствата, които се наблюдават.

Упълномощаване по спешност

Когато гласува ЗНЧР, Конгресът си дава сметка, че предвид чувствителната към времето оперативна природа на събирането на разузнавателни данни, може да не бъде възможно да се получи съдебна заповед преди започване на електронното наблюдение. В такъв случай ЗНЧР дава право за започване на електронно наблюдение въз основа на положителна резолюция на главния прокурор, както е дефиниран от ЗНЧР, когато главният прокурор „има основание да смята, че съществува извънредна ситуация във връзка с прилагането на електронно наблюдение за получаване на информация от чуждо разузнаване, преди да се получи заповед, упълномощаваща такова наблюдение“, и основателно определя, че съществува фактическа основа за издаване на такава заповед по тази подраздел“, Глава 50, Кодекс на САЩ, параграф 1805 (е)(1)(А) и (Б). Според това постановление главният прокурор може да издаде по спешност пълномощно за период не по-дълъг от седем дни. При такова извънредно упълномощаване СНЧР следва да бъде уведомен, а в срок от седем дни след него трябва да се подаде заявка до съда. Глава 50, Кодекс на САЩ.

Използване и свеждане до минимум на информацията по ЗНЧР

Обикновено СНЧР заседава ex parte, като обектите на претърсване и наблюдение са в неведение относно заявката. Заявките за обиск и наблюдение на ЗНЧР са не само класифицирани, но такова е и самото съществуване на конкретната заявка. Следователно, когато се работи със ЗНЧР или със свързани със ЗНЧР дела, класифицираното им естество трябва да бъде защитено. Нещо повече, използването на ЗНЧР или получена по ЗНЧР информация е обект на процедури по одобрение и ограничаване. Използването или оповестяването на информация, получена или произтичаща от наказателно или ненаказателно производство по ЗНЧР, изисква предварителната санкция от главния прокурор. Такова предварително съгласие е задължително при заседанията на голямото жури, заповеди за обиск, предявяване на обвинение, жалби и други наказателни производства. Изискването за предварително одобрение също така се прилага и при граждански, административни, имигрантски, военни и чуждестранни съдебни процедури.

ЗАПОВЕДИ ЗА ОБИСК ПО ЗНЧР

Дефиниция на физическо претърсване по ЗНЧР

ЗНЧР определя физическото претърсване като: всяко физическо проникване на територията на САЩ в помещения или имот (включително проучване на вътрешността на имота с технически средства), което има за цел залавянето, възпроизводството, проверка или промяна на информация, материал или собственост при обстоятелства, когато лицето има основание да очаква да не бъде обезпокоявано и се изисква заповед за обиск за целите на правоприлагането.

ЗНЧР изключва от определението на физическото претърсване следното: (А) „електронно наблюдение“, както е дефинирано в параграф 1801(f), или (Б) придобиването от страна на правителството на САЩ на информация от чуждо разузнаване от международни или чужди комуникации или дейности на чужди разузнавателни служби, проведени съгласно приложим във всяко друго отношение федерален закон, свързан с чужда система за електронни комуникации, с използване на средства, различни от електронното наблюдение, така както е определено в параграф 1801(f).

Стандарт за основателна причина за физическо претърсване по ЗНЧР

Правото за физическо претърсване по ЗНЧР е обусловено от Глава 50 от Кодекса на САЩ, параграфи 1821-1829. За да упълномощи физическо претърсване по ЗКЧР, СНЧР трябва освен всичко друго да намери основателна причина да смята, че: (1) обектът на физическото претърсване е чужда държава или агент на чужда държава и (2) помещенията или собствеността, която се претърсва, е или предстои да бъде притежавана, ползвана или овладяна или преминава към чужда държава или агент на чужда държава. Глава 50, Кодекс на САЩ, параграфи 1824(а)(2)(А) и (Б).

По-нататък заявката на правителството за физическо претърсване по ЗНЧР трябва да съдържа изложение на факти и обстоятелства, „върху които заявителят основава убеждението си, че (1) обектът на физическо претърсване е чужда държава или агент на чужда държава; (2) помещенията или собствеността, които ще се претърсват, съдържат информация от чуждо разузнаване и (3) помещенията или собствеността, която се претърсва, е или предстои да бъде притежавана, ползвана или овладяна или преминава към или от чужда държава или агент на чужда държава. Глава 50, Кодекс на САЩ, параграф 1824(а)(3)(А) – (В). Заявката трябва също така да бъде придружена от удостоверение от високопоставен правителствен служител поради свързаната с чуждо разузнаване цел на претърсването, подобно на удостоверението, разгледано по-горе за приложенията на електронното наблюдение. Глава 50, Кодекс на САЩ, параграф 1823 (а)(6).

Времетраене на правомощието за физическо претърсване по ЗНЧР

Правомощието на ЗНЧР може да бъде удължено за неамерикански граждани. Периодът на прилагане на ЗНЧР за физическо претърсване на американски граждани не може да надхвърля 90 дни (за периода, необходим за постигане на целите, или 90 дни, което е по-малко). Глава 50, параграф 1824 (d)(1). За да се удължи този период отвъд тези 90 дни, правителството трябва да получи одобрение от СНЧР, като подаде пълна заявка до съда за допълнителен период от време, който не може да надхвърля 90 дни. За агенти на чужда държава, които не са американски граждани, правомощията на ЗНЧР могат да бъдат дадени за период от 120 дни до една година след подновяване на заявката, ако съдията има основателна причина да смята, че собственост на американски гражданин няма да бъде отнета. Обаче дори ако заповедите по ЗНЧР са все още валидни, разследващите агенции трябва да проверят, преди да осъществят обиск, дали обектът все още използва имота или сградата.

Няма ограничение за броя на подновяванията, на които една заявка по ЗНЧР може да бъде подложена, обаче за заявки за физическо претърсване правителството трябва да продължава да поддържа пред СНЧР, че има основателно предположение обектът да е чужда държава или агент на чужда държава, че имотът или сградата, които ще бъдат претърсвани, е или предстои да стане собственост, да бъде използван и притежаван, прехвърлян на или от обекта и че то смята, че там ще бъде намерена информация от чуждо разузнаване.

Упълномощаване по спешност

Спешното упълномощаване на обиск по ЗНЧР е подобно на клаузата за спешното електронно наблюдение, разгледано по-горе. За спешно физическо претърсване правното основание е дадено в Глава 50 от Кодекса на САЩ, параграф 1824(e)(1).

ЗАПОВЕДИ ПО ЗНЧР ЗА ПОДСЛУШВАНЕ И РЕГИСТРАЦИЯ, ПРИХВАЩАНЕ И ПРОСЛЕДЯВАНЕ

Дефиниция на „подслушване и регистрация“ и „устройства за прихващане и проследяване“

Правомощията за подслушване, регистрация, прихващане и проследяване (ПРПП) по ЗНЧР са описани в Глава 50 от Кодекса на САЩ, параграфи 1841-1846. ЗНЧР разчита на традиционни наказателни определения, дадени в Глава 18 на Кодекса на САЩ, параграф 3127, за своите дефиниции за „подслушване и регистрация“ и „прихващане и проследяване“. Според Глава 18 „подслушване и регистрация“ означава: устройство или процес на записване или декодиране на телефонна, маршрутна, адресна или сигнална

информация, предадена от устройство или приспособление, от което се предава телефонна или електронна комуникация, при условие че такава информация няма да включва съдържанието на тази комуникация, но този термин не включва приспособление или процес, който използва доставчик или потребител на телефонна или електронна услуга за фактуриране или счетоводство на разходи и други подобни дейности в нормалния ход на бизнеса. Глава 18, Кодекс на САЩ, параграф 3127(3).

Терминът „прихващане и проследяване“ означава: устройство или процес, което улавя входящите електронни или други импулси, които идентифицират изходящия номер или друга телефонна, маршрутна, адресна и сигнална информация, която може вероятно да идентифицира източника на телефонна или електронна комуникация, при условие обаче такава информация да не включва съдържанието на която и да е комуникация. Глава 18, Кодекс на САЩ, параграф 3127(4). Така че типът наблюдателни дейности, за които може да се получи разрешение по ЗНЧР за подслушване и регистрация и прихващане и проследяване, е същият като в обикновените наказателни дела.

Задължение на правителството да получи правомощие за ПРПП

За да получи правомощия да прилага ПРПП, правителството представя пред СНЧР заявка за заповед, даваща право за инсталирането и използването на ПРПП. Всяка заявка изисква одобрение от главния прокурор или определен от правителството прокурор и трябва да включва удостоверение от страна на заявителя, че информацията, която се очаква да се получи, е или: (1) информация от чуждо разузнаване, която не засяга гражданин на САЩ, или (2) има отношение към текущо следствие за защита срещу международен тероризъм или подривни разузнавателни дейности, при условие че такова разследване на гражданин на САЩ не се провежда единствено въз основа на дейности, защитени от Първата поправка на Конституцията. Глава 50, Кодекс на САЩ, параграф 1842 (c)(2). Този език задава по-висок стандарт за заявки, които търсят информация, засягаща гражданин на САЩ, а именно че целта трябва да бъде защита срещу международен тероризъм или подривни разузнавателни дейности (а не просто получаване на информация от чуждо разузнаване) и че предприетото разследване не се води само въз основа на дейности, защитени от Първата поправка. Глава 50, Кодекс на САЩ, параграф 1842(a)(1). Съдията ще издаде заповед за ПРПП, след като се увери, че заявката от правителството отговаря на изискванията на Глава 50, Кодекс на САЩ, параграф 1842.

Времетраене на разрешителното за ПРПП по ЗНЧР

Заповеди за ПРПП по ЗНЧР, насочени срещу гражданин на САЩ, не могат да надхвърлят период от 90 дни, но могат да бъдат подновени за последващ 90-дневен срок след покриване на същите изисквания, както при първоначалната заявка. Глава 50, Кодекс на САЩ.

Упълномощаване по спешност

Както и при електронното наблюдение и физическия обиск, ЗНЧР дава право на главния прокурор да разреши по спешност прилагане на ПРПП за срок, който не надхвърля седем дни, когато извънредна ситуация налага поставянето и използването на ПРПП и съществува фактическа основа за издаването на заповед. Глава 50, Кодекс на САЩ, параграф 1843. СНЧР трябва да бъде уведомен за такава заповед по спешност и до съда трябва да бъде подадена заявка в срок до седем дни след издаването на заповедта.

ЗАПОВЕДИ ПО ЗНЧР ЗА БИЗНЕС ДОКУМЕНТАЦИЯ

Дефиниция на бизнес документация

Раздел 1861 от ЗНЧР дава право на правителството да поиска съдебна заповед, за да изземе материални вещи, като например писмени документи, в хода на разследването. Глава 50, Кодекс на САЩ, параграфи 1861-1862. Законът отбелязва, че материални вещи включват „счетоводни книги, протоколи, документи и други вещи", параграф 1861(a)(1). Заповед за бизнес документация може да изисква предоставянето на вещ само в случай, че тази вещ може да бъде получена с призовка, издадена от съд в САЩ в подкрепа на разследване на голямото жури, или със заповед, издадена от американски съд, изискваща предоставянето на документи или вещи. Глава 50, Кодекс на САЩ, параграф 1861(c)(2)(D)

Стандарт за получаване на бизнес документация

Заявката на правителството за получаване на заповеди за бизнес документация трябва да покаже, че има основание да се смята, че търсените материални вещи имат връзка с разрешено разследване (в това не се включва потвърждаване на заплаха). Разследването трябва да се провежда според насоките, одобрени от главния прокурор в Изпълнителна заповед 123333, или последваща заповед. Глава 50, Кодекс на САЩ, параграф 1861(a)(2)(A). Изискванията за доказване на връзка са още по-големи, когато става въпрос за разследване, което се води срещу американски гражданин. За да получи съдебно разрешение, правителството трябва да покаже, че проверява бизнес документацията във връзка с текущото разследване:

(1) за да получи информация от чуждо разузнаване, което не засяга американски гражданин, или

(2) за да окаже защита срещу международен тероризъм или подривни разузнавателни дейности, като тези вещи се предполага, че имат връзка с официално разследване, ако заявителят покаже в изложението на фактите, че те принадлежат на (a) на чужда държава или агент на чужда държава; (б) свързани са с действията на агент на чужда държава, който е обект

на официалното разследване, или (B) с индивид, който е в контакт или е познат на заподозрян агент на чужда държава, който е обект на такова официално разследване. Глава 50, Кодекс на САЩ, параграф 1861 (b)(2)(A)

Получаване на електронно доказателство по Закона за поверителност на електронната комуникация

Почти във всяко разследване, свързано с националната сигурност, прокурори и следователи искат да получат електронно доказателство, било то под формата на преди време изпратени или получени имейли, телефонни номера, информация за сайтове или някаква друга улика, оставена от обекта на разследването. Освен разузнавателните средства, разгледани по-горе, Законът за поверителност на електронната комуникация също така създава правна основа, в рамките на която прокурори и следователи могат да получат електронно доказателство.

В ограничен брой обстоятелства, свързани с непосредствена заплаха, доставчиците на услугата могат доброволно да предоставят информация на правоприлагащия орган. Според Глава 18 от Кодекса на САЩ, параграф 2702, доставчик на електронни услуги може доброволно да разсекрети съдържателна и несъдържателна информация на правоприлагащия орган, ако доставчикът на услуги вярва, че е налице извънредна ситуация, свързана с опасност от смърт или сериозно физическо нараняване на човек, която изисква незабавно разсекретяване на информация, свързана с извънредната ситуация. Глава 18, Кодекс на САЩ, параграф 2702 (b)(8).

Ограничения

Правоприлагаща агенция може да подаде молба за доброволно разсекретяване по този параграф, обаче не може да изисква такова разсекретяване. Доставчикът на услугата трябва да вярва, че разсекретената информация е свързана с извънредна ситуация, със смърт или сериозно физическо увреждане.

Процес

Доставчикът на услугата ще предаде информация или съдържанието на комуникацията посредством своите процеси или процедури, въпреки че правоприлагащите органи могат да поискат да използват формуляр за доброволен иск със специфична информация във връзка с извънредната ситуация. Всяка година главният прокурор е длъжен да отчита пред Конгреса броя на доброволните разсекретявания, направени под раздел (b)(8), и какво се случва с разследването по всеки отделен случай. Информацията за разсекретявания обикновено се събира за всяка федерална правоприлагаща агенция и след това се обединява от Бюрото за законодателство и политика на Службата за национална сигурност в координация с Бюрото по законодателни въпроси.

Федерални закони за поверителност

Обикновено хората не хранят разумни очаквания личната за тях информация да бъде пазена като поверителна от трети страни. Това означава, че правоприлагащите органи могат да получат тази информация без съдебно дело, което означава без заповед за обиск или призовка от голямото жури. Въпреки това обаче в определени области Конгресът е приел закони, че такива данни трябва да бъдат поверителни, като по такъв начин създава задължително очакване за поверителност на определени данни, съхранявани от трети страни.

Освен данните, защитени по Закона за поверителност на електронната комуникация, други категории данни, които имат федерална защита за поверителност, са:

- Банкови данни (Закон за правото на финансова поверителност от 1978)
- Медицински данни (Закон за здравното осигуряване и отчетност от 1996)
- Образователни данни (Закон за семейните образователни права и поверителност от 1974)
- Данъчни сведения (Глава 26, Кодекс на САЩ, параграф 6103)
- Данни от Отдела за моторни превозни средства (Закон за защита поверителността на водача от 1994)
- Данни за наем на видеокасети (Закон за защита поверителността на видео потреблението от 1988).

Получаване на доказателства от чуждестранни партньори

При много разследвания, свързани с националната сигурност, прокурорите и следователите се налага да потърсят помощ от партньорите си в друга страна. Службата за международно сътрудничество (СМС) е безценен източник на сведения по безброй международни въпроси и трябва да бъде потърсена за консултация, когато става въпрос за получаване на информация от чуждестранни партньори при разследвания с международен елемент. Юристите както от Отдела за борба срещу тероризма, така и от Отдела за контраразузнаване поддържат текущи работни отношения със своите чуждестранни партньори и могат да служат за свръзка за получаване на помощ от чужбина. Програмата „Правен аташе“ на ФБР и правните съветници от Службата за професионално развитие и обучение в чужбина на Департамента по правосъдие изграждат стабилни връзки с прокурори от много страни и съвместно със СМС могат да улеснят получаването на помощ в много случаи. Този раздел прави кратък преглед на различните способи, с които разполагат прокурорите, за да потърсят

помощ от чужди държави. Посредством заявки по Спогодбата за взаимна правна помощ (СВПП), съдебни поръчки и искови писма прокурорите могат да получат разнообразна помощ от чуждестранни партньори. При всички случаи, когато се търсят доказателства от друга страна по въпроси на националната сигурност, вероятността за успех ще се увеличава при провеждане на предварителни консултации с представители на Службата за международно сътрудничество, Отдела за борба срещу тероризма и Отдела за контраразузнаване.

Съдебни поръчки

Съдебните поръчки са традиционни механизми, с които се иска помощ от чужда суверенна държава във връзка със съдебно следствие, което се води в страната, направила поръчката. Това са молби от съда или съдията от една страна (обикновено разследващия магистрат) до съда или съдия от друга страна. Те могат да се използват както в граждански, така и в наказателни дела. Помощта, произтичаща от съдебните поръчки, зависи от отношенията между съдилищата и се дава по усмотрение. Предвид разгледаните по-долу алтернативи, американските висши чиновници рядко търсят помощ при наказателни дела чрез съдебни поръчки.

Искови писма

Исковите писма, както съдебните поръчки, се основават на добрите взаимоотношения. Обикновено те произтичат от изпълнителен орган вместо от разследващи магистрати или съдилища. Във всеки случай, за да се издаде исково писмо, трябва да се потърси образец на страницата за страната на СМС и да се работи със специалиста по страната на СМС.

Споразумение за взаимна правна помощ (СВПП)

Докато процедурата на съдебните заявки може да бъде тежка и силно формализирана, СВПП предоставя по-целенасочени средства за получаване на доказателства от чужбина. Тъй като всяко СВПП е различно в зависимост от това как това споразумение е било договорено между САЩ и съответната страна, важно е да се потърси образец на страницата за съответната страна на СМС и да се работи със специалиста по страната на СМС, за да се издаде молба по СВПП от СМС.

ПРЕТЪРСВАНИЯ И ИЗЗЕМВАНИЯ НА ГРАНИЦАТА

Правен орган

Редица закони и наредби са приложими в контекста на претърсването и изземването на границата. Като общо правило три агенции на САЩ – за митническа и гранична защита (МГЗ), имиграционни и митнически власти

(ИМВ) и Бреговата охрана – имат служители и агенти, които са упълномощени по статут да провеждат претърсвания и изземвания на границата.

Обмен на информация

Обикновено информация и доказателства за лица и стоки, иззети законно от МГЗ или ИМВ според митническите или имиграционни закони по време на претърсване на границата, може законно да бъдат споделяни с други агенции, включително ФБР, с цел да се провери дали информацията се отнася до прилагането на митнически или имиграционни закони, или дали останалите агенции имат независимо основание в закона да получат и да задържат информацията. Политиките на МГЗ и ИМВ изрично упълномощават служителите на МГЗ да споделят информация, получена по време на законно претърсване на границата, както е позволено и се изисква от закона и политиката. В случай когато МГЗ или ИМВ споделя информация, свързана с молба за помощ, политиките и на двете агенции съветват приемащата федерална агенция, че правото ѝ да задържи информацията или доказателството е ограничено, докато другата агенция има независимо законно право да го направи (например когато информацията има стойност за националната сигурност или разузнаването). В такива случаи агенцията, която задържа информация, трябва да уведоми МГЗ за това свое решение.

5. КОДЕКС НА САЩ

Заговор на територията на САЩ за убийство, отвличане или осакатяване на лица или за увреждане на собственост в чужбина – Глава 18, Кодекс на САЩ, параграф 956

Глава 18 от Кодекса на САЩ, параграф 956 инкриминира заговорите за упражняване на насилие срещу лица или собственост в чужбина. Конкретно този закон забранява конспирация на територията на САЩ за осъществяване на каквито и да било действия извън САЩ като убийство, отвличане или осакатяване, извършена под юрисдикцията на САЩ, доколкото един открит акт на този заговор се провежда на територията на САЩ. Глава 18, Кодекс на САЩ, параграф 956(a)(1). Тя също така забранява заговори на територията на САЩ за унищожаването на собственост на територията на чужда държава и притежавана от чуждо правителство, с което САЩ е в мирни отношения, или железопътна линия, канал, мост, летище или друга публична собственост, публичен превоз или публична структура, или религиозна образователна или културна собственост. Глава 18, Кодекс на САЩ, параграф 956(b). Федералното законодателство е приложимо към такова престъпление, ако част от заговора и открит акт от неговото осъществяване се извърши на територията на САЩ. Виж Глава 18, Кодекс на САЩ, параграф 956(a)(1). Престъплението се наказва с доживотен затвор, ако целта на заговора е убийство или отвличане; с до 35 години

затвор, ако целта на заговора е осакатяване; и до 25 години затвор, ако целта е повреждането на някаква собственост.

Престъпления срещу международно защитени лица – Глава 18, Кодекс на САЩ, параграфи 112, 878, 1116, 1201(a)(4)

Глава 18 изрично инкриминира редица действия, насочени срещу международно защитени лица. Международно защитено лице е държавен глава или политическият му еквивалент, правителственият ръководител или министърът на външните работи, когато такова лице е извън своята държава, както и всеки член на семейството му, който го придружава; или всеки друг представител, чиновник или служител на правителството на САЩ, на чуждо правителство или на международна организация, който във въпросното време и място има право според международното законодателство на специална защита срещу атаки, насочени срещу неговата личност, свобода или достойнство, както и срещу всеки член на семейството му.

Други висши чуждестранни служители също попадат под защитата на този закон. Глава 18 от Кодекса на САЩ, параграф 112, забранява извършването на нападение и други насилствени действия срещу международно защитени лица. Конкретно тя забранява нападение, нараняване, затваряне или насилие над висш служител на чужда държава; нападение на офиса, квартирата или колата на чуждестранния служител; сплашването, заплахите, принудата или тормоза над чуждестранен служител и възпрепятстването на чуждестранния служител да изпълнява задълженията си. Глава 18, Кодекс на САЩ, параграф 112(a), (b). Наказуеми са също така и опити да се осъществят тези действия. Тези престъпления са наказуеми, ако се осъществят на територията на САЩ. Законодателството се прилага и когато международно защитеното лице е извън САЩ, но жертвата е представител, служител или чиновник на САЩ, ако извършителят е американски гражданин или ако извършителят впоследствие бъде открит на територията на САЩ. Глава 18, Кодекс на САЩ, параграф 112(e). Престъплението се наказва с до десет години затвор. Глава 18, Кодекс на САЩ, параграф 112(a).

Глава 18 от Кодекса на САЩ, параграф 1116 забранява убийство, непредумишлено убийство или опит за убийство на международно защитено лице. Глава 18 от Кодекса на САЩ, параграф 1201(a)(4) забранява отвличането на международно защитени лица. И двата закона се прилагат при такова престъпление, ако то се извърши на територията на САЩ или ако се извърши извън пределите на САЩ, ако жертвата е официален представител, служител или чиновник на САЩ, ако извършителят е гражданин на САЩ или ако извършителят впоследствие бъде открит в САЩ. Глава 18, Кодекс на САЩ, параграф 116(c); параграф 1201(e). Опит за убийство или отвличане, завършило със смърт, може да получи смъртна присъда, Глава 18, Кодекс на САЩ, параграф 1201(a). Глава 18 от Кодекса на САЩ, параграф 878 забранява заплахите за извършване на гореизброените престъп-

ления или принудата във връзка с всяко от гореизброените престъпления. Нарушаването на параграфи 112, 1116 и 1201 е наказуемо със затвор до пет години освен заплахата за нападение, която не може да бъде наказана с повече от три години затвор. Глава 18, Кодекс на САЩ, параграф 878(a). Нарушение на закона, свързано с изнудване, може да бъде наказано с до 20 години затвор. Глава 18, Кодекс на САЩ, параграф 878(b).

Наркотероризъм – Глава 21, Кодекс на САЩ, параграф 960a

Глава 21 от Кодекса на САЩ, параграф 960a забранява производството и разпространението на контролирани вещества, когато е налице намерение да се прехвърли каквато и да е материална стойност на лице или организация, свързани с терористични дейности. Наказанието за нарушаването на този закон може да достигне доживотен затвор, като минималното наказание не може да бъде по-малко от два пъти минималното наказание, предвидено в Глава 21, Кодекс на САЩ, параграф 841(b)(1).

За да бъде признат за виновен в наркотероризъм в нарушение на параграф 960a обвиняемият, правителството трябва да докаже, че:

1. Обвиняемият съзнателно или преднамерено е възприел, опитал се е да възприеме или е заговорничил да възприеме поведение, наказуемо според Глава 21 от Кодекса на САЩ, параграф 841(a), ако е осъществено на територията на САЩ;
2. Обвиняемият е постъпил така съзнателно или е възнамерявал да предостави директно или опосредствано каквото и да е с материална стойност (според дефиницията в Глава 18, Кодекс на САЩ, параграф 1958(b)(1)) на лице или организация, занимаващи се с терористични дейности (според дефиницията в Глава 8, Кодекс на САЩ, параграф 1182(a)(3)(B)) и тероризъм;
3. Лицето или организацията се е занимавала или се занимава с терористична дейност (както е дефинирана в Глава 8, Кодекс на САЩ, параграф 1182(a)(3)(B)) или с тероризъм (както е дефиниран в Глава 22, Кодекс на САЩ, параграф 2656f(d)(2));
4. Обвиняемият знае, че въпросното лице или организация се е занимавала или се занимава с терористична дейност (както е дефинирана в Глава 8, Кодекс на САЩ, параграф 1182(a)(3)(B)) или с тероризъм (както е дефиниран в Глава 22, Кодекс на САЩ, параграф 2656f(d)(2)) и
5. Юрисдикцията на държавата е правова.

Убийства, извършени по време на нападение над федерално съоръжение – Глава 18, Кодекс на САЩ, параграф 930(c)

Глава 18 от Кодекса на САЩ, параграф 930(c) забранява убийства по време на нападение на федерално съоръжение или убийства, предизвикани

от незаконно притежаване на огнестрелно оръжие или други опасни оръжия във федерални съоръжения. Глава 18, Кодекс на САЩ, параграф 930(g)(1).

В закона „федерално съоръжение" се определя като сграда или част от сграда, притежавана или наета от федералното правителство, където непрекъснато присъстват федерални чиновници, които изпълняват служебните си задължения. Глава 18, Кодекс на САЩ, параграф 930(g)(1).

Присъдите под параграф 930(c) са разгледани по-подробно в параграфи 1111, 1112, 1113 и 1117 в зависимост от естеството на извършеното престъпление. Убийство първа степен според параграф 1111 се наказва със смърт или доживотен затвор. Глава 18, Кодекс на САЩ, параграф 1111(b). Убийство от втора степен според параграф 1111 се наказва най-много с доживотен затвор. Непредумишленото убийство според параграф 1112 се наказва с най-много 15 години затвор за доброволно непредумишлено убийство и с не повече от 8 години затвор за неволно непредумишлено убийство. Глава 18, Кодекс на САЩ, параграф 1112(b). Според параграф 1113 всеки опит за убийство се наказва с до 20 години затвор, а всеки опит за непредумишлено убийство се наказва с не повече от 7 години затвор. Накрая, всеки заговор за извършване на убийство се наказва най-много с доживотен затвор. Глава 18, Кодекс на САЩ, параграф 1117.

Неверни показания – Глава 18, Кодекс на САЩ, параграф 1001

Глава 18 от Кодекса на САЩ, параграф 1001 инкриминира даването на неверни показания пред правителството. За да бъде осъден нарушителят, трябва по някакъв въпрос от юрисдикцията на изпълнителната, законодателната или съдебната власт на САЩ: (а) да фалшифицира, скрие или прикрие чрез измама, схема или устройство материален факт; (б) да даде невярно, измислено или подвеждащо показание или представяне или (в) да направи или използва фалшив писмен документ, като знае, че той съдържа каквото и да е материално невярно, измислено или подвеждащо показание или вписване. Глава 18, Кодекс на САЩ, параграф 1001(а).

Този традиционен наказателен закон често се използва при дела, свързани с националната сигурност. Законът за реформа в разузнаването и превенция на тероризма, приет на 17 декември 2004 г., дава право за налагане на по-големи наказания за нарушаване на този закон, когато е налице връзка с вътрешен или международен тероризъм. (Терминът „международен тероризъм" е дефиниран в Глава 18, Кодекс на САЩ, параграф 2331.) Законът за реформа в разузнаването и превенция на тероризма увеличава максималното наказание по този закон от пет на осем години, ако престъплението е свързано с вътрешен или международен тероризъм.

Защита на компютри – Глава 18, Кодекс на САЩ, параграф 1030

Глава 18 от Кодекса на САЩ, параграф 1030 инкриминира редица престъпления, свързани с непозволен достъп или използване на компютри. Наказуемото поведение включва:

1. Предаване на защитена информация на лица, които нямат право да я получат, след неразрешен достъп до компютър с намерението информацията да бъде използвана в ущърб на САЩ или в полза на чуждо правителство;
2. Проникване в компютър без разрешение с цел получаване на финансови или потребителски документи или документи на министерство или агенция на САЩ;
3. Преднамерено влизане в държавен компютър без разрешение;
4. Проникване в защитен компютър с цел измама;
5. Повреждане на защитен компютър без разрешително;
6. Търговия с компютърни пароли (или подобна информация) с цел измама;
7. Заплаха за повреда или незаконно проникване в защитен компютър с цел изнудване.

В контекста на този закон защитен компютър е този, който принадлежи на финансова институция или на правителството на САЩ и се използва или има значение за междущатската търговия или комуникация. Издаването на присъда по параграф 1030 изисква много специфични факти и той трябва да бъде прилаган внимателно.

Невярна информация и измами – Глава 18, Кодекс на САЩ, параграф 1038

След атентатите от 11 септември и нападенията с антракс правоприлагащите органи бяха засипани от неверни сигнали за свързани с тероризъм престъпления. След няколкогодишните законодателни усилия на Департамента по правосъдие на 17 декември 2004 г. Конгресът гласува федерален закон. Параграф 1038 предвижда в съответната част, че дадено лице е виновно за измама, ако той или тя предприеме каквито и да е действия с цел да подаде фалшива или подвеждаща информация при обстоятелства, при които тази информация може да изглежда правдоподобно и където тази информация показва, че се е осъществило, осъществява се или предстои да се осъществи дадено действие, представляващо нарушение (различни предикатни престъпления).

За да се установи нарушение на Глава 18, Кодекс на САЩ, параграф 1038, правителството трябва да докаже три елемента: (1) че ответникът е предприел действия с намерение да предаде невярна или подвеждаща информация; (2) при обстоятелства, при които такава информация изглежда

достоверна; (3) и е свързана с дейност, която е нарушение на предикатно престъпление.

Предикатните престъпления включват редица престъпления, свързани с тероризма, включително такива, отнасящи се до унищожаване на самолети или моторни превозни средства; престъпления, свързани с химически, биологични, атомни и радиоактивни вещества, оръжия и съоръжения; престъпления, свързани с експлозиви и огнестрелни оръжия; престъпления, свързани с тероризъм; въздушно пиратство и нападение и възпрепятстване на самолетен екипаж и други.

Незаконни парични преводи —Глава 18, Кодекс на САЩ, параграф 1960

Преди атентатите от 11 септември Глава 18 от Кодекса на САЩ, параграф 1960 инкриминираше извършването на парични трансфери от фирми без щатски лиценз. PATRIOT Act на САЩ промени закона от специфично насочено престъпление към такова от общ характер, като прибави и изискване за федерална регистрация. Старата версия на параграф 1960, озаглавена „Забрана на нелицензирани фирми за извършване на парични трансфери“, гласеше:

(а) Който провежда, контролира, управлява, наблюдава, насочва или притежава целия или част от бизнес, за който знае, че това е бизнес за нелегално прехвърляне на пари, ще бъде глобен съгласно този параграф или ще лежи в затвора за срок до пет години, или и двете.

(б) Използван в този параграф – (1) терминът „бизнес за незаконен трансфер на пари“ означава бизнес за прехвърляне на парични средства, който влияе върху междущатската или външната търговия по какъвто и да е начин и в каквато и да е степен и – (а) преднамерено се осъществява без съответния лиценз за извършване на паричен трансфер в щат, където такава операция е наказуема като дребно или углавно престъпление според законите на щата, или (б) не съответства на изискванията за регистрация на бизнес, свързан с парични преводи според параграф 5330 на Глава 31 на Кодекса на САЩ, или регулациите, предписани в този параграф. Глава 18, Кодекс на САЩ, параграф 1960 (2000) (поправен през 2001).

По старата версия на статута бяха възбудени няколко дела и бяха написани становища, всички те в Ню Йорк.

Сегашната версия от параграф 1960 (заглавието е непроменено) гласи:

(а) който провежда, контролира, управлява, наблюдава, насочва или притежава целия или част от бизнес, за който знае, че това е бизнес за нелегално прехвърляне на пари, ще бъде глобен съгласно този параграф или ще лежи в затвора за срок до пет години, или и двете.

(б) както е използван в този параграф – (1) терминът „бизнес за незаконен трансфер на пари“ означава бизнес за прехвърляне на парични средства,

който влияе върху междущатската или външната търговия по какъвто и да е начин и в каквато и да е степен и – (а) преднамерено се осъществява без съответния лиценз за извършване на паричен трансфер в щат, където такава операция е наказуема като дребно или углавно престъпление според законите на щата, независимо от това дали ответникът е знаел или не, че операцията задължително е трябвало да бъде лицензирана или че извършена по такъв начин, е наказуема; (б) не съответства на изискванията за извършване на парични трансфери според параграф 5330 на Глава 31 от Кодекса на САЩ или регулациите, заложени в този параграф, или (в) е свързан с пренасянето или прехвърлянето на средства, за които ответникът знае, че са получени в резултат на извършено престъпление или са предназначени да бъдат използвани за осъществяване на или в подкрепа на престъпна дейност. Глава 18, Кодекс на САЩ, параграф 1960.

Предназначението на поправките е да премахне потенциалната възможност за положителна защита въз основа на това, че ответникът не е знаел за приложими щатски изисквания за лицензиране. Поправките в PATRIOT Act го превръщат в по-ефективно оръдие на прокуратурата.

Терористични атаки в чужбина срещу американски граждани – Глава 18, Кодекс на САЩ, параграф 2332

Глава 18 от Кодекса на САЩ, параграф 2332 инкриминира убийството, умишленото убийство и заговор за извършване на убийство срещу граждани на САЩ извън пределите на страната. По-нататък в нея се инкриминира физическото насилие извън територията на САЩ с намерението да се нанесе сериозна телесна повреда на американец или когато такава сериозна телесна повреда е нанесена на американец. Глава 18, Кодекс на САЩ, параграф 2332(c). Ако престъплението е убийство, както е дефинирано в параграф 1111(а), за него може да се иска смъртно наказание, но иначе е наказуемо с доживотен затвор. Глава 18, Кодекс на САЩ, параграф 2332(а)(1). Ако престъплението е доброволно непредумишлено убийство, както е дефинирано в параграф 1112(а), максималната присъда е десет години затвор. Глава 18, Кодекс на САЩ, параграф 2332(а)(2). Ако престъплението е неволно непредумишлено убийство, максималната присъда е три години затвор. Глава 18, Кодекс на САЩ, параграф 2332(а)(3). Опит за убийство може да получи присъда до 20 години затвор, а заговор по този параграф е наказуем с доживотен затвор. Глава 18, Кодекс на САЩ, параграф 2332(b).

Глава 18 от Кодекса на САЩ, параграф 2332(d), задава ограничение върху преследването на убийството на или насилието върху американски граждани в чужбина. Престъплението може да бъде преследвано само ако главният прокурор или упълномощено от него лице потвърди убеждението си, че престъплението е имало за цел „да принуди, сплаши или накаже правителство или цивилно население“. Критериите за потвърждението са представени в алтернативата; актът трябва или да е „замислен да принуди, сплаши или накаже правителство“, или да е „замислен да принуди, сплаши

или накаже… цивилно население“. Законодателната история на тази клауза показва, че целта на Конгреса е била да предостави на съда извънтериториална компетентност върху атаки на терористи срещу американски граждани и да изключи несвързаното с тероризъм насилие.

Тероризъм, преминаващ националните граници – Глава 18, Кодекс на САЩ, параграф 2332b

Глава 18 от Кодекса на САЩ, параграф 2332b поставя извън закона убийството, осакатяването или нападението на хора на територията на САЩ или създаването на значителен риск от сериозна телесна повреда на дадено лице чрез унищожаването, повреждането или опит да се унищожи или повреди собственост в САЩ, ако действията на нарушителя преминават националните граници. Освен това наказателно преследване по закона изисква престъплението да отговаря поне на едно от правните изисквания, включително, но не само: (1) да е извършено при използването на пощата или друг инструмент на междущатската или външната търговия; (2) жертвата или потенциалната жертва да е униформен служител или висш чиновник, длъжностно лице, служител или агент на законодателната, изпълнителната или съдебната власт или министерство или агенция на САЩ; (3) престъплението е извършено в рамките на териториалната или морската юрисдикция на САЩ.

Поставяне на бомби на обществени места, правителствени съоръжения, системи за обществен транспорт и инфраструктура – Глава 18, Кодекс на САЩ, параграф 2332f

Глава 18 от Кодекса на САЩ, параграф 2332f забранява поставянето, разтоварването или взривяването на избухващо устройство на места за обществено ползване, щатско или правителствено съоръжение, система за обществен транспорт или инфраструктура с цел причиняване на смърт или тежка телесна повреда или увреждане на структурата. Редица правни основания са изброени в параграф 2332f(b).

Ракетни системи, предназначени за унищожение на самолет – Глава 18, Кодекс на САЩ, параграф 2332g

Глава 18 от Кодекса на САЩ, параграф 2332g забранява да се произвежда, създава, прехвърля, използва или да се притежава и да се заплашва да се използва експлозив или взривно устройство или ракета, които са направлявани от система, с намерението да се насочи ракетата към самолет. Съществува изключение за американски служители и предприемачи, които работят за правителството, и за устройства, които не са създадени да бъдат използвани като оръжие. Такова престъпление се наказва с минимум 25 до 30 години затвор в зависимост от материала, който е използван, и с

максимум доживотен затвор. Ако престъплението доведе до смърт, доживотната присъда е задължителна.

Укриване на терористи – Глава 18, Кодекс на САЩ, параграф 2339

Глава 18 от Кодекса на САЩ, параграф 2339 забранява приютяването или укриването на лице, за което нарушителят знае, че е извършило едно или няколко от изброените терористични престъпления. Това се наказва с до 10 години затвор. Глава 18, Кодекс на САЩ, параграф 2339(а).

Престъпления, свързани с материална подкрепа – Глава 18, Кодекс на САЩ, параграфи 2339А и 2339В

Наказателното преследване по тези две наредби е сложно по същество и изисква тясна координация със Сектора за борба срещу тероризма (СБТ). Освен това Отделът за национална сигурност (ОНС) може да окаже подкрепа относно приложимите закони и помощ за написване на подходящ обвинителен акт в светлината на поправките, внесени от Конгреса, и на съдебните тълкувания на забраната за материална подкрепа.

Раздел 2339А, приет през 1994 г., гласи:

Онзи, който предоставя материална подкрепа или ресурси или скрива или прикрива естеството, местонахождението, източника или собствеността на материална подкрепа или ресурси, след като знае или подозира, че те ще бъдат използвани за подготовката или за извършването на престъпление (терористичен акт) или за подготовката или за осъществяването на прикриване от комисията на такова нарушение или се опитва или заговорничи да осъществи такъв акт, следва да заплати глоба по този състав, да лежи в затвора за срок не повече от 15 години или и двете, а при смъртен случай в резултат на всичко това трябва да бъде затворен за какъвто и да е период от време или доживот.

Ключов момент в наказателното преследване по параграф 2339А е, че правителството трябва да докаже, че обвиняемият е възнамерявал материалната подкрепа да бъде използвана за извършването или подготовката на едно от предикатните престъпления. За разлика от нарушение по параграф 2339В, не е необходимо получателят на материалната подкрепа да бъде определена чуждестранна терористична организация, за да се приложи параграф 2339А.

Докато параграф 2339А забранява оказването на материална помощ за терористична дейност, когато се знае или се подозира, че помощта ще бъде използвана за подготовката или извършването на терористична дейност, параграф 2339В забранява съзнателно да се предоставя материална помощ на чуждестранна терористична организация. „Материална помощ или ресурси по смисъла и на двете наредби е дефинирана така, че да включва: имущество, материално или нематериално, или услуга, включително

парични или финансови инструменти или финансови ценни книжа, финансови услуги, подслоняване, обучение, експертен съвет или помощ, тайни квартири, фалшиви документи или лични карти, приспособления за комуникации, устройства, оръжия, смъртоносни вещества, експлозиви, персонал и транспорт, с изключение на лекарства и религиозни материали. Глава 18, Кодекс на САЩ, параграф 2339A(b)(1).

В наказателните производства по параграф 2339B правителството трябва само да докаже, че обвиняемият съзнателно е оказвал материална помощ и че организацията отговоря на известни предварително поставени условия; няма допълнително изискване обвиняемият да е знаел, че нарушава закона. Затова с цел да не се вменява на правителството по-висока степен на доказателствената тежест се препоръчва терминът „доброволно“ да бъде премахнат от обвинителните актове по параграф 2339B. Накрая трябва да се отбележи, че описанието на откритите действия не се изисква в обвинителния акт за конспирация по параграф 2339B, въпреки че може би е желателно да се опишат действия, подкрепящи конспирацията. Въпреки това прокурорът трябва да включи открити действия, ако повдига обвинение в конспирация по параграф 371.

Забрана за финансиране на тероризъм – Глава 18, Кодекс на САЩ, параграф 2339C

Глава 18 от Кодекса на САЩ, параграф 2339C забранява както събирането, така и предоставянето на средства с намерението тези средства да бъдат използвани за осъществяването на терористична атака. Това бе прието, за да се гарантира, че законодателството на САЩ е в съответствие с Конвенцията на ООН за борба с финансирането на тероризма. Тъй като наредбата бе използвана само няколко пъти, прокурорите трябва да работят в тясна координация със СБТ, преди да повдигнат обвинение по параграф 2339C. Нарушение на параграф 2339C може да доведе до лишаване от свобода за срок до 20 години. Глава 18, Кодекс на САЩ, параграф 2339C(d).

Получаване на военно обучение от чуждестранна терористична организация – Глава 18, Кодекс на САЩ, параграф 2339D

През декември 2004 година Конгресът обнародва Глава 18 от Кодекса на САЩ, параграф 2339D, която забранява съзнателното получаване на военно обучение от или вместо всяка определена за терористична чуждестранна организация.

Терминът „военно обучение“ включва обучение в начини и методи, които могат да причинят смърт или тежки телесни наранявания, да разрушат или повредят имущество, да разстроят обслужването на критична инфраструктура, или обучение за използване, съхранение, производство или сглобяване на какъвто и да е експлозив, огнестрелно оръжие или

друго оръжие, включително всяко оръжие за масово поразяване (според дефиницията на Глава 18 от Кодекса на САЩ, параграф 2232a(c)(2)). Глава 18, Кодекс на САЩ, параграф 2339D(c).

Значението на термина „тежко телесно нараняване“ е дадено в параграф 1365(h)(3).

Терминът „критична инфраструктура“ означава системи и активи, жизненоважни за националната отбрана, националната сигурност, икономическата сигурност и общественото здравеопазване и безопасност, включващ както регионалната, така и националната инфраструктура.

Критичната инфраструктура може да бъде публична или частна собственост. Примери за критична инфраструктура включват производството на нефт и газ, съхранение и системи за доставка, финансовата и банковата система, службите за бърза помощ (включително медицински, полицейски, пожарни и спасителни служби) и транспортни системи и услуги (включително магистрали, шосета, авиокомпании и летища)

Трябва да се отбележи, че има известно припокриване между параграф 2339D и клаузите, свързани с конспирация, на параграф 2339B: човек, който получава някакво военно обучение, по необходимост е предприел положително или явно действие, като е предоставил материална подкрепа на организацията, която спонсорира обучението – персонал в свое лице. Престъплението се наказва задължително с десет години затвор. Глава 18, Кодекс на САЩ, параграф 2339D(a).

6. ПРОБЛЕМИ, СВЪРЗАНИ С ПРЕДВАРИТЕЛНОТО СЛЕДСТВИЕ И РАЗКРИВАНЕТО

Класифицирана информация

Специфични проблеми с разкриването могат да възникнат при разследвания, свързани с националната сигурност, защото информацията в такова разследване обикновено е класифицирана. Класифицираната информация е обект на същите правила за разкриване, както некласифицираната. Прокурорът трябва да бъде запознат с класифицираната информация или разкриване на класифицирана информация, свързани с разследването. При положение че прокурорът има надлежното разрешение за достъп до секретни материали, на него или на нея трябва да бъде осигурен достъп до всички важни за делото преписки и до други преписки, съдържащи потенциално чувствителна информация за всички правоприлагащи агенции на Департамента по правосъдие. Прокурорите трябва да имат достъп и до преписките, поддържани от правоприлагащи агенции извън ДП като щатски и местни правоприлагащи агенции. Прокурорът може или сам да прегледа

преписките, или да поиска те да бъдат разгледани от следователите по случая. Протоколите за всеки свидетел (независимо дали е определен като класифициран свидетел или поверителен източник) трябва винаги да бъдат преглеждани за евентуално чувствителна информация, включително потенциална информация за импийчмънт.

Освен че прокурорът лично проверява преписките, той трябва винаги да пита водещия по делото следовател каква информация има и дали може да има класифицирана информация, свързана със случая. Също така е възможно обаче дори водещият следовател да няма достъп до цялата потенциално чувствителна информация и трябва да бъде проведено по-широко разследване.

Информация, получена по Закона за наблюдение на чуждестранното разузнаване

Въпреки че информацията, получена след прилагане на Закона за наблюдение на чуждестранното разузнаване (ЗНЧР), винаги е класифицирана и с нея трябва да се работи по съответен начин, съществуват допълнителни изисквания, които се отнасят до използването или разкриването на получена или извлечена по ЗНЧР информация.

Прокурорът трябва да получи одобрение от главния прокурор според дефиницията от ЗНЧР, преди да използва каквато и да е получена или произтичаща по ЗНЧР информация в наказателно съдебно производство. Това одобрение се изисква, преди да се даде информацията за разкриване и дори преди да се даде информацията на съдия, за да се потърси разрешение за изключването ѝ от разкриване. Процесът на одобрение за използване или разсекретяване на получена и произтекла по ЗНЧР информация задължава местното бюро на ФБР с помощта на прокурора да произведе писмена молба, наречена „молба за ползване“, която трябва да се изпрати в централата на ФБР чрез Генералния съвет на ФБР и след това да се предаде на Процесуалната секция на Разузнавателното бюро на Отдела за национална сигурност (ОНС). Процесуалната секция подготвя меморандум до Главния прокурор, който в последна сметка одобрява или отхвърля молбата. Тъй като има много звена на ФБР/ОНС, които трябва да разгледат и да одобрят молбата за ползване по ЗНЧР, процесът може да бъде продължителен. Прокурорите трябва да направят така, че този процес на одобрение да започне веднага щом стане ясно, че по време на съдебното разследване ще се използва информация, получена или произтичаща от ЗНЧР, било то като улика по делото, да бъде разкрита при делото, или да бъде изключена от разкриване.

Разкриване на обемна класифицирана информация

При дела, свързани с класифицирана информация, има случаи, когато голям обем материали се събират в хода на следствието. Ако прокурорът на-

учи, че се обсъжда използването или вече се прилага подслушване по ЗНЧР или някакво друго разузнавателно устройство, което може да доведе до голям обем от разкрития, най-добре е да се реши отрано каква информация може да подлежи на разкриване и най-вече коя информация може да бъде оправдателна. Особено когато информацията, която се събира, е на чужд език и може да бъде трудно да се прегледа в течение на делото, важно е да се уведомят следователите и лингвистите, които правят прегледа за това кой тип информация трябва да бъде обозначена като потенциално подлежаща на разкриване, и тя да бъде отделена, за да се прегледа от прокурора.

Дори когато по делото трябва бързо да се извърши арест, а прокурорът не е имал време да прегледа информацията, за да реши каква информация подлежи на разкриване, чувствителността на информацията, получена по ЗНЧР, изисква тя да бъде прегледана, за да се определи каква част от нея може да бъде разкрита, преди да се търси разсекретяване или разкриване на информацията. При тези обстоятелства прокурорът може и да не разчита, че ФБР ще разсекрети информацията в нейната цялост, и просто да предаде тази информация на защитата.

7. ФЕДЕРАЛНИ ПРАВИЛА ЗА НАКАЗАТЕЛНА ПРОЦЕДУРА

Приоритет на Департамента по правосъдие е защитата на САЩ и техните граждани срещу терористични актове и други заплахи за националната сигурност. От ключово значение при изпълнение на тази задача е федералните прокурори да използват всички средства, предвидени в Конституцията и федералния закон за споделяне на ценна информация, свързана с националната сигурност, с онези, които имат нужда от тази информация, за да изпълняват служебните си задължения. PATRIOT Act и Законът за разузнавателна реформа и превенция на тероризма от 2004 г. дават на ДП допълнително средство за постигане на тази цел: наредбите внасят поправка в правилото, определящо секретността на голямото жури, и допускат по-свободен обмен на информация между разузнаване и контраразузнаване. На 15 май 2008 г. главният прокурор обнародва *Насоки за разсекретяване и използване на информация от голямото жури по член 6(e)(3)(D).* Насоките издигат на по-горно ниво целта за обмен на информация на тези закони, като улесняват обмена на материал от голямото жури, който е от значение за националната сигурност. В същото време Насоките предоставят защита на този материал, като определят точни методи за разсекретяване и използване. В случай на използване без разрешение потребителят може да стане обект на обвинение за обида на съда и други приложими със случая обвинения.

Заявки за дискретно претърсване

„Дискретно претърсване“ е претърсване на материали на Агенцията на разузнавателната общност обикновено преди предявяване на обвинението, предприето, тъй като екипът на прокурора има определено основание да смята, че материалите на Агенцията съдържат класифицирана информация, която може да се отрази върху обвинителните решения на правителството. Прокурорът трябва да се свърже с Отдела за национална сигурност (ОНС), за да координира дискретно претърсване за потенциално подлежаща на разкриване информация преди предявяване на обвинителния акт, ако има основание да смята, че:

- Агенцията вероятно разполага с информация, която може да се отрази върху това дали, срещу кого и за какви престъпления да се повдигне обвинение;
- Разузнавателната общност или военните разполагат с документи, които влизат в обхвата на задълженията на прокурора за положителна проверка. В такива случаи обсъждания на тема как да се борави с документите и информацията, предшестващи повдигането на обвинение, могат да помогнат да се избегнат конфликти, изненади и дилеми разкриване/отхвърляне;
- Делото може да повдига други въпроси, свързани с класифицирани доказателства, които трябва да бъдат разрешени преди повдигането на обвинение. Въпреки че не е задължително според закона, такова претърсване дава възможност на прокурора да провери въпроси, които биха могли да възникнат след предявяване на обвинението, свързани с класифицирана информация и разкриването, които прокурорът може да отнесе към бъдещ ответник. Такова претърсване може да подпомогне прокурора при анализа на престъпления и обекти, потенциално подлежащи на обвинение, и може да го накара да изключи определени престъпления и обекти от обвинителния акт.

Координация на заявките за претърсване

Всички заявки за обиск на съставна част на разузнавателната общност или на военните от прокурор на Департамента по правосъдие, който се занимава с разследване или преследване в явна връзка с националната сигурност, или с информация, притежавана от разузнавателната общност, трябва да бъдат направени чрез Отдела за национална сигурност, освен в случаите на конкретна различна уговорка между помощник главния прокурор на ОНС и помощник главния прокурор на Криминалния отдел.

Секторът за борба срещу тероризма (СБТ) е контактната точка за всички наказателни дела, които имат определена връзка с международен тероризъм; вътрешен тероризъм; мъчения, военни престъпления и геноцид и оръжия за масово унищожение.

Секторът за контраразузнаване е контактна точка за разследвания, свързани с икономически шпионаж, в който има намерение да се облагодетелства чужда държава, и други престъпления срещу националната сигурност, изброени в Наръчника на прокурорите на САЩ. Секторът за законодателство и политика на ОНС се занимава с всички останали престъпления срещу националната сигурност и заявките за обиск на разузнавателната агенция.

Отделът за национална сигурност (ОНС) координира между съответните прокурори от ДП и разузнавателната общност и военните, за да гарантира, че подлежащ на разкриване класифициран материал е предоставен на прокурорския екип за преглед. ОНС, в консултация със съответните прокурори от ДП, осъществява също така координация с подходящите звена на разузнавателната общност и военните, за да гарантира, че пълномощното и други разрешения са получени навреме; че заявките за разсекретяване са прегледани в срок и че исканите разсекретявания са направени в съответствие с взаимно съгласувани и подходящи механизми за защита на информацията. Прокурорите също трябва да се съветват с подходящото звено на ОНС, ако не са сигурни дали дискретният обиск е оправдан.

Съдържание на заявките за извършване на обиск

Заявките за обиск трябва да бъдат конкретни, внимателно обосновани, базирани върху специфични за делото факти и трябва да съдържат следната информация:

- Естеството на обвиненията или евентуалните обвинения (ако се извършват преди внасяне на обвинителния акт) и евентуалните защити;
- Цялата налична информация за самоличността на всеки обвиняем/заподозрян и евентуален свидетел (например име, включително собствено, бащино и фамилно, прякори и псевдоними и всякакви правописни варианти, които прокурорът иска да бъдат проверени; дата на раждане; гражданство и всякакви държавни идентификационни номера);
- Вид на търсената информация;
- Времеви период, който трябва да се покрие (който обикновено съвпада с времевия период на престъпната дейност, за която е предявено обвинение или предстои да бъде предявено);
- Компонентите на разузнавателната общност и/или военните, които са замесени в делото, и обсъждане на естеството на тяхното участие и
- Основание за заявката за обиск.

ИЗПОЛЗВАНЕ НА ИНФОРМАЦИЯТА, ПОЛУЧЕНА ПО РЕДА НА ЗАКОНА ЗА НАБЛЮДЕНИЕ НА ЧУЖДО РАЗУЗНАВАНЕ (ЗНЧР)

Предварителни разрешителни

По закон се изисква одобрение от главния прокурор, преди каквато и да е информация, получена или произтичаща по ЗНЧР, да се използва при наказателното производство. Политиката на Департамента по правосъдие е да изисква също така одобрение на главния прокурор за използването на получена или произтичаща по ЗНЧР информация при всички останали производства (като граждански или административни дела) както на федерално, така и на щатско ниво. Правното основание за използване в наказателни производства е дадено в Глава 50 от Кодекса на САЩ, параграф 1806(b):

Досъдебна публичност, забранителни заповеди

Тъй като делата, свързани с тероризъм, привличат общественото внимание, в тях често пъти възникват разнообразни теми, включително за досъдебна публичност, забранителни заповеди, промяна на посоката и дълги въпросници на съдебните заседатели.

Досъдебна публичност

Обикновено делата, свързани с тероризъм, привличат силното внимание на медиите. Отделът за национална сигурност (ОНС) има свой медиен координатор в Службата по обществени въпроси на ДП, който работи в тясно сътрудничество с ОНС и прокурорските служби на САЩ, за да координира въпроси, свързани с медиите, по теми на националната сигурност. Параграфи 1.7-400 до 1.7-500 от Наръчника на прокурорите на САЩ указват методи за даване на публична информация за текущи разследвания и предстоящи дела. По отношение на контактите с медиите след повдигане на обвиненията, но преди обявяване на присъдата, всякакви комуникации трябва да се ограничават до информацията, съдържаща се в обвинителния акт или други инструменти на обвинението, публични пледоарии и протоколи и друга несвързана с наказателното производство информация. Пресконференции трябва да се провеждат само при най-знакови и заслужаващи вниманието на медиите действия или ако обслужват някаква особена цел по възпиране или правоприлагане (пак там).

Клаузите от Наръчника на прокурорите на САЩ са кодирани в раздел 50.2 на Глава 28 от Кодекса на федералните наредби, който дава указания на служителите на ДП за предоставянето на информация на медиите за граждански и наказателни дела. Раздел 50.2 гласи:

„В никакъв случай служител на ДП не трябва да прави каквото и да е заявление или да предоставя информация, предназначена да повлияе върху

делото на обвиняемия, нито да прави изявление или да дава информация, която може да бъде разпространена със средствата на масовата комуникация, ако такова изявление или информация има вероятност да повлияе върху изхода на текущо или предстоящо дело. Може да има определени обстоятелства, при които информация може да бъде дадена на медиите, без тя да има изпреварващ делото ефект. Така че, ако представител на Департамента смята, че в интерес на справедливостта и на процеса на прилагане на закона по определено дело трябва да бъде дадена информация извън препоръчителната, за да го направи, той трябва да поиска разрешение от главния прокурор или от заместник главния прокурор".

Заповеди за забрана

Поради значителното внимание от страна на медиите към делата, свързани с тероризъм, понякога съдът налага заповед за забрана на комуникацията между страните и пресата. „Обикновено ограничителна заповед върху комуникацията на участниците в процеса с пресата ще бъде наложена само в случай, че правителството установи, че дейността, която се ограничава, представлява или ясна и съществуваща опасност, или сериозна и непосредствена заплаха за защитен конкурентен интерес." Заповедта също така трябва да бъде конкретна и възможно най-малко рестриктивна.

Клопка

В делото *United States v. Russell, 411 U.S. 423 (1973)* Върховният съд поставя основите за изграждане на защита на базата на поставянето на клопка. Поставянето на клопка е относително ограничена защита. Тя се основава не върху това, каквото и да е правомощие на съдебната власт да отхвърля наказателно производство за нещо, което смята за „прекалено старателно правоприлагане", а върху разбирането, че Конгресът не е предвиждал криминално наказание за обвиняем, който е извършил всички елементи на подсъдното деяние, обаче е бил подтикнат от правителството да го направи.

Поставянето на клопка може да бъде цялостна защита за престъпление, ако са налични два елемента:

- Правителството е предизвикало престъплението и
- Обвиняемият няма предразположение да предприеме престъпно поведение.

От двата елемента предразположението е по-важно. В повечето инстанции, когато защитата представи наличието на първия елемент, доказателствената тежест се прехвърля върху правителството, което трябва да докаже предразположение извън разумното съмнение. Самият намек да бъде извършено престъпление не е подтик. Подтикването изисква да се покаже поне наличието на убеждаване или лека принуда, молби, основа-

ни върху нужда, симпатия или приятелство, или невероятни обещания от такъв порядък, които биха „накарали обикновения гражданин да забрави правните си задължения".

Дори ако се покаже наличието на подтик, откриването на предразположение е от ключово значение за защита, основана върху поставяне на клопка. Разследването на предразположението се съсредоточава върху това дали обвиняемият „е лековерен невинен, или напротив, лековерен престъпник, който с готовност е прегърнал възможността да извърши престъпление".

Правно основание

Две дела на Върховния съд при защита, основана върху поставянето на клопка, са *Mathews v. United States,* 485 U.S. 58, 63 (1988) и *Jacobson v. United States,* 503 U.S. 540, 548 (1992). В *Mathews* Съдът постановява, че обвиняем, който отрича да е извършил престъпление, има право на инструктаж за поставяне на клопка, доколкото е налице достатъчно доказателство, в което съдебните заседатели могат да видят наличието на клопка. *Mathews,* 485 U.S. at 62. Така че обвиняемият може да се защитава непоследователно с аргумента, че не е извършил престъплението, обаче дори да го е извършил, той е бил хванат в клопка. Въпреки че наличието на клопка обикновено се решава от съдебните заседатели, *Mathews, 485 U.S. at 63,* според Върховния съд то е въпрос на правото в делото *Jacobson, 503 U.S. at 550,* където ответникът е поръчал детска порнография, след като „в продължение на 26 месеца е бил обсаждан с писма и комуникации от правителствени агенти и фиктивни организации". Според Съда правителството не е успяло да докаже отвъд всякакво съмнение, че предразположението на Джейкъбсън „е нещо отделно, а не е продукт на вниманието, което правителството е насочило към него". Необичайните факти в делото *Jacobson* го отличават от повечето секретни операции, в които има по-малко контакти с обвиняемия за по-кратък период от време.

Доказване на предразположение

Обвиняем, който твърди, че му е заложена клопка, се подлага на „подходящо разследване на собственото му поведение и предразположение, доколкото имат връзка с този въпрос" *Sorrells v. United States,* 287 U.S. 435, 451 (1932). Така че предразположението може да бъде предявено чрез доказателство за други престъпления – Federal Rule of Evidence 404(b) – доказателство, което в други случаи би било неприемливо. И въпреки че в *Jacobson* се набляга върху задължението на правителството да покаже, че обвиняемият е бил предразположен да извърши престъплението, „преди с него да се свържат правителствените чиновници", *Jacobson, 503 U.S. at 549,* се поражда съмнение доколко е допустимо доказателство за последващи престъпления да покаже предразположение, така както в *United States v.*

Posner, 865 F.2d 654 (5th Cir. 1989) и в *United States v. Warren,* 453 F.2d 738 (2d Cir. 1972), cert. denied, 406 U.S. 944 (1972).

Има основание да се твърди, че доказателството в *Jacobson* е приемливо, доколкото последвалите престъпления са „независими и не са резултат от вниманието, което правителството е насочило" към обвиняемия. Предразположението може да се докаже косвено с доказателство за поведение на обвиняемия след свързването му с агент под прикритие. В *United States v. Ogle,* 328 F.3d 182, 185-87 (5th Cir. 2003) (знанието на обвиняемия и доброволното му участие в международна схема за изпиране на пари – което се доказва с това, че идва на срещата с десет алтернативни схеми за изпиране на пари – показва предразположение).

Поставяне на клопка като въпрос на правото

Поставянето на клопка като въпрос на правото съществува, когато: (1) показанията и фактите са неоспорими и (2) уликите показват липса на предразположение. Обвиняемият може да се позове на поставянето на клопка като правен въпрос като основа за отхвърляне на член 29 от федералната наказателнопроцесуална процедура.

Чуждестранно доказателство

При процеси, свързани с националната сигурност, доказателствата често пъти се намират извън контрола на САЩ. Най-общо казано, има два типа чужди документи, които могат да бъдат представени в американски съд: (1) публични регистри и (2) бизнес документация. Публичните регистри включват актове за раждане, военни книжки, присъди и митнически/паспортни документи. Когато са правилно заверени, публичните документи доказват автоматично автентичността си.

Представянето на чуждестранни доказателства в съдилищата в САЩ до голяма степен е същото, както представянето на събраните на местна почва доказателства. Конституцията на САЩ обаче не се прилага към получените от чужбина доказателства. Важно е да се отбележи, че това се отнася само за чуждестранно доказателство, което не е получено в резултат на съвместно начинание на чуждестранни и американски висши правителствени чиновници.

Вещи лица

Федералното правило 702 за доказателството е основата за експертното мнение на вещо лице във федералния съд. В делото *Daubert v. Merrell Dow Pharm., Inc.,* 509 U.S. 579 (1993), Правило 702 задава подходящи граници за допустимостта на предполагаемо експертно доказателство, като възлага на съдията по делото задачата да провери, че показанието на вещото лице едновременно почива върху достоверна основа и има отношение към

разглежданата задача. Показанието на вещо лице в дела за тероризъм се отклоняват или по посока на социологията, или на специализираното знание, като например история и организационна структура на чуждестранна терористична организация.

При предложение за експертно показание по Правило 702 съдията, спазвайки Федералния закон за доказателствата 104(а), трябва предварително да прецени дали аргументите или методологията на показанието са научно оправдани и могат да се приложат към разглежданите факти. Разследването трябва да взема предвид много съображения, включително дали въпросната теория или техника може (и е била) проверена, дали е била подложена на партньорска проверка или публикация, които да определят известния или потенциален процент на грешка и наличието и поддръжката на стандарти, които да контролират прилагането ѝ, и дали тя е единодушно приета от съответната научна общност.

Проучването е гъвкаво и трябва да се фокусира единствено върху принципи и методология, а не върху заключенията, до които те водят. През цялото време съдията трябва да обръща внимание и на други приложими правила. Кръстосан разпит, представяне на обратни доказателства и внимателни инструкции за доказателствената тежест вместо автоматично изключване под стандарта за „общо приемане“ са подходящите средства, с които може да бъде атакувано доказателство, основано на валидни принципи. Показанията на експерти са вече част от съвременното съдебно преследване на тероризма.

Подтикване към тероризъм

Според тълкуванията на Върховния съд на САЩ гаранцията за свобода на словото в Първата поправка обхваща и словото, подтикващо към незаконно поведение, и ограничаването на такова слово е допустимо само в изключителни обстоятелства: конституционната гаранция за свобода на словото и свобода на пресата не позволява на даден щат да забранява или отхвърля проповядването на употребата на сила или нарушаването на закона, освен когато такова проповядване е насочено към възбуждане или извършване на непосредствено престъпно деяние и вероятно ще доведе до извършване на такова деяние. Съдебната практика показва, че непосредствената заплаха, която се изисква според *Brandenburg*, е строгият стандарт, регулиращ престъпления, свързани с „проповядване“.

Независимо от ограниченията, които Първата поправка налага върху възможността да се регламентира словото, слово, което е равносилно на поведение – или което е средство за това поведение – може законно да бъде забранено, наказано или регламентирано чрез конституционното налагане на обичайно приложими закони.

Тогава възниква въпросът дали конкретно дело за тероризъм може да бъде отнесено към *Brandenburg,* като в такъв случай прокурорите трябва

да инструктират по *Brandenburg* съдебните заседатели. Дадено дело ще се позовава на *Brandenburg,* ако в същината си се стреми да накаже проповядването на тероризъм, а не някакво терористично деяние. От всички терористични престъпления върху *Brandenburg* най-много се позовават в делата за подмолни заговори, Глава 18, Кодекс на САЩ, параграф 2384, където се инкриминира заговорът за употреба на сила с цел сваляне на правителство.

Законът, който най-много се доближава до общото инкриминиране на склоняването, е законът за подбуждането, Глава 18, Кодекс на САЩ, параграф 373. Въпреки това обаче склоняване и подбуждане не са синоними и даден човек може да бъде осъден за склоняване дори в случай, когато се опитва да склони агент под прикритие и следователно няма шанс да успее.

Какво може да се каже за делата за материална подкрепа? В делото *Holder v. Humanitarian Law Project*, 130 S. Ct. 2705 (2010), становището на Върховния съд е, че словото, а не само поведението е обект на разглеждане и че ищците са предлагали материална подкрепа под формата на слово. Независимо от това Съдът решава, че такова слово може да се забрани като забрана за материалната подкрепа, която не е насочена директно към забрана на словото. Съдът отбелязва, че правителството признава че „независимото застъпничество и изразяване“ не е забранено от Глава 18 от Кодекса на САЩ, параграф 2339В и 2723, и хвали Конгреса, задето е осъдил материалната подкрепа, а не независимото застъпничество. Той също така смята, че липсата на забрана за независимото застъпничество е основната причина, поради която параграф 2339В не нарушава Първата поправка. Съдът изброява редица независими дейности, които смята, че не трябва да бъдат забранявани по параграф 2339В: По закона за материална подкрепа ищците могат да говорят каквото си искат по всяка тема. Могат свободно да говорят и да пишат за чуждестранни терористични организации, за правителствата (във връзка с тези чуждестранни терористични организации), човешките права и международното право. Това подсказва, че параграф 2339В е насочен единствено към поведението и прокурорите трябва да възразяват срещу позоваването на *Brandenburg* в този контекст.

Демонстрации

Демонстрации или демонстративни улики са аспект от доказателството, които представят или поставят в контекст друго доказателство, представено пред съда и целящо да подпомогне търсещия истината. Демонстрационната улика може да включва карти, диаграми или модели на сцената на престъплението или анимации, стимулации или компютърни възстановки на престъплението. В случаи на процеси, свързани с националната сигурност, демонстрационната улика често пъти показва контролирано взривяване на устройства за разрушение, за да се илюстрира пред съдебните заседатели силата на експлозията или как устройството,

използвано от обвиняемия, е трябвало да действа. Демонстрационното доказателство е приемливо, ако е уместно. „Стандартът за уместност е „изключително либерален". Доказателството е уместно, ако има „тенденция да направи съществуването на даден факт, който е следствие от дадено действие, по-вероятен или по-малко вероятен, отколкото би бил без доказателството".

Обикновено обвиняемите твърдят, че такива демонстрации са несправедливо преднамерени. Въпреки това обаче фактът, че демонстрациите на правителството са инкриминиращи, не означава, че те са несправедливо преднамерени. „Несправедлива преднамереност не означава да се нанесе вреда на делото на ответника, произтичаща от доказателствената сила на уликата; по-скоро става дума за улика, която подсказва за решение, взето на неправилна основа. Доказателство, което е смущаващо и дори скандално, обикновено се приема, когато е подходящо.

На едно дело се случва следното:

Правителството взема показания от експерт по експлозиви, който първо описва как е конструирана бомбата. Експертът анализира частите от демонтираната бомба и изгражда модел, за да покаже как е изглеждала бомбата в нейната цялост. Като използва модела, след това той провежда кратка демонстрация, срещу която адвокатът на Смит възразява, за да илюстрира как е трябвало да функционира бомбата. Той също така изразява мнение, че подготвяната експлозия не се е случила, защото е имало повреда или в електрическата верига, или в детонатора. Той заключава, че бомбата е имала за цел да осакати или убие случайни минувачи или да разруши имущество. При обжалването обвиняемият заявява, че моделът и демонстрацията са били несправедливо преднамерени. Седмият федерален апелативен съд излиза със становище че „окръжният съд правилно е допуснал експертната демонстрация ... тъй като е било необходимо да се помогне на правителството да се справи с доказателствената тежест да покаже, че Смит е възнамерявал да използва бомба с намерението да причини вреда".

Апелативният съд постановява, че „улика, която е доказателство за елемент на престъплението, трябва да бъде допусната във всяко освен в най-бруталните дела". Съдът по-нататък заявява, че „показанията на експерта са важно доказателство, че бомбата е била предназначена да избухне, и подкрепят становището на правителството по делото". Седмият федерален апелативен съд отхвърля твърдението, че демонстрацията била неоправдано преднамерена, тъй като „експертната демонстрация не е била направена по провокативен начин с цел да се възбудят емоциите на съдебните заседатели". Съдът отбелязва, че демонстрацията на експерта видимо противоречи с теорията на обвиняемия, че бомбата не е била предназначена да избухне, но този факт не прави уликата несправедливо преднамерена. Както обяснява съдът: „Смит е можел да подложи на кръстосан разпит експерта, което е направил, или да призове свой свидетел".

Призоваване на обвиняеми и свидетели от чужбина

Съединените щати имат подписани редица споразумения за екстрадиция, споразумения за взаимна правна помощ (СВПП) и други договори с други страни, които изискват нашите чуждестранни партньори да направят всичко възможно за връщането на бегълци обратно в САЩ и за получаване на достъп до доказателства и свидетели, намиращи се в чужбина. Трябва да се обърнете към Международната служба на Криминалния отдел, ако имате дело, в което обвиняемият или ключов свидетел са може би в чужбина. Довеждането на обвиняем в престъпление или на свидетел по дело в САЩ изисква този човек да има някакъв легален статут, за да може да влезе в страната. Един такъв статут е значителната обществена полза.

Значителна обществена полза: Статутът за значителна обществена полза може да бъде използван, за да влезе в САЩ чуждестранен обвиняем, свидетел или сътрудничещ източник, а ако е възможно, в изключително редки случи и най-близките роднини на чужденеца. Това е временна мярка, която се използва, за да се даде възможност на чужденец, който по друг начин не може да влезе в САЩ, да се яви на делото. Това е и временна мярка в подкрепа на усилията на правоприлагащите органи, която създава легален механизъм за информатори, свидетели и обвиняеми, които инак не могат да бъдат приети в САЩ да пристигнат, за да окажат помощ при текущи разследвания, съдебни преследвания и други дейности, необходими за защита на националната сигурност. Значителна обществена полза се дава за минималния срок, необходим за постигане на правоприлагащата цел, до една година, и може да бъде подновяван няколкократно. INA, параграф 212(d)(5)(A), Глава 8, Кодекс на САЩ, параграф 1182(d)(5)(A). На територията на САЩ спонсориращата правоприлагаща агенция ще трябва да съблюдава изискванията за наблюдение на условно пуснатия на свобода. След като целта се постигне, чужденецът трябва да си замине от страната. Веднъж доведени в САЩ обаче, обратното връщане на обвиняеми и свидетели може да се окаже трудно. Те могат да поискат убежище или да настояват, че в страната, в която трябва да бъдат върнати, ще станат жертви на мъчения, което противоречи на Конвенцията на ООН срещу изтезанията. Затова е необходимо да се постигне възможно най-тясна координация между службите, преди да се призоват свидетели и обвиняеми на територията на САЩ.

Вътрешен тероризъм

Разследванията за вътрешен тероризъм се провеждат в съответствие с Ръководството на главния прокурор за разследване на престъпления от общ характер, рекет и тероризъм. Това Ръководство задава предикативния праг и граници за разследване на американски граждани, живеещи в САЩ, които не действат в интерес на друга държава и които може би извършват престъпни дейности. Съвместните отряди за борба срещу тероризма на ФБР разглеждат въпроси, свързани както с вътрешния, така

и с международния тероризъм. Секторът за борба с тероризма (СБТ) на Департамента по правосъдие е определил неколцина прокурори за координатори по вътрешен тероризъм. Тези прокурори имат опит в разследването и възбуждането на съдебни дела за вътрешен тероризъм и работят в тясно сътрудничество с централата на ФБР.

Прокурорските служби са длъжни да уведомяват СБТ, когато разследват или завеждат дела за вътрешен тероризъм. Уведомлението може да бъде подадено чрез Съвместните отряди за борба срещу тероризма или чрез координаторите на регионалните консултативни съвети за борба срещу тероризма. Уведомлението до СБТ е задължително, когато помощник-прокурор на САЩ научи за дело за вътрешен тероризъм, възбудено от Съвместните отряди за борба срещу тероризма на ФБР, и започне да наблюдава случая.

8. БОРБА СРЕЩУ КИБЕРЗАПЛАХИТЕ ЗА НАЦИОНАЛНАТА СИГУРНОСТ

Киберзаплахи за националната сигурност

Киберзаплахите за националната сигурност включват киберпрониквания и атаки, които са извършени в полза на терористи или чужди държави или които по друг начин имат последици за националната сигурност.

Примери за последната категория могат да включват, но не се ограничават до:

- Прониквания, насочени към защитена информация (например отбрана, контролирана или класифицирана информация);
- Прониквания, осъществени с цел, заплашваща националната сигурност (например получаване на пари за финансиране на тероризъм), или
- Прониквания, при които обемът, мащабът или набелязаният обект повдигат опасения, свързани с националната сигурност.

Предвид предизвикателствата, свързани с установяване на авторството в киберсредата, когато се случи киберинцидент, често пъти не е възможно да се установи кой стои зад определена атака или проникване и дали то има отношение към националната сигурност. За да гарантира, че целият арсенал от средства и ресурси на Департамента по правосъдие, включително правоприлагащият разузнавателен потенциал, е на разположение в подкрепа на тези усилия, ДП, включително и ФБР, трябва да предположат – освен или докато по категоричен начин не се изясни нещо друго – че лицата, представляващи заплаха за националната сигурност, може би са отговорни за тези заплахи и атаки.

Мрежа на киберспециалистите по национална сигурност

В подкрепа на масирания подход за борба срещу киберзаплахите за националната сигурност и за да запази всичките си възможности при известни и подозирани киберпрониквания в националната сигурност, през юни 2012 г. Отделът за национална сигурност създаде мрежата КСНС. Мрежата КСНС бе създадена, за да се подобри координацията, подкрепата и образованието в рамките на цялото ДП относно разследването и съдебното преследване на киберпрониквания, засягащи националната сигурност. Мрежата КСНС е разработена по такъв начин, че да бъде източник на ресурси, които да се използват при киберинциденти, в които могат да участват терористи или национални държави или които покриват други критерии, показващи потенциална заплаха за националната сигурност.

Мрежата КСНС има два компонента: Главно, със седалище във Вашингтон – КСНС – Главно; и национална мрежа от контактни точки за КСНС, базирани в щатските прокурорски служби.

КСНС – Главно включва юристи и други киберспециалисти, привлечени от различни секции и служби на ОНС (Сектора за борба срещу тероризма (СБТ), Разузнавателната служба, Звеното за преглед на чуждестранните инвестиции, Правния и политически отдел, както и Сектора за компютърни престъпления и интелектуална собственост на Криминалния отдел и Службата за силови операции).

Когато е необходимо, КСНС – Главно координира действията си с други компоненти на ДП, включително Гражданския отдел, Антимонополния отдел, Службата за правна политика и Службата за правен съвет, и работи в тясно сътрудничество с разследващите компоненти на ДП, включително с ФБР.

Мрежата КСНС също така включва по един помощник-прокурор във всяка щатска прокурорска служба, който служи като първа контактна точка за своята служба за дела, свързани с киберзаплахи за националната сигурност, и работи в тясна координация с КСНС – Главно. Той има разрешително за работа със секретна информация и е преминал през специализирано обучение.

Проблеми, възникващи при разследване и наказателни дела за киберпрестъпления, свързани с националната сигурност

Структурата на Мрежата КСНС отразява обстоятелството, че отговорът на киберинциденти изисква наличието на експертиза по отношение на престъпления срещу националната сигурност и компютърни престъпления. Тези теми поставят много от същите предизвикателства, свързани с разследването и наказателното преследване на традиционните киберпрестъпления, както и нови проблеми, възникващи поради последиците за националната сигурност. Тези предизвикателства включват:

- Да се действа със съзнанието за потенциалното влияние на случая върху разузнаването и други аспекти на националната сигурност;
- Да се работи с различни правоприлагащи и разузнавателни агенции;
- Да се защитава класифицирана информация;
- Да се установи източникът на заплахата („да се сложи пръст върху клавиатурата“);
- Да се преодоляват предизвикателствата, свързани с уликите, включително възможността за унищожаване на електронни улики;
- Да се работи с жертви и
- Да се разбират законите и наредбите, отнасящи се до жертвата и нарушаването на уведомление и условията за събиране на такси и забавяне на тези изисквания, когато се налага.

Координация и ресурси

Сложността на тези дела – и разнообразието на правоприлагащи, разузнавателни, технически и правни въпроси, които те повдигат – изисква тясна координация и честа комуникация между КСНС – Главно и компонентите в прокурорските офиси, между всички членове на КСНС и помощник-прокурорите и членовете на мрежата КСНС в съответните прокурорски служби.

Следователно съществуващите клаузи в Наръчника на прокурорите на САЩ (например USAM, параграф 9-90.020) трябва да се тълкуват в широк смисъл в контекста на киберинцидентите. Мрежата КСНС, и в частност КСНС – Главно, трябва своевременно да бъде уведомявана за възникването или съществуването на всеки киберпроблем, който отговаря на главните критерии, изброени в тази глава, и може да представлява заплаха за или да е свързан с националната сигурност. Уведомлението няма автоматично да задейства изисквания за допълнителни консултации и одобрения, освен ако ясно не посочват съществуващите изисквания в Наръчника; то само ще съдейства за по-бързо решение за възлагане и за по-голяма обща ситуационна осведоменост.

ВТОРА ЧАСТ: ПОДСЛУШВАНЕ

Прокурорите обикновено се сблъскват със Закона за подслушването по време на наказателни разследвания, защото той регулира използването на подслушването като метод за разследване на престъпление. Въпреки това обаче Законът за подслушването, известен още като „Глава III", е едновременно процесуален и съдържателен. Той забранява не само на правоприлагащите органи, но и „на всеки човек" да подслушва незаконно, да разкрива или използва незаконно подслушан материал. Глава 18, Кодекс на САЩ параграф 2511(1). Така например Законът за подслушването бе използван за даване под съд на нарушителите по аферата „Уотъргейт". Виж *United States v. Liddy,* 509 F.2d 428 (D.C. Cir. 1974). През 1986 г. той стана полезен закон за компютърните престъпления, след като Конгресът прие поправки, за да покрие изрично „електронните комуникации" – широк термин, който включва компютърните мрежови комуникации. Виж *Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995). („Главната цел на поправките от 1986 г. в Глава III бе да разпростре върху „електронните комуникации" същите защити срещу незаконно прихващане, каквито Глава III дава на „устни" и „жични" комуникации посредством общ предавател.")

Прокурорите трябва да решат дали Законът за подслушването е приложим по дело, включващо потребители и производители на шпионски софтуер, нарушители, които използват незаконни компютърни програми, лица, които клонират имейл акаунти, или какъвто и да е друг нелегален начин за събиране на комуникации от компютъра на жертвата.

Законът за подслушването е сложна тема и тази глава не е изчерпателна. Тя е насочена към забраните в него, всяка от които е разгледана по-долу: *подслушване* на комуникации, Глава 18, Кодекс на САЩ, параграф 2511(1) (a) & (b); *разкриване* на подслушани комуникации, Глава 18 от Кодекса на САЩ, параграф 2511(1)(c) & (e) и *използването* на подслушани комуникации, Глава 18 от Кодекса на САЩ, параграф 2511(1)(d). Тези забрани са обект на редица изключения. В тази глава се разглеждат практически най-приложимите от тези изключения.

1. ПОДСЛУШВАНЕ НА КОМУНИКАЦИЯ

Глава **18,** Кодекс на САЩ**,** параграф **2511(1)(a)**

Основаната забрана в закона за подслушването е записана в параграф 2511(1)(a), който забранява „който и да е" преднамерено да подслушва или да се опита да подслушва всякаква телефонна, устна или електронна комуникация.

2511(1)(а) Обобщение

1. преднамерено
2. подслушване (или опитване или склоняване на друг да подслушва) на съдържанието на телефонна, устна или електронна комуникация
3. чрез използването на устройство.

Глава 18, Кодекс на САЩ, параграф 2511(1)(а) гласи:

Освен в случаите, изрично указани в тази глава, всяко лице, което – (а) преднамерено подслушва, опитва се да подслушва или дава възможност на трето лице да подслуша или да се опита да подслуша която и да е телефонна или устна комуникация... ще бъде наказано според разпоредбите, записани в параграф (4)

Първият федерален апелативен съд неотдавна излезе с изчерпателно становище на елементите, престъпление по параграф 2511(1)(а), в гражданско дело. *Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 18 (1st Cir. 2003). Тези елементи са изредени в горната таблица и се разглеждат по-долу. Текстът на параграф 2511(1)(а) описва само три елемента: (1) преднамерено, (2) подслушва и (3) комуникация. Въпреки това обаче в тези дефиниции са заключени допълнителни изисквания, което обвинителните актове и инструкциите на съдебните заседатели често пъти включват: по-точно, изискванията подслушването да е извършено с „устройство“ и то да е направено едновременно с предаването му.

ПРЕДНАМЕРЕНО

В гражданско дело по Закона за подслушването Четвъртият федерален апелативен съд одобри следната приета дефиниция за „преднамерено“ за инструктаж на съдебните заседатели.

Дадено действие е извършено преднамерено, ако е направено осъзнато и целенасочено. Което означава, че дадено действие е извършено преднамерено, ако съзнателната цел на лицето е да извърши действието или да причини резултата. Дадено действие е непреднамерено, ако е резултат от непредпазливост или грешка. Въпреки това обаче мотивът на обвиняемия не е приложим и няма нужда обвиняемият да е целял

конкретните резултати от своето поведение или да е знаел, че поведението му нарушава закона.

Abraham v. County of Greenville, 237 F.3d 386, 391 (4th Cir. 2001); вижте също *United States v. Townsend,* 987 F.2d 927, 930 (2d Cir. 1993).

Понякога обвиняемите твърдят, че те не са били в изискваното психическо състояние, тъй като са вярвали, че подслушването им е законно. Въпреки това обаче даден човек може да бъде признат за виновен за това, че преднамерено е подслушвал комуникация, макар погрешно да е смятал, че подслушването е законно. През 1986 г., като част от Закона за поверителност на електронните комуникации, Конгресът промени психическото състояние в параграф 2511 от „умишлено" в „преднамерено". Виж S. Rep. No. 99-541, at 23 (1986), препечатано в 1986 U.S.C.C.A.N. 3555, 3577; *United States v. Townsend*, 987 F.2d 927, 930 (2d Cir. 1993). Преди промяната някои съдилища поддържаха становището, че старият стандарт „умишлено"означава, че съдебните заседатели могат да вземат под внимание „доказателство, че обвиняемият е действал или не е действал поради незнание на закона", където незнание на закона съответства на „дали обвиняемият е действал или не е действал със специфично намерение" *United States v. Schilleci,* 545 F.2d 519, 523-24 (5th Cir. 1977). Докладът на Сената ясно заявява, че „преднамереното психическо състояние е приложимо единствено към поведение и резултати" S. Rep. No. 99-541, at 23.

Следователно грешка в закона не може да служи за защита по обвинение по Закона за подслушването; обвиняемият трябва да е възнамерявал да подслуша лична комуникация, но не е необходимо той или тя да е възнамерявал да нарушава законното си задължение да не подслушва. Виж *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 178-79 (5th Cir. 2000); *Reynolds v. Spears*, 93 F.3d 428, 435-36 (8th Cir. 1996) (където се поддържа становището, че осланянето на погрешен съвет на служител на правоприлагащ орган не е защита); *Williams v. Poulos*, 11 F.3d 271, 285 (1st Cir. 1993) (който отхвърля защита, основана на добросъвестност, където обвиняемият погрешно е мислел, че използването и разкриването са разрешени от закона); *Thompson v. Dulaney*, 970 F.2d 744, 749 (10th Cir. 1992) (където се отбелязва, че „може да се предполага, че обвиняемият познава закона); *Heggy v. Heggy*, 944 F.2d 1537, 1541-42 (10th Cir. 1991) (който отхвърля защита за „добросъвестност", построена въз основа на грешка на закона); *Narducci v. Village of Bellwood,* 444 F. Supp. 2d 924, 935 (N.D. Ill. 2006) (изискването за преднамереност „не изисква задължително наличието на намерение да се наруши законът или дори каквото и да е знание, че подслушването ще бъде незаконно").

По подобен начин „терминът „преднамерен" не загатва наличието на мотив". S. Rep. No. 99-541, at 24. Обвиняемите могат да бъдат в състояние да твърдят, че техните цели при незаконното подслушване на комуникации са били благородни, тъй като са били част от лично разследване на престъпление или нарушение. Такива цели са неприложими към психичното състояние. Виж *Gelbard v. United States,* 408 UPS. 41, 50 (1972) („По принцип

всички са съгласни, че използването на техники за телефонно или електронно подслушване от частни лица, които нямат разрешение за това, нямат оправдание, когато комуникациите се подслушват без съгласието на един от участниците."); *Townsend,* 987 F.2d at 931 („следователно дали обвиняемият има добри или лоши намерения при използването на автоматично записващо устройство, е безпредметно"); S. Rep. No. 99-541, at 24 („Хората, които крадат, защото обичат да го правят или за да се сдобият с повече пари или да нахранят бедните като Робин Худ, всички те извършват едно и също престъпление... Думата „преднамерено" описва психичното поведение, свързано с действие, което е направено с някаква цел. Това не предполага действието да е било извършено с определена злонамерена цел").

ПОДСЛУШВАНЕ

Законът за подслушването определя „подслушване" като слухово или по друг начин придобито съдържание на телефонна, електронна или устна комуникация посредством използването на електронно, механично или друго устройство. Глава 18 от Кодекса на САЩ U.S.C., параграф 2510(4). Въпреки че се състои от едва двадесетина думи, това определение е учудващо сложно. То използва не по-малко от пет термина, които са определени поотделно в параграф 2510 – „съдържание", „телефонна комуникация", „електронна комуникация", „устна комуникация" и „електронно, механично или друго устройство". Виж Глава 18 от Кодекса на САЩ, параграф 2510(8), (1), (12), (2) & (5). Всяко едно от тези понятия е достатъчно сложно, затова се разглеждат по-долу поотделно. Освен това по-голямата част от съдилищата са разчели в определението за „подслушване" изискване, което не се съдържа в текста на закона – че „придобиването на комуникацията" трябва да бъде „едновременно" с осъществяването на комуникацията.

„Слуховото или друго придобиване" на съдържанието на комуникацията се позовава на някаква „дейност, предприета по време на ... комуникацията, поради която комуникацията е подслушана от непоканени слушатели." *United States v. Turk,* 526 F.2d 654, 658 (5th Cir. 1976). Обикновено тази дейност е свързана с „вмешателство в установените средства на комуникация". *United States v. Campagnuolo,* 592 F.2d 852, 862 (5th Cir. 1979), quoting *United States v. Pasha,* 332 F.2d 193, 198 (7th Cir. 1964). Обвиняемият подслушва комуникация по силата на придобиването; не е необходимо обвиняемият също така да слуша или да чете комуникацията. *See Sanders v. Robert Bosch Corp.,* 38 F.3d 736, 740 (4th Cir. 1994) („самото записване на телефонен разговор представлява „слухово ... придобиване на този разговор"); *Walden v. City of Providence,* 495 F. Supp. 2d 245, 262 (D.R.I. 2007).

Съдът по делото *Turk* разгледа аргумента, че полицаи, които са намерили касетка със запис, направен от обвиняем за престъпление на негови собствени разговори, са „подслушвали" записания разговор всеки

път, когато са прослушвали касетата. Съдът отхвърля твърдението, че „подслушването“ изисква, най-малкото, участие в първоначалното използване на устройството едновременно с комуникацията за предаване или запазване на комуникацията.“ *Turk,* 526 F.2d at 658 n.3.

Така както касетката в *Turk* съдържа запис на телефонен разговор, компютрите могат да съдържат записи на електронни комуникации. За разлика от телефонните разговори, които първоначално Законът за подслушването защитава, електронните комуникации обикновено са под формата на текст. Компютърните системи, които обработват имейли, текстови съобщения, моментни съобщения, записват и пазят пълно копие от съдържанието на комуникацията. Това обикновено е внедрено в дизайна на системата: „всички съобщения се записват и пазят не защото някой „подслушва“ системата, а просто защото самата система работи по такъв начин.“ *Bohach v. City of Reno,* 932 F. Supp. 1232, 1234 (D. Nev. 1996). Самото получаване на копие от записана комуникация – имейл с едногодишна давност от сървъра например, не е непременно „подслушване“ на комуникация според Закона за подслушването.

При прилагането на *Turk* повечето съдилища поддържат становището, че телефонните и електронни комуникации са „подслушани“ по смисъла на Глава III само в случаите, когато такива комуникации са придобити по времето на тяхното излъчване. Дадено лице, което получава достъп до съхранено копие на комуникация, изоставено, след като комуникацията е постигнала предназначението си, не „подслушва“ комуникацията. Виж *e.g., Steve Jackson Games, Inc. v. United States Secret Service,* 36 F.3d 457, 460-63 (5th Cir. 1994) (достъп до съхранена електронна комуникация); *Fraser v. Nationwide Mut. Ins. Co.,* 352 F.3d 107, 113-14 (3d Cir. 2003) (същото); *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868, 87679 (9th Cir. 2002) (уебсайт); *United States v. Steiger,* 318 F.3d 1039, 1047-50 (11th Cir. 2003) (файлове, запазени в харддрайва); *United States v. Mercado-Nava,* 486 F. Supp. 2d 1271, 1279 (D. Kan. 2007) (телефонни номера, запазени в мобилен телефон); *United States v. Jones,* 451 F. Supp. 2d 71, 75 (D.D.C. 2006) (текстови съобщения);*United States v. Reyes,* 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (комуникации по пейджър); *Bohach,* 932 F. Supp. at 1235-36 (същото).

Въпреки това обаче Първият федерален апелативен съд намеква, че изискването за съ-временност, което бе разработено в епохата на телефонните подслушвания, „може би няма да бъде в състояние да се прилага към въпроси, свързани с прилагането на Закона за подслушването към електронните комуникации“. *United States v. Councilman,* 418 F.3d 67, 79-80 (1st Cir. 2005) (citing *In re Pharmatrak, Inc. Privacy Litigation,* 329 F.3d 9, 21 (1st Cir. 2003)); виж също *Potter v. Havlicek,* 2007 WL 539534, at *6-7 (S.D. Ohio Feb. 14, 2007) („голяма вероятност“, че Шестият федерален апелативен съд ще намери, че изискването за съ-временност не може да се приложи към електронните комуникации).

По делото *United States v. Szymuszkiewicz*, --- F.3d ----, 2010 WL 3503506 (7th Cir. 2010), Седмият федерален апелативен съд изразява становище че „в Закона за подслушването няма времево изискване и съдиите трябва да внасят добавки към законови дефиниции". Той заявява, че придобиването на запазено гласово съобщение попада в обсега на дефиницията на „подслушване" и че „според закона всяко придобиване на информация с използване на устройство е подслушване". Делото *Szymuszkiewicz* е съдебен процес за нарушаване на Закона за подслушване чрез прихващане на имейл. Съдебните заседатели решават, че уликата в това дело показва, че обвиняемият е прихванал имейла едновременно с неговото изпращане. В резултат на това въпреки *Szymuszkiewicz* препоръчително е в обвинителния акт прокурорите да се позовават върху нарушаване на Закона за подслушване само когато е налице изискването за съ-временност.

Съдиите обикновено не се задълбочават върху значението на термина „съ-временен". Точно колко близо дадено придобиване трябва да бъде по време до съответното излъчване, остава отворен въпрос. Ясно е, че съ-временен не може да означава „едновременен". Трудно можем да си представим, че Конгресът ще разграничи защитата си на комуникации по части от секундата, като ги защитава, докато те пътуват като електрически или оптически импулси по даден кабел, но след това веднага ще преустанови защитата в момента, в който те се запишат по какъвто и да е начин. Въпреки това обаче Единадесетият федерален апелативен съд предположи, че „съ-временен" следва да съвпада с комуникация „в полет". *Steiger,* 318 F.3d at 1050. Обратно, според Първия апелативен съд изискването за съ-временност може да бъде разчетено просто като средство да се изключат придобивания, „направени значително време след като материалът е бил въведен в електронно хранилище". *Pharmatrak, Inc. Privacy Litigation,* 329 F.3d 9, 21 (1st Cir. 2003).

Този въпрос възниква особено често в някои дела, свързани с подслушване на имейли. Имейлът лесно може да бъде прихванат от сървъра; някой, който може да конфигурира сървъра, може да го накара да запазва копия на писма, свързани с даден акаунт. Например в делото *United States v. Councilman*, 373 F.3d 197 в обвинителния акт се твърди, че преди имейлите да се доставят на потребителите, софтуерната програма на обвиняемия ги е копирала от сървърите, които са били поставени, за да предадат съобщенията. Обвинението поддържа тезата, че това е нарушение на Закона за подслушването. Двама от тримата съдии заявяват, че имейл съобщения, получени от случайна памет за достъп на компютър или харддиск, не са прихванати „съ-временно с излъчването. Първият апелативен съд оборва решението с твърдението, че имейл в „електронно хранилище" – законодателен термин, означаващ „временно, междинно хранилище", виж Глава 18 от Кодекса на САЩ U.S.C., параграф 2510(17) – може да попадне под Закона за подслушването. Виж *United States v. Councilman,* 418 F.3d 67 (1st Cir. 2005) (en banc).

На практика прокурорите следва да решат дали елементът на „съ-временност“ е приложим. Когато даден обвиняем се е намесил в начина, по който компютърната система обработва получавани или изпращани съобщения, като е направил така, че копия от тях да бъдат съхранявани или препращани до него приблизително по същото време, когато компютърът ги обработва, тогава може да се твърди, че изискването за съ-временност е било удовлетворено. Обаче ако обвиняемият само е проникнал в компютърна система и е получил съхранени отпреди копия от съобщение, тогава е възможно обвиняемият да не е нарушил Закона за подслушването. Вместо това прокурорите следва да обмислят възможността да повдигнат обвинения по Глава 18, Кодекс на САЩ, параграф 1030(a)(2), които забраняват достъпа до защитен компютър и получаването на информация, или по по-рядко използвания параграф 2701 от Глава 18 от Кодекса на САЩ, който забранява достъпа до някои комуникации, които се намират на компютрите на доставчика на електронни комуникационни услуги.

СЪДЪРЖАНИЕ НА КОМУНИКАЦИЯТА

За да бъде подслушване, придобивката трябва да бъде съдържанието на комуникацията. Глава 18 Кодекс на САЩ, параграф 2510(4). „Терминът „съдържание“, когато е използван във връзка с телефонна, устна или електронна комуникация, включва всяка информация, отнасяща се до същността, предназначението или значението на тази комуникация.“ Глава 18 от Кодекса на САЩ, параграф 2510(8). Конгресът внесе поправки в закона през 1986 г., „за да изключи от определението на термина „съдържание“ самоличността на страните или самото съществуване на комуникацията“. Затова узнаването на факта на съществуването на или знанието за това кой комуникира, не е подслушване на комуникация. Получаването на тази не-съдържателна информация за дадена комуникация може да бъде престъпно нарушаване забраната за подслушване и регистрация и устройствата за прихващане и проследяване. Виж Глава 18, Кодекс на САЩ, параграф 3121(d).

Някои типове информация, свързана с мрежови комуникации като айпи адреси и интернет протоколи, могат да възбудят спор дали изобщо имат съдържание. В случай че прокурорите имат съмнения дали определена информация представлява „съдържание“ според Закона за подслушването, следва да се обърнат към Отдела за компютърни престъпления и интелектуална собственост на Департамента по правосъдие.

ТЕЛЕФОННА, УСТНА ИЛИ ЕЛЕКТРОННА КОМУНИКАЦИЯ

Законът за подслушването забранява подслушването на „каквато и да е жична, устна или електронна комуникация.“ Глава 18 от Кодекса на САЩ, параграф 2511(1)(a). Това са три различни класификации на комуникации,

всяка една със законово установена дефиниция. „Жични“ комуникации отговарят най-общо на традиционните телефонни разговори: тези, които улавят човешкия глас, пренесен чрез жични или други подобни системи за комуникация. Виж Глава 18 от Кодекса на САЩ, параграф 2510(1), (18). „Устни“ комуникации са гласови комуникации, осъществени от хора насаме. Виж Глава 18 от Кодекса на САЩ, параграф 2510(2); *Doe v. Smith*, 429 F.3d 706, 709 (7th Cir. 2005) (забрана за подслушване на устни комуникации включва саундтрака на видео материал). „Електронни“ комуникации са всеки друг тип комуникация, осъществена с използването на електронния спектър, включително компютърни мрежови комуникации, които не съдържат човешки глас. Виж Глава 18 от Кодекса на САЩ, параграф 2510(12); S. Rep. 99-541, at 14 („Като общо правило комуникацията е електронна комуникация, защитена от федералния закон за подслушването, ако не е осъществена чрез звукови вълни, и не може да бъде определена като съдържаща човешки глас.“)

И двете дефиниции на „жична комуникация“ и „електронна комуникация“ изискват „комуникацията“ да бъде изпратена с помощта на устройство или система, която оказва влияние върху общуването с различните щати или с чужбина. Въпреки че това не изисква комуникацията в действителност да пътува между щатите, то изключва някои чисто локални комуникации. Например „устройство за вътрешна комуникация, което физически прилича на телефонен апарат“, което се използва, за да даде възможност на затворниците да контактуват с посетителите, не отговаря на изискванията, тъй като „не е свързано с устройство, способно да осъществи комуникации между различните щати или държави. *United States v. Peoples,* 250 F.3d 630, 636 (8th Cir. 2001). Интернет лесно покрива дефиницията за устройство или система, която оказва влияние върху междущатското или междудържавното общуване. *See United States v. Sutcliffe,* 505 F.3d 944, 952-53 (9th Cir. 2007) (Както по отношение на средствата за общуване, така и на метода, посредством който се осъществява обменът, интернет е инструмент и канал за междущатски обмен“.)

Най-малко в един окръжен съд невъзможността да се установи междущатски аспект на устройствата е довела до оправдателна присъда по обвинение по Глава III. Виж *United States v. Jones*, 580 F.2d 219 (6th Cir. 1978). В отговор Петият федерален апелативен съд излиза със становище, че тривиалното доказателство за кода на телефонния номер е достатъчно, за да се установи междущатската връзка. Виж *United States v. Lentz*, 624 F.2d 1280, 1285-86 (5th Cir. 1980); *Виж също United States v. Burroughs*, 564 F.2d 1111, 1115 (4th Cir. 1977) (as to, параграф 2511(1)(a), („най-съществениият елемент по време на процеса е да се установи база за прилагане на федералното законодателство“).

Понякога обвиняемите се опитват да твърдят, че комуникацията, която са подслушали, не отговаря на изискването за междущатски обмен, тъй като определената част от комуникацията, която са подслушали, се е провела вътре в щата. Например един обвиняем твърдял, че неговото

устройство, което прихващало трансфери между клавиатура и компютър, не е прихващало електронна комуникация. *United States v. Ropp,* 347 F. Supp. 2d 831 (C.D. Cal. 2004). В делото *Ropp* обвиняемият поставил хардуерно устройство между компютъра на жертвата и нейната клавиатура, което записвало протичащите между тях сигнали. Съдът отхвърлил обвиненията за нарушаване на параграф 2511, защото решил, че комуникациите, които обвиняемият е прихванал, не са „електронни комуникации" по смисъла на закона. Съдът постановил, че „въпросните комуникации са свързани с подготовката на имейли и други комуникации по времето на подслушването". Тъй като съдът решил, че писането на машина е комуникация „със собствения компютър на жертвата", той се обосновал, че „по време на подслушването комуникациите са имали връзка с междущатския обмен толкова, колкото и писмо, запечатано в плик с марка, но което все още не е изпратено по пощата".

Независимо от решението по делото *Ropp* прокурорите трябва да продължават да водят дела, свързани с подслушвания, осъществявани върху компютри или вътрешни мрежи, които се отразяват върху междущатския обмен. Например ако даден индивид инсталира зловреден софтуер на компютъра на жертвата, който прави незаконно копие всеки път, когато се изпрати имейл, или прихваща такива съобщения, докато те пътуват по локалната мрежа към крайната си дестинация някъде по света, такива дела могат да бъдат преследвани по параграф 2511.

Текстът на параграф 2511 и законодателната история на закона подкрепят тази интерпретация. Трансферът трябва да включва целия пренос на комуникацията от подателя до получателя. Самият текст на дефиницията „електронна комуникация" е несъвместим с подхода на парче. Дефиницията изрично предполага, че „трансферът" може да бъде пренесен от системата „в цялост или частично". Ако „трансфер" е трябвало да означава всяко препредаване между компоненти по пътя на комуникацията от подателя до получателя, никоя система не би могла да осъществи трансфера.

Освен това законодателната история на поправките от 1986 г., които добавиха термина „електронна комуникация", дава полезно обяснение. В доклада на Конгреса изрично се казва: „доколкото електронните и жични комуникации, преминаващи през устройството на потребителя, се отразяват върху междущатския обмен, Комисията смята, че тези комуникации следва да бъдат защитени по параграф 2511". По подобен начин докладът на Сената разглежда включването на комуникации по частни мрежи и вътрешномрежови комуникационни системи. В тези разисквания Конгресът изрично отхвърля предпоставката, че придобиването на комуникация на собственото устройство на потребителя го поставя извън защитите на Закона за подслушването.

ИЗПОЛЗВАНЕ НА ПРИСПОСОБЛЕНИЕ

По смисъла на Закона за подслушването „подслушването" трябва да се осъществи със средствата на „електронно, механично или друго приспособление". Глава 18 от Кодекса на САЩ, параграф 2510(4). Обикновено „електронно, механично или друго приспособление" означава всяко приспособление или апаратура, която може да се използва, за да се подслушва жична, устна или електронна комуникация" с две изключения, разгледани по-долу. Глава 18 от Кодекса на САЩ, параграф 2510(5). Въпреки че езикът на „устройството" не се съдържа в самия раздел 2511(1)(а), а в дефиницията на „подслушване", някои съдилища са го третирали като независим елемент на нарушаване на раздел 2511(1)(а). Виж *United States v. Duncan,* 598 F.2d 839, 847 (4th Cir. 1979); *United States v. Harpel,* 493 F.2d 346, 351 (10th Cir. 1974).

Конгресът включва изискването за „приспособление" в закона, за да постави извън обхвата му обикновеното, неподпомогнато използване на естествените човешки сетива за получаване на съдържанието на комуникацията. Тъй като Законът за подслушването защитава не само жичните и електронните, но също така и „устните" комуникации – комуникация, „изречена от човек" при основателно очакване за поверителност, Конгресът се опитва да дефинира „подслушване" по начин, който да не инкриминира неволното дочуване на частен разговор. Когато се подслушват жични или електронни комуникации, използването на „приспособление" се подразбира; просто няма начин да се придобие съдържанието на радио съобщение, без да се използва радио, или да се придобие съдържанието на съобщение в компютърната мрежа без наличието на компютър. В типично компютърно престъпление „приспособлението" представлява компютър, който се използва да се подслушва комуникацията или софтуерна програма, качена на компютър. И двете задоволяват изискванията по закона. Виж Глава 18 от Кодекса на САЩ, параграф 2510(5); *cf. MetroGoldwyn-Mayer Studios Inc. v. Grokster, Ltd.,* 545 U.S. 913, 940 (2005).

В дефиницията си за „приспособление" законът изключва три категории от своя обхват. *See Adams v. City of Battle Creek,* 250 F.3d 980, 983 (6th Cir. 2001) (където „друг освен" се интерпретира в дефиниция като „изключващ"). Законът изключва „слухов апарат или друго подобно приспособление, чието предназначение е да коригира влошения слух до степен не по-висока от нормалната". Глава 18, Кодекс на САЩ, параграф 2510(5)(b). Това изключение е в подкрепа на целта на Конгреса да не инкриминира използването на човешкия слух.

Освен това законът създава две „обичайни за воденето на бизнес" изключения от съдебна отговорност за подслушване в раздел 2510(а).

Изключение „телефонен дериват"

Първият цитат от тези изключения гласи:

Всеки телефонен или телеграфен апарат, съоръжение или устройство или техен компонент ... доставен на абоната или на потребителя от доставчик на жична или електронна комуникационна услуга в обичайния ход на бизнеса му, и който се използва от абоната или потребителя в обичайния ход на бизнеса му или доставен от такъв абонат или потребител за достъп до улесненията на такава услуга и използван в обичайния ход на бизнеса му. Глава 18, Кодекс на САЩ, параграф 2510(5) (а)(i).

Подточка (I) изключва от обхвата на закона използването на основни, всекидневни устройства, които повечето хора използват, като например собствения телефон на абоната. Тези „не-приспособления" трябва да бъдат използвани от абоната или потребителя, а не от външно лице. (Думата „потребител" е дефинирана в параграф 2510(13) и означава някой, който е бил „надлежно упълномощен" от доставчика да използва услугата му). Освен това те трябва да бъдат „доставени" или от доставчика „в обичайния ход на бизнеса", или от „абоната или потребителя". Ако го нямаше това изключение, даден човек, който използва телефона, за да говори с някого, би се въвлякъл в „подслушване" на собствения си разговор, тъй като „добива" неговото „съдържание", като използва „приспособление; това изключение заличава собствения телефон на абоната от дефиницията за „приспособление". (Дори в отсъствието на такова изключение такова „подслушване" най-вероятно би се оказало законно според изключението за съгласие, разгледано по-долу.)

Изключението в раздел 2510(5)(а)(i) понякога се нарича изключение „телефонен дериват" поради редица телефонни дела, в които участниците използват деривати (което означава допълнителен телефон, свързан със същата линия), за да подслушват разговорите на други хора. Изключението „телефонен дериват" ясно казва, че когато телефонна компания предостави на работодател дериват за законни, свързани с работата цели, когато работодателят наблюдава как служителите използват деривата за законни, свързани с работата цели, той не нарушава Глава III. Виж *Briggs v. American Air Filter Co.*, 630 F.2d 414, 418 (5th Cir. 1980) (преглед на законодателната история на Глава III); *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983) (прилагане на изключение, за да се разреши наблюдение на търговски представители); *James v. Newspaper Agency Corp.*, 591 F.2d 579, 581 (10th Cir. 1979) (прилагане на изключение за проследяване на разговорите на вестникарски служители с клиенти).

Съдебната практика обаче е разделена в интерпретацията си на изключението телефонен дериват, което се дължи на неопределеността на изречението „обичаен ход на бизнеса". Някои съдилища го интерпретират в широк смисъл като „в обхвата на законния интерес на дадено лице" и са прилагали изключението телефонен дериват в такива контексти като се-

мейни спорове. Виж *Simpson v. Simpson*, 490 F.2d 803, 809 (5th Cir. 1974) (съпругът не е нарушил Глава III, като е записвал телефонните разговори на жена си), *cert. denied*, 419 U.S. 897 (1974); *Anonymous v. Anonymous*, 558 F.2d 677, 678-79 (2d Cir. 1977) (съпругът не е нарушил Глава III, като е записвал разговорите на жена си с дъщеря им, поставена под негова опека). Други съдилища отхвърлиха това широко тълкуване и изрично или мълчаливо изключиха нелегалната дейност от поведение в рамките на „обичайния ход на бизнеса". Виж *Glazner v. Glazner,* 347; *Adams,* 250 F.3d at 984 („наблюдението в обичайния ход на бизнеса изисква лицето или лицата, които са обект на наблюдение, да бъдат предупредени); *Kempf v. Kempf*, 868 F.2d 970, 973 (8th Cir. 1989). (Глава III забранява всякакви дейности, свързани с подслушване, освен в случаите, когато това е специално упоменато, а в Закона няма никакво изключение за подслушване между съпрузи); *United States v. Harpel*, 493 F.2d 346, 351 (10th Cir. 1974) („Ние смятаме в духа на правото, че телефонен дериват, който е използван без упълномощаване или съгласие за нелегално записване на частен телефонен разговор, не е употребен в обичайния ход на бизнеса"); *Pritchard v. Pritchard*, 732 F.2d 372, 374 (4th Cir. 1984) (отхвърля гледището, че параграф 2510(5)(a) изключва подслушването между съпрузи от наказателна отговорност по Глава III).

Политиката на Департамента по правосъдие е да предпочита съдебното преследване на незаконно подслушване, свързано с домашни спорове, да се извършва на местно ниво, тъй като такива дела имат по-малък федерален интерес. Виж Наръчник на прокурорите на САЩ, 9-60.202.

Освен тези неопределености, които възникват от дефиницията на приспособление, изобщо не е ясно как това изключение ще се пренесе в контекста на престъпленията в мрежа. Това изключение се отнася само до „телефонен или телеграфен апарат, съоръжение или устройство...". Глава 18 от Кодекса на САЩ, параграф 2510(5)(a)(i). Докато компютрите могат да бъдат приети за съоръжения или устройства, все още не е установено дали „телефонен или телеграфен" определя всичките три типа обекти.

Изключение „обичаен ход на бизнеса"

Второто изключение „в обичайния ход на бизнеса" в раздел 2510(5)(a) гласи:

> *Всеки телефонен или телеграфен апарат, съоръжение или устройство или техен компонент ... използван от доставчик на жична или електронна комуникационна услуга в обичайния ход на бизнеса му или от служител на разследващите или правоприлагащите органи в обичайния ход на задълженията му. Глава 18, Кодекс на САЩ, параграф 2510(5)(a)(i)(i)*

Втората клауза на това изключение се прилага към записването на телефонни разговори на затворници в затвора, когато е направено в съответствие със заявена политика. Виж *United States v. Lewis,* 406 F.3d 11, 18 (1st Cir. 2005); *United States v. Hammond*, 286 F.3d 189, 192 (4th Cir. 2002) (където се прави заключението, че рутинното записване на разговори от затвора попада в обсега на изключението); *United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996). Обаче съдът е прилагал това изключение само при няколко други обстоятелства. Въпреки привидно широкия обсег на фразата „обичайния ход на задълженията си" съдилищата заключават, че „фактът, че даден индивид е служител на разследващ или правоприлагащ орган, не означава, че цялата следователска дейност попада в обичайния ход на задълженията му". И наистина, предпоставката на Глава III е, че няма нищо „обичайно" относно използването на приспособление с цел подслушването на комуникации с разследващи цели. Както обяснява върховният съдия Познер:

„Разследването е в рамките на обичайния ход на правоналагането, така че ако „обичаен" се възприема буквално, много рядко, ако не и никога нямаше да се изискват съдебни заповеди за електронно подслушване, каквото очевидно не е било намерението на Конгреса. Тъй като целта на закона първоначално е била да се регулира телефонното подслушване и други форми на електронно следене за целите на разследването, „обичаен" не трябва да се интерпретира толкова широко; по-разумно е да се тълкува като термин, отнасящ се до рутинен, несвързан с разследването запис на телефонен разговор… Такъв запис едва ли може да нарушава много личното пространство и по тази причина доближава изключението за обичаен ход до изключението за съгласие: което е обичайно, следва да се знае; то представлява косвено предизвестие". *Amati v. City of Woodstock*, 176 F.3d 952, 955 (7th Cir. 1999).

Не всички записи от затвора могат да бъдат подведени под това изключение. Само онези, направени от „служител на разследващ или правоприлагащ орган", отговарят на изискванията. Този термин, дефиниран в раздел 25109(7), се отнася само до лица, „овластени от закона да провеждат разследвания или да осъществяват арести" по законите за специални престъпления, изброени в раздел 2516. Тази категория включва служителите във федералните затвори. Виж *Lewis,* 406 F.3d, 16. Второ, за да може запис от затвора да бъде причислен към „обичайния ход на неговите задължения", този телефонен запис не трябва изрично да бъде записан за целите на разследването. Например това изключение е неприложимо, когато затворът изрично дава възможност на затворника „да проведе телефонен разговор … така че той да може да бъде контролиран", и прилага техника за запис, която обикновено не се използва в затвора. *Campiti v. Walonis,* 611 F.2d 387, 392 (1st Cir. 1979).

2. РАЗКРИВАНЕ НА ПОДСЛУШАНА КОМУНИКАЦИЯ: ГЛАВА 18, КОДЕКС НА САЩ, 2511(1)(C)

Законът за подслушването също така забранява преднамереното оповестяване на комуникации, за които се знае, че са били подслушани незаконно. Глава 18, Кодекс на САЩ, параграф 2511(1)(c).

Глава 18, Кодекс на САЩ, 2511(1)(c) гласи:

Освен в случаите, изрично упоменати в тази глава, всеки, който –

.....

преднамерено оповести или се опита да оповести на друго лице съдържанието на каквато и да е жична, устна или електронна комуникация, когато знае или има основание да знае, че тази информация е получена чрез подслушване на жична, устна или електронна комуникация в нарушение на този подраздел...

ще бъде наказан съобразно разпоредбите на подраздел (4).

РАЗКРИВАНЕ

Текстът на закона забранява разкриването на действителното съдържание на комуникацията. Освен това някои съдилища поддържат тезата, че законът забранява разкриването на „естеството“ на комуникацията. Виж *Deal v. Spears*, 780 F. Supp. 618, 624 (W.D. Ark. 1991), *aff'd*, 980 F.2d 1153 (8th Cir. 1992). Обаче разкриване на самия факт, че се е провело нелегално подслушване, не е нарушение на забраната за разкриване на съдържанието на подслушани комуникации. Виж *Fultz v. Gilliam*, 942 F.2d 396, 403 (6th Cir. 1991). Освен това разкриването на съдържанието на подслушана комуникация, която вече е станала „публична“ или „широко известна“, не е забранено. Виж S. Rep. No. 90-1097 (1968), преиздадено в 1968 U.S.C.C.A.N. 2112, 2181; *Bartnicki v. Vopper,* 532 U.S. 514, 546 (2001) („Човек не може да „разкрива“ нещо, което вече е публично достояние“).

Разкриването трябва да бъде направено пред „всяко друго лице“. С други думи, разкриването трябва да бъде пред „трета страна“, различна от лицето, осъществило подслушването или от участниците в подслушаната комуникация. Виж *Lanier v. Bryant,* 332 F.3d 999, 1005 (6th Cir. 2003) (разкриване пред подслушаната страна или нейния адвокат не е забранено от 2511(1)(c)).

ПСИХИЧЕСКО СЪСТОЯНИЕ

Раздел 2511(1)(c) има две изисквания за психично състояние.

Актът на разкриването на комуникацията трябва да бъде направен „умишлено". Това е същото изискване за психично състояние, което бе разгледано по-горе във връзка с раздел 2511(1)(a).

Обвинението също така трябва да докаже, че разкриващият индивид е знаел или е имал основание да знае, че „информацията е получена вследствие на подслушване на жична, устна или електронна комуникация в нарушение на този подраздел". Глава 18, Кодекс на САЩ, параграф 2511(1)(c). Така че в наказателно дело за разкриване „знанието или основанието да се знае за незаконността, е елемент". *United States v. Wuliger,* 981 F.2d 1497, 1501 (6th Cir. 1992); виж също *Forsyth v. Barr,* 19 F.3d 1527, 1538 (5th Cir. 1994) (където се иска доказателство, че „обвиняемият е знаел или е трябвало да знае, че подслушването е било незаконно"). Тъй като законът споменава „основание да знае" за незаконността, грешка на закона не е база за защита; обвинението трябва да покаже само, че обвиняемият знае съответните факти, а не че обвиняемият разбира Закона за подслушването достатъчно добре, за да знае, че подслушването е било незаконно. Виж *Wuliger*, 981 F.2d at 1501; виж също *Williams v. Poulos*, 11 F.3d 271, 284-85 (1st Cir. 1993). Въпреки това обаче прокурорът трябва да бъде подготвен да обори всяко твърдение, че обвиняемият е сгрешил относно който и да е факт, който би разрешил подслушването.

НЕЗАКОННО ПОДСЛУШВАНЕ НА КОМУНИКАЦИЯ

Въпреки че не е необходимо обвиняемият да бъде същият индивид, който е подслушал комуникацията, в повечето случаи обвинението трябва да докаже, че някой е подслушал поверителна комуникация в нарушение на раздел 2511(1)(a). Ако обвиняемият едновременно е подслушал и разкрил комуникация, би било уместно да бъде обвинен по два състава – за подслушване и за разкриване.

Един съд обаче изразява становище, че разкриването на комуникация може да бъде незаконно дори когато подслушването не е било. Раздел 2511(1)(c) изисква разкритата информация да бъде придобита посредством подслушване, което е „в нарушение на *този* подраздел"). По делото In *Cafarelli v. Yancy,* 226 F.3d 492 (6th Cir. 2000) становището на Шестия федерален апелативен съд е, че въпреки че раздел 2511(2)(g)(ii)(II) разрешава „подслушването" на някои радио комуникации, той не разрешава също така тяхното „разкриване". Въпреки че раздел 2511(2) разрешава подслушването, съдът тълкува, че позоваването на „този подраздел" в 2511(1)(c) изключва действието на многото изключения, съдържащи се в 2511(2). По такъв начин забраната за „разкриване", съдържаща се в 2511(1)(c), е нарушена, въпреки че подслушването е било законно. Въпреки това обаче други съдилища са

се произнасяли по различен начин. Виж *United States v. Gass,* 936 F. Supp. 810, 816 (N.D. Okla. 1996) („След като не представлява нарушение по смисъла на параграф 2511 да се подслушват лесно достъпни правителствени радио комуникации, параграф 2511(1)(c) и (d) не забраняват разпространяването или използването на такива комуникации").

Докладът на Сената подсказва допълнително изключение към общото правило, че раздел 2511(1)(a) е нарушен. Ако дадена комуникация се подслушва, но подслушването не нарушава 2511(1)(a) само защото не е било преднамерено, Докладът на Сената заявява, че използването или разкриването на комуникацията все пак нарушава Закона за подслушването. Виж S. Rep. No. 99-541, at 25 (1986), 1968 U.S.C.C.A.N. 3555, 3579.

ВЪПРОСИ, ВЪЗНИКВАЩИ ВЪВ ВРЪЗКА С ПЪРВАТА ПОПРАВКА

Първата поправка възпрепятства прилагането на раздел 2511(1)(c) към разкриването на информация от обществен интерес от трета страна, която не участва в подслушването, когато третата страна няма друго задължение да пази информацията поверителна. Виж *Bartnicki v. Vopper*, 532 U.S. 514 (2001); виж също *Jean v. Massachusetts State Police,* 492 F.3d 24, 33 (1st Cir. 2007). В делото *Bartnicki* няколко новинарски организации получават запис на телефонен разговор, който би трябвало да знаят, че е бил незаконно подслушан. Делото е свързано с въпроса за имунитет срещу нормативно наложена гражданска отговорност, обаче същите принципи на Първата поправка се прилагат и към наказателната отговорност. Върховният съд излиза със становище, че разкриванията, направени от новинарските агенции, не са незаконни.

Въпреки че *Bartnicki* показва, че Първата поправка наистина ограничава прилагането на раздел 2511(1)(c), подкрепящите становища подсказват, че тези граници са много тесни. Например даден обвиняем няма да бъде освободен от съдебно преследване само защото разкрива информация от интерес за обществото. Двама от шестимата върховни съдии в делото *Bartnicki* пишат отделни становища, което показва, че по-голямата част от Съда отхвърля изключението „обществен интерес" в Закона за подслушването. Виж *Bartnicki*, 532 U.S. at 540 (Breyer, J., concurring).

Като подкрепя решението по делото *Bartnicki,* съдия Брейър, към когото се присъединява и съдия О'Конър, се съгласява, че интересите за поверителност, защитени в раздел 2511(1)(c), трябва да бъдат балансирани срещу медийната свобода, кодифицирана в Първата поправка. Съдия Брейър пише отделно, за да подчертае някои факти, които той намира за напълно уместни в представения случай. В частност той подчертава, че „говорещите са имали малък или никакъв *легитимен* интерес да запазят поверителността на този определен разговор". Съдия Брейър обосновава това заключение с три фактора: (1) съдържанието на комуникацията, (2) обществения статут на говорещия и (3) метода, посредством който

е осъществена комуникацията. Според съдия Брейър подслушаната комуникация е свързана със заплахи за нараняване на други хора, които традиционно законът смята, че нямат право да останат поверителни. Нещо повече, съдия Брейър заключава, че говорещите са „обществени фигури с ограничена власт". На последно място, разговарящите са избрали да комуникират по несигурен метод според съдия Брейър, по некриптирани мобилни телефони. Подслушването на разговор по обикновен мобилен телефон на улицата (което мнозина от говорещите, изглежда, приемат) е много различно нещо от подслушването на разговори, които се провеждат по криптиран мобилен телефон или в спалнята.

Въпреки че прокурорите следва да са наясно с ограниченията, наложени от Първата поправка в *Bartnicki,* позоваването на Първата поправка вероятно рядко ще се случва. В делото *Bartnicki* Върховният съд умишлено не засяга случаи, когато (1) разкриващата страна нарушава по някакъв начин закона, за да придобие информацията, или (2) разкриването е свързано с „търговски тайни или домашни клюки или друга информация от чисто частен характер". Освен това ограниченията, въведени от *Bartnicki,* не се прилагат към съдебни производства по раздел 2511(1)(d) за използване на незаконно подслушана комуникация, което Върховният съд изрично характеризира като регулация на поведението, а не на словото.

Първата поправка не дава на медиите автоматична защита срещу нарушения на Закона за подслушването. Ако това не е ясно поради предпазливостта, с която Върховният съд ограничи изключението в *Bartnicki,* редица съдилища ясно поддържат това становище. Виж *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158 (5th Cir. 2000); *Sussman v. American Broadcasting Companies, Inc.*, 186 F.3d 1200 (9th Cir. 1999); *Vasquez-Santos v. El Mundo Broad. Corp.*, 219 F. Supp. 2d 221, 228 (D.P.R. 2002) (отхвърля изключение за нарушение на Закона за подслушването за подслушвания, които са свързани със закононарушения в медийно разследване).

Следователно не всеки, „който законно е получил вярна информация от обществена значимост, има право според Първата поправка да разкрие тази информация". *Boehner v. McDermott,* 484 F.3d 573, 577 (D.C. Cir. 2007). В делото *Boehner* Джим Макдермот, член на Конгреса и на Етичната комисия, получава запис на незаконно подслушан телефонен разговор, в който участва Джон Бенър, също член на Конгреса. Макдермот разкрива съдържанието на записа пред медиите. Съдията решава, че Макдермот няма право според Първата поправка да разкрива записа, тъй като Макдермот е обект на правило на Комисията, което забранява разкриването на каквато и да е улика, свързана с разследване на когото и да е извън Комисията.

3. ИЗПОЛЗВАНЕ НА ПОДСЛУШАНА КОМУНИКАЦИЯ: ГЛАВА 18, КОДЕКС НА САЩ, ПАРАГРАФ 2511(1)(D)

Подобно на нарушение на подраздел (1)(c), обвинение по раздел 2511(1)(d) има три елемента. Първите два елемента са същите, както в раздел 2511(1)(c), и поставят същите въпроси като разгледаните по-горе.

Глава 18 от Кодекса на САЩ, раздел 2511(1)(d) гласи:

Освен в случаите, когато изрично е упоменато друго, всяко лице, което –

.....

преднамерено използва или възнамерява да използва съдържанието на каквато и да е жична, устна или електронна комуникация, като знае или като има основание да знае, че информацията е получена посредством подслушване на жична, устна или електронна комуникация в нарушение на този подраздел ...

ще бъде наказано според разпоредбите в подраздел (4).

ИЗПОЛЗВАНЕ НА СЪДЪРЖАНИЕ

На пръв поглед „използване на съдържанието“ на подслушаната комуникация изглежда изключително широко понятие. Въпреки това обаче „използване“ изисква някакво „активно прилагане на съдържанието на незаконно подслушана информация с някаква цел“. *Peavy v. Harman*, 37 F. Supp. 2d 495, 513 (N.D. Tex. 1999), *aff'd in part and rev'd in part*, 221 F.3d 258 (5th Cir. 2000). По подобен начин „използване“ не включва само простото слушане на подслушани разговори. Виж *Dorris v. Absher*, 179 F.3d 420, 426 (6th Cir. 1999); *Reynolds v. Spears*, 93 F.3d 428, 432-33 (8th Cir. 1996); *Fields v. Atchison, Topeka and Santa Fe Ry. Co.*, 985 F. Supp. 1308 (D. Kan. 1997), *withdrawn in part*, 5 F. Supp. 2d (D. Kan 1998). Обаче виж *Thompson v. Dulaney*, 838 F. Supp. 1535, 1547 (D. Utah 1993) (където слушането е използване).

Тъй като забраната за „използване“ регулира по-скоро поведението, отколкото словото, може да се стигне до дела, които по друг начин би било трудно да се преследват по съдебен ред поради затруднения, свързани с Първата поправка. Виж *Boehner v. McDermott,* 484 F.3d 573, 583-84 (D.C. Cir. 2007) (където се въвежда разграничение между забрана върху словото и забрана върху използване на информация). Например по едно дело съдът постановява, че заплахата за разкриване с цел да се повлияе на някого е „използване“. В контекста на мрежата други употреби могат да включват използването на прихванати пароли за получаване на достъп до други ком-

пютри или използването на подслушана поверителна бизнес информация за получаване на търговско предимство. *See Leach v. Bryam*, 68 F. Supp. 2d 1072 (D. Minn. 1999).

4. НОРМАТИВНИ ИЗКЛЮЧЕНИЯ И ЗАЩИТИ

Законът за подслушването въвежда обширни забрани в подраздел 2511(1), но също така и много изключения в подраздел 2511(2). Прокурорът трябва да реши дали тези изключения се отнасят до конкретното дело, преди да внесе обвинителен акт по Закона за подслушването.

Всяко от изключенията в подраздел 2511(2) е положителна защита, а не елемент на престъпление. Виж *United States v. McCann,* 465 F.2d 147, 162 (5th Cir. 1972); *United States v. Harpel,* 493 F.2d 346 (10th Cir. 1974). Тъй като става дума за положителни защити, няма нужда правителството да ги отрича в обвинителния документ, виж *United States v. Sisson,* 399 U.S. 267, 288 (1970); *McCann,* 465 F.2d at 162, обвиняемият има право на инструктаж на съдебните заседатели само ако теорията е подкрепена с доказателство, виж *United States v. Ricketts,* 317 F.3d 540 (6th Cir. 2003), а на обвиняемия е вменена доказателствената тежест в процеса.

Изключенията, които са особено приложими в контекста на престъпленията в мрежа, са разгледани по-долу.

СЪГЛАСИЕ НА СТРАНАТА

Дадено подслушване е законно, ако подслушващият е страна в комуникацията или ако една от страните в комуникацията се съгласи с подслушването. Два подраздела на раздел 2511(2) формулират това изключение. Подраздел 2511(2) дава право на „лице, действащо под шапката на закона“, да подслушва комуникация при съгласие:

> *Няма да бъде незаконно по тази глава лице, действащо под шапката на закона, да подслуша жична, устна или електронна комуникация, когато това лице е страна в разговора или когато една от страните в разговора е дала предварително съгласие за такова подслушване.*
>
> *Глава 18, Кодекс на САЩ, параграф 2511(2)(c).*

Раздел 2511(2)(d) използва почти същия език, за да позволи на лице, което *не* действа „под шапката на закона“, да подслушва разговор при наличието на съгласие, но формулира и изключение-на-изключението: подслушването е незаконно, ако „такава комуникация е подслушана с цел извършването на каквато и да е престъпен или незаконен акт в нарушение

на Конституцията на САЩ или на който и да е щат". Глава 18, Кодекс на САЩ, параграф 2511(2)(d).

Изключенията за съгласие в параграфи 2511(2)(c) и (d) са вероятно най-често цитираните изключения на общата забрана на Закона за подслушването за подслушване на комуникации.

Страна в комуникацията

Докладът на Сената относно Закона за подслушването определя „страна" като „лицето, което всъщност участва в комуникацията". S. Rep. No. 90-1097 (1968), препечатана в 1968 U.S.C.C.A.N. 2112, 2182. По такъв начин съпругът не може да се „съгласи" да подслушва телефонните разговори на съпругата си с други хора, проведени от домашния съпружески телефон. *Simpson v. Simpson,* 490 F.2d 803, 805 n.3 (5th Cir. 1974). Въпреки това обаче, когато електронни комуникации се правят с използването на сървърен компютър, някои съдилища са били на мнение, че компанията, която притежава сървъра, е „страна" в комуникации, изпратени към тези компютри, и е способна на съгласие. Виж *United States v. Mullins,* 992 F.2d 1472, 1478 (9th Cir. 1993) (компания, която притежава компютър, с който е комуникирано, е „една от страните в комуникацията"); *United States v. Seidlitz,* 589 F.2d 152, 158 (4th Cir. 1978) (компания, „която наема, подслонява, програмира и поддържа компютрите и е абонат на съответните телефонни номера, е според всички намерения и цели страна в комуникацията, започната от обвиняемия").

Индивидите са страна в комуникация, когато към тях се отправят послания дори когато те не отговарят, *United States v. Pasha*, 332 F.2d 193 (7th Cir. 1964) (полицай, който отговаря по телефона по време на изпълнение на съдебна заповед в игрален дом, е част от заявките за залагания) и дори ако лъжат относно самоличността си, *United States v. Campagnuolo*, 592 F.2d 852, 863 (5th Cir. 1979) (полицай, който отговаря по телефона в игрален дом и претендира, че е обвиняемият, е страна). Поне в един съдебен процес като че ли е бил възприет по-широк подход със становището, че някой, чието присъствие е известно на комуникиращите, може да бъде страна дори ако комуникиращите не разговарят с него, нито той с тях. Виж *United States v. Tzakis*, 736 F.2d 867, 871-72 (2d Cir. 1984). При дела, когато това е уместно, прокурорите могат да обмислят да повдигнат обвинение към индивид, който подслушва или записва разговори между други хора, които не знаят за присъствието му, тъй като такова лице не е страна в комуникацията.

Доставчик на услуги обикновено не трябва да бъде смятан за страна в комуникации, които се осъществяват по неговата система; доставчикът не *участва* в комуникациите на своите абонати, а по-скоро и единствено ги *предава.* И наистина, ако доставчиците на услуги можеха да се съгласят като страни разговорите, които се провеждат по системите им, да бъдат

подслушвани, нямаше да бъде необходимо изключението, което защитава правата и собствеността на доставчиците на услуги. Виж Глава 8, Кодекс на САЩ, параграф 2511(2)(a)(i).

Предварително съгласие

Съгласието според подраздели 2511(2)(c) и (d) може да бъде изрично или косвено, по подразбиране. Виж *United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987). Съгласието може да бъде косвено, когато „околните обстоятелства показват, че (страната) съзнателно се е съгласила на наблюдението. *United States v. Amen,* 831 F.2d 373, 378 (2d Cir. 1987). Тези обстоятелства обикновено изискват да се покаже, че съгласяващата се страна е получила своевременно уведомление за наблюдението и въпреки това е избрала да използва наблюдаваната система. Виж *United States v. Workman*, 80 F.3d 688, 693 (2d Cir. 1996); *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-17 (1st Cir. 1990) („Косвеното съгласие е фактическо съгласие, което е извлечено от заобикалящите обстоятелства, показващи, че страната съзнателно се е съгласила на наблюдението.); *Berry v. Funk*, 146 F.3d 1003, 1011 (D.C. Cir. 1998) („Без своевременно уведомление съгласието може да се подразбира само когато заобикалящите обстоятелства показват, че страната е знаела за и се е съгласила с подслушването.“). Например редица съдилища са поддържали тезата, че затворници, които доброволно избират да използват телефони, които знаят, че се подслушват, чрез този си избор косвено се съгласяват с подслушването на телефонните разговори, проведени по този телефон. Виж *United States v. Verdin-Garcia,* 516 F.3d 884, 894 (10th Cir. 2008); *United States v. Faulkner,* 439 F.3d 1221, 1224 (10th Cir. 2006); *United States v. Horr,* 963 F.2d 1124, 1125 (8th Cir. 1992). Въпреки това обаче „самото знание за възможността за проследяване не може да се смята за косвено съгласие“, особено когато на страната е било казано, че комуникациите няма да бъдат следени. *Watkins v. L.M. Berry & Co.,* 704 F.2d 577, 581 (11th Cir. 1983); виж също *Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir. 1992) (където се доказва липса на съгласие въпреки уведомление за възможността за проследяване).

Съгласието трябва да бъде по-скоро „фактическо“, отколкото „конструктивно“. Виж *Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 19-20 (1st Cir. 2003). Доказателство за уведомление на страната подкрепя заключението, че страната е знаела за наблюдението. Виж *Workman*, 80 F.3d. at 693; *United States v. Corona Chavez,* 328 F.3d 974, 979 (8th Cir. 2003) („щом Миноз е била длъжна да постави механично устройство в ухото си с цел да запише разговора, едва ли може да има съмнение, че тя е знаела, че разговорът се подслушва“). При липса на доказателство за уведомление трябва да се покаже „убедително“, че страната е знаела за подслушването въз основа на заобикалящите обстоятелства в подкрепа на твърдението за косвено съгласие. Виж *United States v. Lanoue*, 71 F.3d 966, 981 (1st Cir. 1995).

Един начин за доказване на фактическо уведомление е мрежови банер, уведомяващ потребителя, че мрежата се наблюдава и подслушва; този банер може да бъде използван, за да се покаже, че потребителят е дал съгласие за подслушване на комуникациите по тази мрежа. *United States v. Angevine*, 281 F.3d 1130, 1133 (10th Cir. 2002); *Muick v. Glenayre Elecs*., 280 F.3d 741, 743 (7th Cir. 2002); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000). Например по отношение на определен служител, който е знаел за политиката на наблюдение и всекидневно е бил уведомяван за нея посредством предупредително съобщение, се е поддържала тезата, че той косвено се е съгласил неговият имейл да се следи от работодателя му *Sporer v. UAL Corp.,* 2009 WL 2761329, at *6 (N.D. Cal. 2009). Обикновено мрежовите банери не изискват потребителите да са съгласни всеки да следи техните комуникации, а по-скоро само техният работодател или собственикът на компютърната мрежа. В случай че даден обвиняем подслуша комуникации и не може да докаже, че е сред лицата, които имат право на това според текста на банера, то тогава обвиняемият не може да твърди, че наличието на банер означава съгласие с подслушването.

Дейност под шапката на закона

Раздел 2511(2)(c) се прилага само когато лицето, което осъществява подслушването, действа „под шапката на закона“. В противен случай в сила може да бъде раздел 2511(2)(d).

Държавните служители не „действат под шапката на закона“ само защото са държавни служители. Виж *Thomas v. Pearl*, 998 F.2d 447, 451 (7th Cir. 1993). Дали даден индивид „действа под шапката на закона“, зависи от това дали когато провежда подслушването, той действа по поръчение на държавата. Виж *United States v. Andreas,* 216 F.3d 645, 660 (7th Cir. 2000); *United States v. Craig*, 573 F.2d 455, 476 (7th Cir, 1977); виж също *Obron Atlantic Corp. v. Barr*, 990 F.2d 861, 864 (6th Cir. 1993); *United States v. Tousant*, 619 F.2d 810, 813 (9th Cir. 1980). Фактът, че дадена страна, на която е предоставено съгласие, тайно сътрудничи с правителството, не снема валидността на съгласието по параграф 2511(2)(c). *United States v. Shields*, 675 F.2d 1152, 1156-57 (11th Cir. 1982).

Цел да се извърши престъпно или закононарушително действие

Параграф 2511(2)(d) се прилага, когато лицето, извършващо подслушването, не действа „под шапката на закона“, но съдържа клауза изключение-на-изключението, каквато 2511(2)(c) няма: подслушването е незаконно, ако лицето, извършващо подслушването, действа „с цел да осъществи каквото и да е престъпно или закононарушително действие в противоречие на Конституцията на САЩ или на който и да е отделен щат“. Глава 18, Кодекс на САЩ, параграф 2511(2)(d); виж също *Payne v. Norwest Corp.,* 911

F. Supp. 1299, 1303 (D. Mont. 1995) (прилагане на изключение за липса на доказателство за престъпна или закононарушителна цел за записването на разговори).

Намерението на Конгреса с това изключение-на-изключението е да забрани подслушване, извършено с цел да се нанесе щета на някой друг в степента, в която щетата е отделно забранена от някой друг приложим закон. Виж *Simpson v. Simpson,* 490 F.2d 803, 805 n.3 (5th Cir. 1974) (закононарушителното или престъпно действие може да включва „изнудване на отсрещната страна, заплашване или публично опозоряване"). Дали едно „действие" представлява нарушение на наказателния кодекс или закононарушение, може, разбира се, да се реши единствено въз основа на всеки конкретен случай. Прокурорът трябва да взема предвид най-вече приложимите щатски закононарушения, свързани с проникване в личното пространство.

При установяване на целта на подслушването съдът разглежда намерението как да се използва подслушаното. Виж *High Fructose Corn Syrup Antitrust Litig.,* 216 F.3d 621, 626 (7th Cir. 2000). Възможно е дадено подслушване да бъде мотивирано от няколко цели, някои законни, други незаконни. Например журналистът може да запише разговор, за да напише материал (законна цел) и за да наруши личното пространство (незаконна цел). Виж *Sussman v. American Broadcasting Companies, Inc.,* 186 F.3d 1200, 1202 (9th Cir. 1999). В такъв случай „съществуването на законна цел няма да направи по-приемлив запис, който е направен също и с незаконна цел: записът е в нарушение на параграф2511." (Пак там.)

Изключение за доставчика

Законът за подслушването постановява, че:

По тази глава няма да бъде незаконно оператор на комутаторно табло, длъжностно лице, служител или представител на доставчик на жични или електронни комуникационни услуги, чиито способности се използват за предаването на жична или електронна комуникация, да записва, разкрива или използва тази комуникация в обичайния ход на своята работа, докато се занимава с каквато и да е дейност, необходима за предоставянето на услугата или за защита на правата или собствеността на доставчика на тази услуга, обаче доставчикът на жична комуникационна услуга на обществото няма да използва наблюдение на услугата или случаен мониторинг, освен за проверка на механичните устройства и качествения контрол.

Глава 18, Кодекс на САЩ, § 2511(2)(a)(i).

Клаузата „права или собственост на доставчика“ в параграф 2511(2)(a)(i) дава на доставчиците правото да „подслушват и наблюдават (комуникации) противащи по техните съоръжения с цел да се борят с измама и кражба на услуги“. *United States v. Villanueva,* 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998). Например служителите на компания за мобилни телефонни услуги могат да подслушат комуникации от нелегално „клониран“ клетъчен телефон, докато установяват произхода му. Виж *United States v. Pervaz,* 118 F.3d 1, 5 (1st Cir. 1997). Изключението също така позволява на доставчиците да следят за злоупотреба със системата с цел да я предпазят от увреждане или нарушаване на личното пространство. Например системните администратори могат да проследят нарушителите в своите мрежи, за да предотвратят по-нататъшни щети. Виж *United States v. Mullins,* 992 F.2d 1472, 1478 (9th Cir. 1993) (необходимостта да се проследи злоупотреба с компютърна система оправдава подслушването на електронни комуникации по параграф 2511(2)(a)(i)).

Важно е, че изключението в клаузата за правата и собствеността на доставчика не дава право на доставчиците да провеждат неограничен мониторинг. Виж *United States v. Auler,* 539 F.2d 642, 646 (7th Cir. 1976). Вместо това изключението разрешава на доставчиците и техните пълномощници да провеждат разумен мониторинг, който да балансира между нуждата на доставчиците да защищават правата и собствеността си и правото на техните абонати комуникациите им да останат поверителни. Виж *United States v. Harvey,* 540 F.2d 1345, 1351 (8th Cir. 1976) („Федералните съдилища … са изработили наредбата, за да наложат стандарт за разумност върху разследващия комуникацията.“). *United States v. Councilman,* 418 F.3d 67, 82 (1st Cir. 2005) („неопровержимо“ е, че изключението за доставчика не му разрешава да чете имейлите на абонатите си с надеждата да спечели търговско предимство).

По такъв начин доставчици, които разследват незаконно използване на своите системи, имат широка власт да проследяват и да разкриват улики за незаконна употреба според параграф 2511(2)(a)(i), но те трябва да се опитат да приспособят своя мониторинг и оповестяване така, че да сведат до минимум подслушването и разкриването на частни комуникации, несвързани с разследването. Виж *United States v. Freeman*, 524 F.2d 337, 341 (7th Cir. 1975) (със заключението, че телефонна компания, която разследвала използването на незаконни приспособления, използвани, за да откраднат междуградска услуга, е действала допустимо според параграф 2511(2)(a)(i), когато е подслушвала първите две минути от всеки незаконен разговор, но не е подслушвала законно разрешените комуникации). В частност трябва да има „фактическа връзка“ между мониторинга и заплахата за правата или собствеността на доставчика. *United States v. McLaren*, 957 F. Supp. 215, 219 (M.D. Fla. 1997); виж *Bubis v. United States*, 384 F.2d 643, 648 (9th Cir. 1967).

Клаузите „нормалният ход на неговата работа“ и „необходима за предоставянето на услугата“ на параграф 2511(2)(a)(i) задават допълни-

телни контексти, в които се прилага изключението за доставчика. Според решенията на съдилищата първото от тези изключения дава право на даден бизнес да получава имейли, изпратени на адрес, предоставен от бизнеса на бивш служител, или на адрес, свързан с новопридобит бизнес. Виж *Freedom Calls Found. v. Bukstel,* 2006 WL 845509, * 27 (E.D.N.Y. 2006) (работодател, упълномощен в обичайния ход на работата да чете имейлите, изпратени на адреса на бивш служител, тъй като „проследяването е необходимо, за да гарантира, че … на имейлите се отговаря своевременно"); *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.,* 2007 WL 4394447, at *5-6 (E.D. Pa. 2007) (корпорация, упълномощена в обичайния ход на работата да чете имейли, изпратени до бизнес, който е придобила). Клаузата „необходима за предоставянето на услугата" разрешава на доставчиците да подслушват, използват или разкриват комуникации в обичайния ход на работата, когато подслушването не може да бъде избегнато. Виж *United States v. New York Tel. Co.,* 434 U.S. 159, 168 n.13 (1977) (където се отбелязва, че параграф 2511(2)(a)(i) „изключва всички нормални бизнес практики на телефонната компания" от забраната на Глава III). Тези казуси обикновено възникват, когато се използват аналогови телефонни линии. Например операторът на комутаторното табло може за кратко да дочуе разговорите, когато свързва линиите. Виж *United States v. Savage,* 564 F.2d 728, 731-32 (5th Cir. 1977); *Adams v. Sumner,* 39 F.3d 933, 935 (9th Cir. 1994). По подобен начин ремонтните техници могат да дочуят откъслеци от разговори в течение на ремонта. Виж *United States v. Ross,* 713 F.2d 389, 392 (8th Cir. 1983). Тези дела, свързани с жичните комуникации, подсказват, че формулировката „необходим за предоставяне на услугата" по подобен начин би разрешила на системния администратор да подслушва комуникации, докато поправя или поддържа компютърната мрежа.

ДОБРОСЪВЕСТНОСТ

Раздел 2520(d) предоставя три свързани основания за защита въз основа на „добросъвестност":

Защита – Добросъвестно упование в –

(1) *съдебно разпореждане или заповед, призовка от голямото жури, правно или законно разрешително;*

(2) *заявка от разследващ или правоприлагащ служител по раздел 2518(7) на тази глава или*

(3) *добросъвестно убеждение, че раздели 2511(3) или 2511(2)(i) от тази глава разрешават поведението, което се оспорва;*

представлява пълна защита срещу всеки граждански или наказателен иск, заведен по тази глава или всеки друг закон.

Защитите по „добросъвестност“ в раздел 2520 предотвратяват наказателното преследване на обвиняем, който добросъвестно е разчитал на изброените правни процедури (напр. съдебни заповеди, призовки от голямото жури) или заявка по спешност (по Глава 18, Кодекс на САЩ, параграф 2518(7). Тези защити са най-често приложими към служители на правоприлагащите органи, които работят по законно дело, и доставчици на услуги, които се подчиняват на законното дело дори когато това дело впоследствие се окаже с известни несъвършенства. Те се прилагат дори когато обвиняемите се позовават на убедително фалшифицирани призовки. Виж *McCready v. eBay, Inc.,* 453 F.3d 882, 892 (7th Cir. 2006).

Заключителният подраздел на раздел 2520(d) постановява, че „добросъвестно упование“ на „добросъвестно убеждение, че раздел 2511(3) ... позволява поведението, което се оспорва“, представлява „пълна защита“. Глава 18, Кодекс на САЩ, параграф 2520(d)(3). Раздел 2511(3) дава право на доставчик на електронни комуникационни услуги да разкрива съдържанието на комуникациите при определени и изрично посочени обстоятелства. По такъв начин някои добросъвестни прегрешения на закона са защита за доставчика на комуникационни услуги според подраздел 2520(d)(3). Виж *United States v. Councilman,* 418 F.3d 67, 83-84 (1st Cir. 2005) („Конгресът взе под внимание възможността доставчиците на услуги добросъвестно да объркат границите на своите правомощия във връзка с определени факти и разработи правни механизми за справяне с този проблем.“).

ИЗКЛЮЧЕНИЕ ЗА „ОБЩЕСТВЕНА ДОСТЪПНОСТ“, ГЛАВА 18, КОДЕКС НА САЩ, ПАРАГРАФ 2511(2)(G)

Раздел 2511(2)(g)(i) позволява „всяко лице“ да прихване електронна комуникация, осъществена посредством електронна комуникационна система, „която е конфигурирана по такъв начин … че комуникацията е лесно достъпна за широката публика. Конгресът е използвал този език, за да позволи подслушването на електронна комуникация, която е публикувана в публичен сайт, публичен чат сайт или новинарски форум. Виж S. Rep. No. 99-541, at 36 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3590 („Никакви очаквания за поверителност не трябва да се предявяват към електронни комуникации, станали достъпни посредством лесно достъпни устройства, и подслушването на такива комуникации е разрешено от Закона за подслушването.“) *Konop v. Hawaiian Airlines, Inc.,* 236 F.3d 1035, 1045 (9th Cir. 2001). Това изключение може да се прилага дори когато потребителите задължително трябва да се регистрират и да са съгласни с условията за ползване, за да получат достъп до комуникацията. Виж *Snow v. DirecTV, Inc.,* 450 F.3d 1314, 1321-22 (11th Cir. 2006) (електронен бюлетин, който изисквал посетителите да се регистрират, да получат парола и да удостоверят, че не са свързани с DirecTV, е бил достъпен за широката публика). Показателно, раздел 2511(2)(g)(i) се прилага само за електронните комуникации.

Когато електронната комуникация е изпратена по радиото – със сателитна комуникация или безжична мрежа – се прилагат специални правила. Въпреки че всяка антена може да получи радиосигнали, не всички електронни комуникации, изпратени по радиото, са „лесно достъпни за широката публика“ според раздел 2511(2)(g)(i). Раздел 2510(16) определя кои са „лесно достъпни за широката публика“. Криптирани електронни комуникации, изпратени по радиото, не са „лесно достъпни за широката публика“. Глава 18, Кодекс на САЩ, параграф 2510(16)(A); *United States v. Shriver,* 989 F.2d 898 (7th Cir. 1992). Раздел 2510(16) изброява редица други защитени техники на предаване и честоти, описани с технологични спецификации.

Раздел 2511(2)(g)(ii) разглежда жичните и електронни комуникации, изпратени по радиото. Той изключва някои от тези комуникации от защитите, предвидени от Закона за подслушването. Радио емисии, изпратени от „която и да е станция, предназначена за широката публика“, като радиостанции на FM и AM вълни, не попадат под защита. Глава 18, Кодекс на САЩ, параграф 2511(2)(g)(ii)(I). Радио предавания, осъществени от „правителствен, правоприлагащ, частен наземен мобилен номер или комуникационни системи за обществена безопасност, включително на полицията и на пожарната, лесно достъпни за широката публика“, също не са защитени. Пак там, параграф 2511(2)(g)(ii)(II); *United States v. Gass,* 936 F. Supp. 810, 816 (N.D. Okla. 1996) („Ако правителствена радио комуникация е „лесно достъпна за широката публика, тогава къде е вредата съдържанието на тази комуникация да бъде подслушано и разпространено?“). В случаите обаче, когато се използва електронна комуникационна система, която не е система за обществена безопасност, като частна пейджър система, това изключение не е приложимо. Виж *United States v. Sills, 2000 WL 511025, at *3 (S.D.N.Y. 2000).*

ТРЕТА ЧАСТ: СЪБИРАНЕ НА КОМПЮТЪРНИ ДОКАЗАТЕЛСТВА

Тази част разглежда законодателните и действащи правила при използването на съдебни заповеди за събиране на доказателства, въведени в компютри и електронни медии. В раздел (1) се разглеждат стратегическите съображения, които всеки следовател или прокурор трябва да има предвид, преди да подаде заявка до съда за издаване на съдебна заповед. Раздел (2) разглежда проблеми, които възникват при написването на съдебна заповед или клетвена декларация за претърсване на компютър. Раздел (3) разглежда съдебното претърсване на медия. Раздел (4) разглежда предизвикателствата пред процеса на претърсването. Накрая Раздел (5) разглежда ограничените случаи, в които наредбите и други правила забраняват на правителството да използва съдебна заповед за изземване на компютри или електронни медии.

1. РАЗРАБОТВАНЕ НА СТРАТЕГИЯ ЗА ПРЕТЪРСВАНЕ

Преди да се напише заявка за съдебна заповед или клетвена декларация, внимателно следва да се разгледа какво точно доказателство се търси при обиска. Претърсване на твърдия диск на компютър може да разкрие много различни видове доказателства. Стратегията за претърсването трябва да се избере, след като се разгледат възможните роли, които компютърът е изпълнявал в престъплението:

1. Компютърът може да бъде контрабанда – или защото компютърът съхранява контрабандни данни (като детска порнография), или защото компютърът е откраднатa чужда собственост;

2. Компютърът може да съхранява данни, които са доказателство за престъпление – например таблица, показваща незаконна търговия с лекарства, писмо, използвано в текуща измама, или входящи файлове, които показват IP адреси, въведени в компютъра, или достъп до интернет сайтове; или

3. Компютърът може да бъде инструмент на престъпление – например компютърът е бил използван като оръдие за проникване в защитени интернет сайтове, за разпространение на видео материали без заплащане на авторски права или за създаване на незаконна порнография.

Освен това при разработването на стратегия за обиска следователите трябва да имат предвид както елементите, които трябва да бъдат до-

казани, ако разследването доведе до съдебен процес, така и източниците на електронно доказателство, които отговарят на тези елементи.

Типичният потребител на компютър мисли за съдържанието на твърдия диск в рамките на онова, което решава да разкрие на интерфейса: файлове, папки и приложения, прегледно подредени и с отделно съдържание. Това всъщност е абстракция, която се прави, за да се улесни използването на компютъра. Тази абстракция скрива доказателството за ползването на компютъра, което съвременните операционни системи оставят в твърдия диск. Докато компютърът работи, те оставят улики по твърдия диск – значително повече доказателства, отколкото просто файловете, видими за потребителя.

Останки от изцяло или частично заличени файлове могат да съществуват на диска. Части от файлове, издадени на друго място, също могат да се открият. „Метаданни“ и други артефакти, оставени от компютъра, могат да разкрият информация в какви файлове се е влизало напоследък, кога даден файл е бил създаден и редактиран и понякога дори как е бил редактиран. Виртуалните системи за страниране могат да оставят следи от информация в твърдия диск, които потребителят може би мисли, че се съхраняват само във временната памет на компютъра, като рампаметта, и които изчезват, когато изключи компютъра. Браузери, четци, клиенти на чатове и други програми оставят след себе си конфигуриращи файлове, които могат да разкрият прозвища и пароли. Операционните системи и приложенията съхраняват допълнителна информация на твърдия диск, като записи за влизания в интернет, включването на периферни и флашдрайвове, и времето, когато компютърът е бил използван. Взета заедно, тази информация може да разкрие на следователя не само съдържанието на компютъра по време на претърсването, но също така улика за това кой го е използвал, кога и как.

Очевидно разкриването на контрабанда или веществено доказателство за престъпление често пъти ще бъде целта на претърсването на компютър. Въпреки това следователите трябва да разгледат и други цели, които претърсването на компютъра може да постигне. Да разгледаме следните примери:

1. Може да се окаже необходимо да се докаже, че именно определен индивид е извършил престъплението, а не някой друг с достъп до компютъра. Това може да се установи посредством доказателство, че определен потребител се е регистрирал, или посредством улика, че компютърът е бил използван малко след извършването на престъплението за проверка на банковата сметка или имейла.
2. Възможно е следователят да иска да провери дали някакъв вирус или друг зловреден софтуер не е виновен за престъплението. Често пъти следователят може да установи това просто като включи антивирусна програма на копирания твърд диск.

3. Може да се окаже необходимо да се покаже, че обвиняемият има познания по определена тема. Историята на търсенията в мрежата например може да разкрие, че даден индивид е изследвал възможностите да създаде лаборатория за метамфетамини.

Прокурорът или следователят трябва внимателно да преценят възможните цели, когато пишат съдебната заповед, за да гарантират, че в резултат на нейното изпълнение ще се съберат достатъчно доказателства.

2. ПОДГОТОВКА НА КЛЕТВЕНА ДЕКЛАРАЦИЯ, ЗАЯВКА И СЪДЕБНА ЗАПОВЕД

Клетвената декларация и заявката за съдебна заповед за претърсване на компютър в много отношения са същите, както в останалите случаи: декларторът се заклева във факти, според които има достатъчно основание да се смята, че доказателства за престъпление като записи, контрабанда, резултати от престъпление или инструменти на престъпление се намират в частно пространство (като твърдия диск на компютъра или друга медия, които от своя страна могат да се намират в друго частно пространство като дома или офиса) и съдебната заповед описва с подробности нещата (записи или други данни или самия компютър), които трябва да се претърсят и изземат. Следователно процесът на написването на клетвена декларация и заявка се извършва на два етапа: установяване на достатъчно основание за претърсване на компютъра и описание в подробности на данните, които трябва да се изземат от компютъра или твърдия диск на компютъра.

Включване на данни, представляващи достатъчно основание

Достатъчното основание, необходимо за претърсването на компютър или електронна медия, е основанието да се смята, че има доказателство за престъпление или инструмент на престъпление. Виж *Fed. R. Crim. P. 41*(c). Доказателство за престъпление включва доказателство за собственост и контрол. Виж *United States v. Horn*, 187 F.3d 781, 787-88 (8th Cir. 1999) (в дело за детска порнография приема клауза в съдебната заповед, която дава право да се изземат „записи, документи, квитанции, ключове или други предмети, които показват достъп до и контрол върху жилището“). Според Върховния съд изискването за достатъчно основание е удовлетворено от клетвена декларация, удостоверяваща че „съществува вероятност на дадено място да се намери контрабанда или доказателство за престъпление“. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Това изисква фактическо, в духа на здравия разум, определяне на вероятностите въз основа на сбора от обстоятелствата. Разбира се, достатъчно основание не съществува, ако служителят се позове само на „голо подозрение“, че на подлежащото на обиск място ще се намери престъпна улика. Виж *Brinegar v.*

United States, 338 U.S. 160, 175 (1949). Щом прокурорът намери достатъчно основание и издаде съдебна заповед, убеждението на прокурора за съществуването на достатъчно основание се приема с „голямо уважение“ и ще се поддържа, докато има „фактическо основание да се смята, че съществува достатъчно основание“.

Често пъти за претърсването на компютър не се изискват специални факти, за да се намери достатъчно основание. Като общо правило „контейнер, който може да съдържа обекта на претърсването, разрешено със съдебна заповед, може да бъде отворен незабавно; интересът на индивида за запазване на личното пространство трябва да отстъпи пред убеждението на прокурора за наличието на достатъчно основание“. *United States v. Ross*, 456 U.S. 798, 823 (1982). Затова, ако съдебната заповед дава разрешение да се претърси дадено помещение (например лекарски кабинет) за конкретен списък от документи (например фалшиви сметки за здравни осигуровки), тогава съдебната заповед трябва да даде право на полицаите да претърсят компютър, който се намира на това място, ако те с основание смятат, че описаните в заповедта документи може да са въведени в компютъра. Виж *United States v. Giberson*, 527 F.3d 882, 887 (9th Cir. 2008) (полицаите имат право да претърсят компютър, „защото има голяма вероятност документите, изброени в заповедта, да бъдат намерени“ в този компютър); *United States v. Rogers*, 521 F.3d 5, 9-10 (1st Cir. 2008) (със становище, че видеокасета е вероятно хранилище за снимки, така че съдебна заповед, която упълномощава изземването на „снимки на съпругата на лицето“, дава право за конфискация и преглед на касетата за такива снимки). В такъв случай е необходимо да се посочи достатъчно основание да се смята, че документите ще бъдат намерени на въпросното място, но не е необходимо да се установи, че там ще има компютър или друго електронно хранилище, както и че там ще има шкафове за папки, купчини документи или други системи за съхранение. Накратко, изискването за позоваването на достатъчно основание не налага полицаите да бъдат ясновидци и да знаят предварително точните форми на доказателството или контрабандата, които ще има на мястото, подлежащо на обиск. Виж *United States v. Reyes*, 798 F.2d 380, 382 (10th Cir. 1986) (където се отбелязва, че „в епохата на съвременните технологии … не може да се очаква от съдебната заповед да описва с точност конкретните форми, под които могат да съществуват документите).

Обаче в делото *United States v. Payton*, F.3d, 2009 WL 2151348 (9th Cir. July 21, 2009) Деветият федерален апелативен съд излиза със становището, че служителите на правоприлагащия орган нямат автоматически право да претърсят компютър, който евентуално съдържа улика, попадаща в обхвата на заповедта. В делото *Payton* служител, който изпълнявал заповед за обиск, която давала право да се изземат документи за продажба на лекарства и други финансови документи, претърсил компютър, в който било възможно да се съхраняват такива документи. Съдът решил, че тъй като заповедта за обиск изрично не упълномощавала претърсване на

компютъра и тъй като нищо друго на мястото на обиска не подсказвало, че документите от обсега на заповедта могат да бъдат намерени в компютъра, то обискът нарушава Четвъртата поправка.

Предвид делото *Payton,* може да се каже, че е уместно прокурорите и полицаите, които искат съдебна заповед от Деветия апелативен съд, винаги да изискват специално разрешение за претърсване на компютри, въпреки че липсата на такова разрешително няма непременно да направи невалидно претърсването.

Достатъчното основание ще бъде различно при всеки отделен случай, но в контекста на претърсването на компютри се очертават няколко сценариия.

а) достатъчно основание въз основа на интернет протокол

В обичайния сценарий на претърсване на компютър следователите научават за престъпно поведение онлайн. Като използват документи, получени от жертвата или от доставчика на услуги, следователите определят интернет портал – айпи адрес, използван за извършване на престъплението. Със съдебен механизъм следователите убеждават доставчика на интернет услуги, който контролира айпи адресите, да идентифицира клиента, на когото е даден този айпи адрес в съответното време, и да предостави (ако са известни) името на потребителя, адрес и друга информация. В някои случаи следователите установяват, че лицето, посочено от доставчика, наистина живее на посочения адрес, като проверят пощата или сметките за домакинството.

Писмени клетвени декларации, които описват подобно разследване, обикновено са достатъчни за установяване на достатъчно основание, което от своя страна се подсилва, ако клетвената декларация потвърждава с някои допълнителни факти връзката между айпи адреса и физическия адрес. Виж *United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007) (достатъчно основание, установено чрез айпи адрес, използван за достъп до детска порнография и документи от интернет доставчика за физически адрес); *United States v. Grant*, 218 F.3d 72, 76 (1st Cir. 2000) (доказателство, че интернет акаунт, принадлежащ на обвиняемия, е замесен на няколко пъти в престъпна дейност и че колата на обвиняемия е била паркирана пред къщата му по време на поне едно от престъпленията, е достатъчно основание за обиск в дома на обвиняемия); *United States v. Carter*, 549 F. Supp. 2d 1257, 1261 (D. Nev. 2008) (достатъчно основание, установено чрез айпи адрес, документи от интернет доставчика и квитанции от сметки); *United States v. Hanson*, 2007 WL 4287716, at *8 (D. Me. Dec. 5, 2007) (достатъчно основание въз основа на айпи адрес и домашен адрес, въпреки че „липсва директна информация дали какъвто и да е компютърен хардуер ... физически присъства“ в дома); *United States v. Huit*t, 2007 WL 2355782, at *4 (D. Idaho

Aug. 17, 2007) (достатъчно основание, установено по айпи адрес и отделен имейл адрес, и двата свързани с едно и също физическо местоположение).

Обвиняемите понякога възразяват, че връзката между айпи адрес и физически адрес не може да бъде достатъчно основание, тъй като технически е възможно лица, които не живеят на този адрес, да използват интернет връзката на обвиняемия. Най-често това възражение се формулира в смисъл, че обвиняемият е имал или е можел да има отворена безжична интернет връзка, която би дала възможност на всеки живеещ в съседство, който разполага с такова устройство, да използва интернет връзката и айпи адреса му. Съдът последователно е отхвърлял такова възражение, защото стандартът за достатъчно основание за издаване на съдебна заповед изисква само наличието на достоверна възможност, че ще бъде открито доказателство или контрабанда. Виж *Perez*, 484 F.3d at 740 (стандартът за достатъчно основание е покрит от връзката между айпи адрес и физически адрес независимо от възражението на обвиняемия, че може би е имал „неосигурена интернет връзка", която дава възможност на други лица да използват айпи адреса му); *Carter*, 549 F. Supp. 2d at 1267-69 (където се отхвърля възражението, че в клетвената декларация за съдебната заповед за обиск е трябвало да се отбележи възможността за отворена интернет връзка); *United States v. Latham*, 2007 WL 4563459, at *11 (D. Nev. Dec. 18, 2007) (където се потвърждава достатъчното основание, въпреки че е „било възможно друг освен Лари Латам или член на семейството му да е имал достъп до интернет или посредством безжичен рутер, или като е използвал адреса му с цел да се включи в група за обмен на детска порнография"). И наистина, това възражение е особено слабо, тъй като самата точка на безжичен достъп обикновено съдържа улика, попадаща в обсега на съдебната заповед. По подобни причини съдилищата са отхвърляли възражения срещу наличието на достатъчно основание въз основа на това, че клетвената декларация не отхвърля „незаконно проникване", „измама", „подправяне", „кражба", „унищожаване" или заразяване с вирус от други лица". *United States v. Hibble*, 2006 WL 2620349, at *4 (D. Ariz. Sept. 11, 2006) (citing *United States v. Gourde*, 440 F.3d 1065, 1073 n.5 (9th Cir. 2006). Както се мотивира Петият федерален апелативен съд, „въпреки че е възможно съобщенията да идват извън дома, където е регистриран айпи адресът, все пак е вероятно източникът на съобщенията да е бил вътре в тази къща". *Perez*, 484 F.3d at 740. Алтернативните обяснения е по-подходящо да бъдат повдигнати като защита по време на процес." *Hibble*, 2006 WL 2620349, at *4.

б) достатъчно основание въз основа на онлайн акаунт информация

В друг сценарий обвиняемият открива акаунт за онлайн услуги – като имейл услуги или порнографски сайт – и информацията от кредитната му карта или контактната информация, свързана с този акаунт, се използва, за да се идентифицира обвиняемият и в подкрепа на достатъчно основание за претърсване на компютърната медия в дома на обвиняемия. Например

в делото *United States v. Kelley*, 482 F.3d 1047, 1053 (9th Cir. 2007) клетвена декларация установява достатъчно основание въз основа на истинско име и физически адрес, свързани с редица „никнейм" в „Америка Онлайн", използвани за получаване на детска порнография. По подобен начин в *United States v. Terry*, 522 F.3d 645, 648 (6th Cir. 2008) като достатъчно основание за обиск на дома се изтъква, че даден имейл акаунт е използван за изпращане на детска порнография, че притежателят на този акаунт живее в тази къща, че притежателят на този акаунт има компютър в тази къща и в миналото е изпращал електронни съобщения от този акаунт. Виж също *United States v. Wilder*, 526 F.3d 1, 6 (1st Cir. 2008) („от абонамента му за сайта „Галерия на похотта" може да се направи изводът, както е описано в клетвената декларация, че е твърде възможно да последва сваляне и съхранение на снимки с детска порнография").

Често пъти този сценарий възниква, когато следователите открият сайт с детска порнография или имейл група и успешно се сдобият със списъка на членовете. В *United States v. Gourde*, 440 F.3d 1065, 1070-71 (9th Cir.2006) клетвената декларация установява достатъчно основание въз основа на членството на обвиняемия в известен сайт за детска порнография без наличието на независима улика като айпи адрес. Редица други съдилища подкрепят становището, че от доброволното членство на обвиняемия в уебсайт за детска порнография или „е-група" (хибрид между имейл група и форум в мрежата) може да се направи изводът, че обвиняемият е свалял или съхранявал детска порнография, въпреки че много от тези съдилища посочват и подкрепящи улики. Виж *United States v. Wagers*, 452 F.3d 534, 539-40 (6th Cir. 2006); *United States v. Shields*, 458 F.3d 269, 279 (3d Cir. 2006) (членство в група в мрежата за детска порнография, съчетано с „многозначителен" имейл адрес „Малката Лолита", обосновават достатъчното основание); *United States v. Martin*, 426 F.3d 68, 77 (2d Cir. 2005) („има вероятност онези, които разглеждат снимките, да свалят и да съхраняват детска порнография"); *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004) (където се вземат под внимание фактори като включване в група, едномесечно членство в нея и използването на прозвища в мрежата, „които отразяват интереса му към детската порнография").

Не всички съдилища обаче са съгласни, че членството само по себе си е достатъчно основание. В *United States v. Coreas*, 419 F.3d 151 (2d Cir. 2005) съставът на Втория федерален апелативен съд остро възразява срещу състава в *Martin*. Делото *Coreas* е свързано с клетвена декларация, която след отхвърляне на фалшивите обвинения съдържа „просто" твърдението, че обвиняемият, „като е кликнал върху бутона, е отговорил положително на покана от три изречения … да се присъедини към е-група (за детска порнография)". *Coreas*, 419 F.3d at 156. Становището на съда е, че това твърдение „в никакъв случай не задоволява стандарта на Четвъртата поправка", защото „близостта на даден индивид с други заподозрени в престъпна дейност сама по себе си не може да представлява достатъчно основание за обиск на този индивид". По подобен начин в делото *United States v. Falso*,

544 F.3d 110, 121 (2d Cir. 2008) Вторият федерален апелативен съд излиза със становище, че няма достатъчно основание в съдебна заповед, която твърди само, че „както изглежда", обвиняемият „е получил достъп или се е опитал да получи достъп" до сайт за детска порнография.

в) достатъчно основание въз основа на поведение извън мрежата

В някои случаи името и адресът на обвиняемия се знаят благодарение на традиционни разследващи техники, а полицаите искат да претърсят личния компютър за улика, свързана с престъплението. Тези случаи не се различават от всеки друг случай за претърсване на компютър: клетвената декларация има за цел да установи „достатъчно основание, че контрабанда или доказателство за престъпление ще се открие в компютрите" на мястото, което ще се обискира. *United States v. Adjani*, 452 F.3d 1140, 1145 (9th Cir. 2006). Например в *United States v. Khanan*i, 502 F.3d 1281, 1290 (11th Cir. 2007) съдът намира достатъчно основание да претърси компютъра на счетоводител, тъй като клетвената декларация го идентифицира като счетоводител на работодател на нелегални имигранти, твърди, че негова данъчна декларация е била намерена в кофата за боклук пред офиса и че полицай е видял, че вътре в офиса има компютри. Виж също *United States v. Khanani*, 502 F.3d 1281, 1290 (11th Cir. 2007) (достатъчно основание за претърсване на компютър, подкрепено от „сексуално посегателство върху дъщерята в миналото" от страна на обвиняемия, както и с решението му да снима детето голо).

г) давност

Обвиняемите често възразяват, че фактите, за които се твърди в клетвената декларация за съдебна заповед, са с голяма давност, за да се приемат за достатъчно основание по времето, когато е издадена съдебната заповед. Много такива възражения са били повдигани при дела за детска порнография и обикновено съдебните заседатели не намират особена тежест в тези аргументи: „Когато даден обвиняем е заподозрян, че притежава детски порнографски материали, определянето на давност е нещо изключително, тъй като е добре известно, че снимки с детска порнография крият хората, заинтересувани от такива материали в уединението на дома си". *United States v. Irving*, 452 F.3d 110, 125 (2d Cir. 2006); виж също *United States v. Paul*l, 551 F.3d 516, 522 (6th Cir. 2009) („защото престъплението обикновено се извършва в неприкосновеността на дома и през дълъг период от време, същите времеви ограничения, които се прилагат към повечето мимолетни престъпления, не могат да определят давността при детската порнография"); *United States v. Watzman*, 486 F.3d 1004, 1008 (7th Cir. 2007) (потвърждава клетвена декларация, в която се казва че детските порнографи „пазят и събират неща, съдържащи детска порнография, за дълъг период от време"); *United States v. Newsom*, 402 F.3d 780, 783 (7th Cir. 2005) („информация с едногодишна давност не е непременно

остаряла по закон, особено когато става дума за детска порнография“); *United States v. Riccardi*, 405 F.3d 852, 861 (10th Cir. 2005) (информация отпреди пет години, че обвиняемият се е опитал да прехвърли полароидна снимка в дигитален формат, не е с изтекла давност); *United States v. Hay*, 231 F.3d 630, 636 (9th Cir. 2000); *United States v. Horn,* 187 F.3d 781, 786-87 (8th Cir. 1999); *United States v. Lacy*, 119 F.3d 742, 745-46 (9th Cir. 1997). Съдебните състави също така отбелязват, че напредъкът в съдебния анализ на компютъра дава възможност на следователите да възстановят файлове дори след като са били изтрити, което поставя под още по-голямо съмнение аргумента за „давността“. Виж Hay, 231 F.3d at 636; *United States v. Cox*, 190 F. Supp. 2d 330, 334 (N.D.N.Y. 2002). Обаче виж и *United States v. Doan*, 2007 WL 2247657, at *3 (7th Cir. Aug. 6, 2007) (информация отпреди седемнадесет месеца, съчетана с липса на информация за „времетраенето на абонамента за уебсайтовете, възможностите за сваляне, свързани с тези абонаменти, за последната дата, на която Дуан е влязъл в тези сайтове, дали Дуан е свалял снимки от тези сайтове, дали Дуан е притежавал компютър или дали Дуан е имал интернет достъп в дома си“, не стигат за установяването на достатъчно основание); *United States v. Zimmerman*, 277 F.3d 426, 433-34 (3d Cir. 2002) (където се прави разлика между съхраняване на порнография за възрастни и съхраняването на детска порнография с аргумента, че уликата за това, че порнография за възрастни е била качена на компютъра поне шест месеца преди издаването на съдебна заповед, е с изтекла давност); *United States v. Frechette*, 2008 WL 4287818, at *4 (W.D. Mich. Sept. 17, 2008) (информация отпреди шестнадесет месеца има давност в дело за детска порнография).

ПОДРОБНО ОПИСАНИЕ НА НЕЩАТА, КОИТО СЕ ИЗЗЕМВАТ

а) изискването за подробност

Четвъртата поправка изисква всяка съдебна заповед „подробно да описва“ две неща: „мястото, което ще бъде обискирано, и „лицата или нещата, които ще се изземат“. U.S. Const. Amend. IV; see *United States v. Grubbs*, 547 U.S. 90, 97 (2006). Описването с подробности на нещата, които ще се изземат, има два отделни елемента. Първо, съдебната заповед трябва да опише нещата, които трябва да се изземат, с достатъчно точен език, така че да покаже на полицаите как да отделят нещата, обект на изземване, от нещата, които нямат връзка със случая. Виж *Marron v. United States*, 275 U.S. 192, 296 (1927) („колкото до нещата, които трябва да се вземат, нищо не е оставено на волята на полицая, изпълняващ съдебната заповед“). Второ, описанието на нещата, които ще се изземат, трябва да се ограничи до обхвата на достатъчното основание, описано в съдебната заповед. Разгледани заедно, тези елементи забраняват на следователите да получават „общи съдебни заповеди“, а вместо това ги задължават да провеждат конкретни изземвания, които целят „да сведат до минимум

нарушаването без съдебна заповед на личното пространство". *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976).

б) изземване на компютър/ изземване на информация

Най-важното решение, което служителите трябва да вземат, когато описват собствеността в съдебната заповед, е дали собствеността, която ще се изземе, е хардуерът на компютъра, или само информацията, която се съдържа в този хардуер. Ако хардуерът на компютъра е контрабанден, улика, резултат или средство за престъпление, съдебната заповед трябва да описва самия хардуер. Обаче, ако вероятната причина се отнася само до информацията, съдебната заповед трябва да описва информацията, която трябва да се изземе, и след това да поиска пълномощно да изземе информацията в какъвто и вид да се съхранява тя (било то електронен, или не).

в) изземване на хардуер

В зависимост от естеството на престъплението, което се разследва, хардуерът на компютъра може да бъде контрабанда, средство или резултат на престъпление и следователно може да бъде иззет физически по Правило 41. Например компютър, който съхранява детска порнография, сам по себе си е контрабанда. Виж *United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000) (където се одобрява изземването на целия компютър като контрабанда в дело за детска порнография). Компютърът може да бъде инструмент на престъпление в случаите, когато се използва за хакерство или за изпращане на заплахи. Виж *United States v. Adjani,* 452 F.3d 1140, 1145-46 (9th Cir. 2006) (компютър, използван за изпращане на заплахи, е инструмент); *Davis v. Gracey*, 111 F.3d 1472, 1480 (10th Cir. 1997) (компютър, използван за поддържането на електронен бюлетин за разпространение на порнографски материали, е инструмент); *United States v. Lamb*, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) (компютър, използван за изпращане или получаване на детска порнография, е инструмент). Въпреки че може да се възрази, че всеки компютър, използван за съхраняване на улика за престъпление, е инструмент, аргументацията в *Davis* подсказва, че за да бъде инструмент даден компютър, е необходимо по-същественото му участие в престъплението. Виж *Davis*, 111 F.3d at 1480 (становище, че „компютърното устройство е било не само „контейнер" за файлове; то е инструмент на престъплението").

Ако самият хардуер на компютъра е контрабанда, инструмент на престъпление или резултат от престъпление, съдебната заповед трябва да опише хардуера и да заяви, че компютърът ще бъде иззет. В повечето случаи следователите просто ще изземат компютъра по време на обиска и след това ще го претърсят за контрабанди файлове на обвиняемия в съдебната компютърна лаборатория. В такива случаи служителите трябва ясно да обяснят в приложената клетвена декларация, че възнамеряват да

претърсят компютъра за доказателство и/или контрабанда, след като компютърът бъде иззет и изнесен от мястото на обиска. Обикновено становището на съдилищата е било, че описание на хардуера може да задоволи изискването за конкретност, доколкото при последващите претърсвания на компютърния хардуер вероятно ще се открият улики за престъпление; в много от тези случаи компютрите съдържат детска порнография и следователно са контрабанда. Виж *United States v. Hay*, 231 F.3d 630, 634 (подкрепя изземването на „компютърен софтуер" в търсене на материали, съдържащи детска порнография); *United States v. Campos*, 221 F.3d 1143, 1147 (10th Cir. 2000) (подкрепя изземването на „компютърно устройство, което може би е било или се използва за визуално описание на детска порнография", и отбелязва, че клетвената декларация, приложена към съдебната заповед, обяснява защо е било необходимо да се изземе хардуерът и да се претърси извън мястото на обиска за снимките, които се съдържат в него); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (поддържа изземването на „целия хардуер и софтуер на компютъра ... компютърни дискове и компютърни файлове" в дело за детска порнография, защото „в практическо отношение изземването и последващото претърсване на всички налични дискове по дефиниция е най-старателното претърсване и изземване, което има вероятност да доведе до намиране на търсените снимки"); *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) (не особено конкретна съдебна заповед, която допуска „тотално изземване" на компютърно устройство от дома на обвиняемия, когато има достатъчно основание да се смята, че компютърът съдържа доказателства за престъпления, свързани с детска порнография); *United States v. Henson*, 848 F.2d 1374, 1382-83 (6th Cir. 1988) (разрешава изземването на компютри, компютърни терминали ... кабели, принтери, дискове, флопи дискове и касети, „които могат да съдържат доказателство за схемата за фалшификация на обвиняемия, тъй като обискът е насочен към предмети, които вероятно съдържат информация, отнасяща се до участието на обвиняемия в ... схемата и следователно дава право на служителите да изземат само онова, което е основателно при тези обстоятелства"); *United States v. Albert*, 195 F. Supp. 2d 267, 275-76 (D. Mass. 2002) (подкрепя съдебна заповед за изземване на компютър и целия свързан с него софтуер и устройства за съхранение, когато такова разширено претърсване е „единственият практически начин" да се намерят снимки на детска порнография).

г) изземване на информация

Когато трябва да се претърсват електронни медии за съхранение, тъй като съхраняват информация, която е улика за престъпление, нещата, които трябва да бъдат иззети със съдебната заповед, обикновено са свързани със съдържанието на съответните файлове, а не с физическата медия за съхранение.

Много разследвания претърсват компютри единствено в търсене на доказателство за престъпление; компютърът може да съдържа бизнес до-

кументи, отнасящи се до престъпление на висш чиновник например, но самият компютър да не съхранява контрабанда и да не е използван за извършване на престъплението. Компютърът е „улика“ само до степен, в която някои от данните, които се съхраняват, са доказателство. Виж *United States v. Giberson,* 527 F.3d 882, 887 (9th Cir. 2008) („Компютрите, подобно на дипломатическото куфарче или записите на касети, могат да съхраняват документи и протоколи.“).

Когато достатъчното основание за претърсването се отнася изцяло или отчасти до информация, съхранявана в компютъра, а не до самия компютър, съдебната заповед трябва подробно да идентифицира тази информация, като се насочи към съдържанието на съответните файлове, а не толкова към устройствата за съхранение, които може би ги съдържат. Виж *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (където се заявява, че способността на компютъра да съхранява „огромно количество“ информация „прави изискването за конкретност още по-важно“); *United States v. Vilar*, 2007 WL 1075041, at *36 (S.D.N.Y. Apr. 4, 2007) („информацията, която се търси, трябва да бъде описана в подробности и нейното изземване обусловено независимо от достатъчното основание“); *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (където се казва, че съдебна заповед за изземване на улика, съхранявана в компютър, трябва да посочва конкретно „какъв тип файлове се търсят“); *United States v. Gawrysiak*, 972 F. Supp. 853, 860 (D.N.J. 1997), aff’d, 178 F.3d 1281 (3d Cir. 1999) (подкрепя изземването на документи, които съдържат информация и/или данни, съхранявани на магнитни или електронни кодове в компютърната медия … които представляват доказателство“ за изброените федерални престъпления). В случаи, когато компютърът е само устройство за съхранение на улика, липсата на фокус към конкретни документи може да доведе до нарушение на Четвъртата поправка. Например в процеса *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005), свързан с разследване на телефонни заплахи, съдът излиза със становището, че съдебната заповед, която дава право да се изземе цялата медия за съхранение, без „да се ограничи и да посочи определени файлове“, нарушава Четвъртата поправка.

Служителите трябва да бъдат особено внимателни, когато търсят пълномощие да изземат широк спектър информация. Такива случаи понякога възникват, когато служителите претърсват компютри в бизнес офис. Служителите не могат просто да поискат разрешение да изземат „всички документи“ от действаща фирма, освен ако нямат достатъчно основание да смятат, че престъпната дейност, която се разследва, е просмукала целия бизнес. Виж *United States v. Ford*, 184 F.3d 566, 576 (6th Cir. 1999). Въз основа на друга, по подобен начин опасна фраза, „всички данни, включително, но ограничени не само до“ списък на артикули, съдебна заповед за претърсване на компютър се оказва неконституционна. *United States v. Fleet Management Ltd*., 521 F. Supp. 2d 436, 443-44 (E.D. Pa. 2007); виж също *Otero*, 563 F.3d at 1132 (съдебна заповед, която дава разрешение за из-

земване на „цялата информация и/или данни“, не отговаря на изискването за конкретност).

Вместо това описанието на файловете, които трябва да бъдат иззети, трябва да се ограничи. Една успешна техника в тази насока е да се посочат документи, които се отнасят до конкретно престъпление, и да се включат специфични категории от типове документи, които вероятно ще бъдат намерени. Например Деветият федерален апелативен съд подкрепя такава съдебна заповед, която ограничава търсенето на доказателство за определено (и изрично посочено) престъпление. Виж *United States v. Adjani*, 452 F.3d 1140, 1148 (9th Cir. 2006). Понякога е добре да се посочи обектът на разследването (ако е известен) и времевата рамка за търсените документи (ако е известна). Виж *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (анулиране на съдебна заповед поради пропуск да се назове престъплението или да се ограничи изземването до документи, произведени във времевата рамка на разследването); *United States v. Hunter*, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (заключение, че съдебна заповед за изземване на „всички компютри“ не е достатъчно конкретна, защото описанието „не посочва специфичните престъпления, поради които се изземва оборудването, нито подкрепящите клетвени декларации или ограниченията, заложени в инструкциите за провеждане на обиска“).

Така че ефективен подход би било да се започне с описание на „всички документи“; да се въведе стегнат стил, като се опишат престъплението, заподозрените и времевият период, ако това е възможно; да се включат примери на документите, които трябва да бъдат иззети; и след това да се посочи, че документите могат да бъдат иззети във всяка форма, било то електронна или хартиена. Например, когато се съставя съдебна заповед за претърсване на компютър във фирма за улика за търговия с наркотици, служителите могат да опишат собствеността, която трябва да бъде иззета по следния начин:

Всички документи, свързани с нарушения на Глава 21, Кодекс на САЩ, параграф 841(а) (трафик на наркотици) и/или Глава 21, Кодекс на САЩ, параграф 846 (заговор за трафик на наркотици), в която участва заподозреният след 1 януари 2008, включително списък на клиенти и информация за идентифициране; типове, количества и цени на пренесените наркотици, както и дати, места и количества по определени трансакции; всяка информация, отнасяща се до източник на наркотици (включително имена, адреси, телефонни номера или всяка друга информация за идентификация); всяка информация, даваща сведение за програмата или пътуванията (на заподозрения) от 2008 до сега; всички банкови извлечения, чекове, сметки по кредитни карти, информация за сметки и други финансови документи.

Термините „документи“ и „информация“ включват всички гореизброени части от доказателства, в каквато и да е форма или с каквито и средства те да са създадени или да се съхраняват, включително всякакви форми на компютърно или електронно съхранение (като твърди дискове или друга

медия, която може да съхранява данни); всяка ръчна форма (като писане, рисуване, скициране); всяка механична форма (като принтиране или печатане) и всяка фотографска форма (като микрофилми, микрофишове, разпечатки, слайдове, негативи, видеозаписи, филми, фотокопия).

Забележката, че документите могат да се появят в електронна форма, помага на служителите и юристите, които четат съдебната заповед. Въпреки това обаче обикновено съдиите позволяват на служителите да изземат компютърни устройства, когато те основателно смятат, че съдържанието, описано в съдебната заповед, е възможно да се намира там, независимо от това дали в съдебната заповед изрично се казва, че информацията може да се съхранява в електронна форма. Виж *United States v. Giberson*, 527 F.3d 882, 888 (9th Cir. 2008) („форматът на документ или протокол не трябва да бъде диспозитив на разследване по Четвъртата поправка"); *United States v. Pontefract*, 2008 WL 4461850, at *3 (W.D. La. Oct. 1, 2008) (съдебна заповед, в която се упоменават фотографии, но не компютри, разрешава претърсването на компютър, защото „в съвременния дигитален свят лаптопът е вероятното място, където могат да се намерят снимки, както във фотоалбум"). Както се произнася Десетият федерален апелативен съд по делото *United States v. Reyes*, 798 F.2d 380, 383 (10th Cir. 1986), „в епохата на модерните технологии и търговската достъпност на различни устройства не може да се очаква съдебната заповед да опише с точност формата, която могат да имат документите". По подобен начин от значение е съдържанието на уликата, а не нейната форма, и съдилищата ще се съгласят с основанията на действащия служител за това каква собственост трябва да се изземе, за да се получи уликата, описана в съдебната заповед. Виж *United States v. Hill*, 19 F.3d 984, 987-89 (5th Cir. 1994); *Hessel v. O'Hearn*, 977 F.2d 299 (7th Cir. 1992); *United States v. Word*, 806 F.2d 658, 661 (6th Cir. 1986); *United States v. Gomez-Soto*, 723 F.2d 649, 655 (9th Cir. 1984) („Невъзможността на съдебната заповед да предвиди в какъв точно контейнер ще се намира търсеният материал, не е фатална."). Виж също *United States v. Abbell*, 963 F. Supp. 1178, 1997 (S.D. Fla. 1997) (служителите могат законно да изземат „документ, който по подразбиране попада в обхвата на съдебната заповед – дори когато не е изрично упоменат").

Разбира се, не е необходимо служителите да следват такъв подход при всеки казус; съдебният преглед на съдебната заповед за обиск да бъде по-скоро „разумен" и „практичен", а не „прекалено технически". *United States v. Ventresca,* 380 U.S. 102, 108 (1965). Когато служителите не могат да знаят точната форма на документите преди провеждането на обиска, общото описание би трябвало да бъде достатъчно. Виж *United States v. Logan*, 250 F.3d 350, 365 (6th Cir. 2001) (където се одобрява най-общо формулирана съдебна заповед със забележката, че „общият дух на съдебната заповед" е приемлив, предвид обстоятелствата на разследването); *Davis v. Gracey,* 111 F.3d 1472, 1478 (10th Cir. 1997) („Дори съдебна заповед, която описва нещата, които трябва да бъдат иззети, с широки или най-общи понятия, може да бъде валидна, когато описанието е толкова специфично, колкото

обстоятелствата и естеството на дейността, която се разследва, го позволяват"); *United States v. Lacy,* 119 F.3d 742, 746-47 (9th Cir. 1997) (със становище, че общото описание на компютърното устройство, което трябва да бъде иззето, е достатъчно, тъй като „няма начин да се каже с точност какъв хардуер или какъв софтуер трябва да бъде иззет, за да се възстановят снимките"); *United States v. London*, 66 F.3d 1227, 1238 (1st Cir. 1995) (където се отбелязва че „тъй като обвиняемият е ръководел сложна престъпна схема, в която е смесвал обикновени документи с привидно обикновени документи, които всъщност са запаметявали незаконни трансакции ... би било трудно за магистрата да ограничи езика в съдебната заповед, а за изпълняващия служител да бъде по-точен в намерението си какво да изземе"); *United States v. Scharfman*, 448 F.2d 1352, 1354-55 (2d Cir. 1971); *Gawrysiak*, 972 F. Supp. At 861. Понякога съдебните заповеди разрешават изземвания на всички документи, свързани с определено престъпление. Виж *London*, 66 F.3d at 1238 (разрешава обиск в търсене на „счетоводни книги, протоколи ... и всякакви други документи, които показват незаконна хазартна дейност); *United States v. Riley,* 906 F.2d 841, 844-45 (2d Cir. 1990) (разрешава изземване на „вещи, които представляват улика за конспирация за разпространение на контролирани вещества"); *United States v. Wayne*, 903 F.2d 1188, 1195 (8th Cir. 1990) (разрешава обиск за „документи и материали, които могат да бъдат свързани с контрабанда на наркотици"). Дори обиск на „всички документи" може да бъде приемлив при някои обстоятелства. Виж *United States v. Hargus*, 128 F.3d 1358, 136263 (10th Cir. 1997) (разрешава изземване на „всеки и всички документи, свързани с бизнеса", който се разследва за измама и пране на пари).

Установяване на необходимост от копиране и преглед извън мястото на обиска

С малки изключения, претърсване на твърд диск и други медии изискват твърде много време, за да се проведат на място при изпълнение на съдебна заповед. Клетвената декларация към съдебната заповед трябва да обясни защо е необходимо да се копира целият твърд диск (или физически да се изземе) и след това да се прегледа за търсените документи.

Проверката на компютър в търсене на улика за престъпление почти винаги изисква много време. Дори когато служителите имат конкретна информация за файловете, които търсят, данните могат да бъдат сложени под грешни етикети, съхранени в скрити директории или скрити в „луфтове", които списъкът на файловете не взема под внимание. Виж *United States v. Hill*, 322 F. Supp. 2d 1081, 1089-90 (C.D. Cal. 2004) (Kozinski, J.), aff'd 459 F.3d 966 (9th Cir. 2006); *United States v. Gray*, 78 F. Supp. 2d 524, 530 (E.D. Va. 1999) (където се отбелязва, че служителите, които извършват претърсване на компютърни файлове, „не са длъжни да приемат за точно каквото и да е име или разширение „и да ограничат търсенето си по съответен начин", тъй като престъпниците може „преднамерено да са именували погрешно файлове или да са се опитали да скрият инкриминиращите файлове

в безобидно именувани директории"). Нещо повече, доказателството за престъпление не винаги трябва да бъде под формата на файл. То може да бъде в логаритъм, следа в операционната система или други данни, които е трудно да се намерят и възстановят, без да се разполага със съответните пособия и с достатъчно време. Може да минат дни или седмици, докато се намери специфичната информация, описана в съдебната заповед, защото устройствата за съхранение в компютъра могат да съдържат огромно количество информация. Виж *United States v. Hill*, 459 F.3d 966, 974-75 (9th Cir. 2006) („служителите ще трябва да проверят всеки един от може би хилядите файлове в диска – процес, който може да отнеме часове, а може и дни").

Тъй като проверяването на компютър за доказателство за престъпление изисква толкова много време, почти във всички случаи ще бъде невъзможно да се проведе претърсване на място на компютър или друга медия за съхранение. Не е разумно да се очаква служителите да прекарат повече от няколко часа в търсене на улики на място, а при някои обстоятелства (като извършване на обиск в дома на заподозрения) продължителен обиск би бил неоснователен. Виж *United States v. Santarelli,* 778 F.2d 609, 61516 (11th Cir. 1985). В случаи, свързани голямо количество хартиени документи, съдът обикновено разрешава на следователите да изнесат тези документи извън мястото на обиска, за да ги прегледат и да решат кои документи попадат в обсега на съдебната заповед. Виж *Santarelli,* 778 F.2d at 616; *United States v. Hargus*, 128 F.3d 1358, 1363 (10th Cir. 1997) (разрешава изнасянето на цяла картотека, когато такова изземване е мотивирано с непрактичността на проверката на място); *United States v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982).

Водени от подобни съображения, съдебните заседатели са разрешавали изнасянето на компютри за проверка. Виж *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) („най-мясно дефинираното претърсване и изземване, което се очаква" да се сдобие с доказателството, описано в съдебната заповед, е в повечето случаи „изземването и последващото претърсване на компютъра и всички налични дискове".); *United States v. Hay,* 231 F.3d 630, 637 (9th Cir. 2000) (изземването на целия компютър е основателно, тъй като клетвената декларация „аргументира изнасянето на цялата система с времето, експертизата и контролираната среда, която се изисква за точен анализ"); *Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001) („поради техническите трудности за провеждането на претърсването на компютъра в дома на заподозрения изземването на компютри, включително тяхното съдържание, е оправдано в тези случаи, за да се даде възможност на полицията да идентифицира престъпните файлове"); *United States v. Giberson*, 527 F.3d 882, 886 (9th Cir. 2008) (становище, че съдебна заповед, която „ясно ограничава типа документи и протоколи, които подлежат на изземване", разрешава изземването на целия компютър); *United States v. Grimmett,* 439 F.3d 1263, 1269 (10th Cir. 2006) („възприехме по-скоро доброжелателно отношение към изискването за „конкретност" в съдебна заповед, разреша-

ваща изземване на компютри“). Нещо повече, опитът да се претърси медия за съхранение на място в някои случаи може дори да доведе до повреда на уликата. Съвременните операционни системи непрекъснато четат от и пишат върху твърдия диск, като променят част от информацията, съхранявана там; така че самото използване на компютъра може да промени уликата, записана на твърдия диск. Свързаните с интернет компютри са още по-уязвими, тъй като лице, намиращо се далеч от мястото на обиска, може да успее да проникне в компютъра и да изтрие данни, докато следователите го проверяват на място. Така че най-добрата стратегия е да се преглеждат медиите за съхранение извън мястото на обиска, където съдебните специалисти ще могат да гарантират за интегритета на данните.

В много случаи вместо да изземат целия компютър за проверка, служителите могат вместо това да създадат дигитално копие на твърдия диск, който е идентичен във всяко отношение с оригинала. Копието се нарича „имидж копие“ – копие, което „репродуцира всеки бит и байт на драйва, включително всички файлове и луфтове, мастър файлове и метаданни в същия порядък като в оригинала. *United States v. Vilar*, 2007 WL 1075041, *35 n.22 (S.D.N.Y. Apr. 4, 2007). Имидж копие не може да се създаде с простото изтегляне и копиране на икони или включване на обичайните програми за създаване на копия; процесът на създаването му обикновено включва отварянето на компютъра и свързването на хардуера на следователя директно с твърдия диск. В някои случаи следователите могат да направят имидж копие на място; в други следователите ще изземат хардуера на компютъра от мястото на обиска и ще направят имидж копие.

За да се оправдае създаването на имидж копие и/или изземване на компютъра или медията за съхранение за проверка извън мястото, Деветият федерален апелативен съд изисква клетвената декларация да обясни практическите ограничения, които налагат изземването на цялата компютърна система. Виж *United States v. Hill*, 459 F.3d 966, 975-76 (9th Cir. 2006) (клетвената декларация трябва „да покаже на магистратите с факти защо е разумно да се даде разрешение за такова широко претърсване и изземване в дадения случай“). Тъй като създаването на имидж копие и/или изземването е необходимо почти при всяка съдебна заповед за претърсване на компютър, съмнително е пропуск да се включи такава заявка в клетвената декларация да представлява нарушение на Четвъртата поправка. Въпреки това обаче, независимо че изрично се изисква само от Деветия апелативен съд, добра практика би било всяка клетвена декларация на съдебната заповед да обяснява защо е необходимо да се създаде имидж копие на целия твърд диск (или той физически да се изземе) и впоследствие да се изследва за съответните документи. Когато такива факти се включат в клетвената декларация, това създава допълнителна гаранция, че изискванията на Четвъртата поправка ще бъдат удовлетворени. Виж *United States v. Hill*, 459 F.3d 966, 976 (9th Cir. 2006); *United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000) F.3d 630, 637 (9th Cir. 2000) („клетвената декларация обяснява защо е

било необходимо да се изземе цялата компютърна система“ и „оправдава изнасянето на цялата система поради периода от време, експертизата и контролираната среда, необходими за провеждането на анализа“); *United States v. Adjani*, 452 F.3d 1140, 1149 n.7 (9th Cir. 2006). Както се отбелязва по-нататък, фактите, които оправдават изнасянето на медия за съхранение за проверка извън мястото на провеждане на обиска, не трябва да изискват от служителите някакъв специален „протокол“, за да могат да проверят медията и да намерят улика, която попада в обсега на съдебната заповед. Вместо това в клетвената декларация просто трябва да се отбележи, че може би ще бъде необходим преглед извън мястото на обиска.

Да не се поставят ограничения върху съдебните техники, които могат да се използват при обиск

Ограничения върху технологиите за претърсване потенциално могат сериозно да попречат на правителството да разкрие електронно доказателство. „Обискът може да бъде изкуство, а не само наука“, *United States v. Brooks,* 427 F.3d 1246, 1252 (10th Cir. 2005), а съдебният процес може да изисква детективска работа, включително интуиция и бърза преценка при вземането на решение въз основа на онова, което следователят е видял в дадения момент, и каква трябва да бъде следващата крачка.

Едно особено тежко ограничение, което може да се постави на съдебен следовател, е изискването следователят да ограничи търсенето си до файлове, които съдържат определени ключови думи. Съдебните анализи могат да включват търсене по ключови думи, но един правилно проведен съдебен анализ рядко ще приключи с това, тъй като търсенията по ключова дума няма да намерят много видове файлове, които попадат в обсега на съдебната заповед. Например по време на писането на този текст редица типове файлове като TIFF файлове и някои PDF файлове не могат да се търсят по ключови думи. Виж *United States v. Evanson*, 2007 WL 4299191, at *5 (D. Utah Dec. 5, 2007) (където се отбелязва, че при претърсването някои файлове „са в „TIFF формат“, дигитална картина на хардкопие на документа, който е сканиран“, и че тези файлове „имат номера вместо разпознаваеми имена, които изрично описват данните във файловете“). Освен това търсенията по ключова дума могат да бъдат затруднени от използването на кодови думи или дори случайни правописни грешки. Правните и инвеститорски фирми – и естествено, индивидите, които се занимават с престъпна дейност – често пъти използват кодови думи за обозначаване на общности, лица и специфични бизнес споразумения в документи и комуникации; понякога значението на такива термини се разбира едва след като започне внимателен преглед на всеки файл поотделно. Всеки, който ползва търсачките Westlaw или LEXIS, е запознат с трудността да се измислят ключови думи, които да намерят от първия път търсеното дело; също толкова неизпълнимо е да се иска от съдебен следовател да намери важна улика с търсене по ключова дума преди съдебния анализ.

Упълномощени от съда съдебни протоколи също са ненужни, тъй като следователите действат в условия на значителни конституционни ограничения. Както и при всеки обиск, „начинът, по който е изпълнена съдебната заповед, е обект на последващ съдебен преглед относно неговата основателност". *Dalia v. United State*s, 441 U.S. 238, 258 (1979); *United States v. Ramirez*, 523 U.S. 65, 71 (1998) („Крайъгълният камък за основателност, който е водещ в Четвъртата поправка ... е водещ и при метода на изпълнение на съдебната заповед."); *Hill*, 459 F.3d at 978 („основателността на действията на полицая при изпълнение на съдебната заповед и при провеждането на последвалия обиск на иззети материали е обект на съдебна проверка").

Някои магистрати издават съдебни заповеди за претърсване на компютри с ограничения само по отношение на начина, по който изземата медия може впоследствие да бъде проверена. Например някои магистрати изискват съдебният анализ да приключи в определен период от време. Освен това някои магистрати могат да откажат да подпишат съдебна заповед, в която няма протокол, в който се уточнява как правителството ще изследва медията, за да намери доказателството, което влиза в обхвата на съдебната заповед. Нито Правило 41, нито Четвъртата поправка изискват от магистратите да налагат такива ограничения, а прокурорите трябва да се противопоставят на тях, когато те значително накърняват способността на правителството да получи доказателство, което попада в обсега на съдебната заповед. Докато може би е полезно клетвената декларация да съдържа някаква обща информация, която да оправдае конкретни стъпки, предприети по време на обиска – например да се опише колко лесно уликата може да бъде укрита в компютъра, да се обясни необходимостта от претърсване извън мястото на обиска или да се оправдае изземването на смесени документи – нито заявката за съдебната заповед, нито клетвената декларация трябва да съдържат специални ограничения върху това как служителите търсят нещата, описани в съдебната заповед.

Всяко значително ограничение (като ограничения до ключови думи) върху техниките, които правителството може да използва, за да намери улика, която попада в обсега на съдебната заповед, противоречи на прецедент на Върховния съд. Върховният съд излиза със становище, че „Нищо в езика на Конституцията или в решенията (на Върховния съд), които интерпретират този език, не подсказва, че освен изискванията, зададени в текста (на Четвъртата поправка), съдебните заповеди трябва да включват спецификация за точния начин, по които те трябва да бъдат изпълнени". *United States v. Grubb*s, 547 U.S. 90, 98 (2006) (quoting *Dalia*, 441 U.S. at 255). „Това ще разшири клаузата за съдебната заповед дотам, че да изисква, независимо дали е вероятно да бъдат нарушени права по Четвъртата поправка, съдът да посочи с точност процедурите, които изпълнителните служители трябва да следват." *Dalia*, 441 U.S. at 258. По-нататък, всяко ограничение на способността на правителството да намери улика, която попада в обсега на съдебната заповед, е несъвместимо с правилото, че „контейнерът, в който може да се крие обектът на обиска, разрешен със съдебната запо-

ред, може да бъде отворен незабавно; заинтересоваността на индивида да запази личното си пространство трябва да отстъпи пред увереността на магистрата за наличието на достатъчно основание". *United States v. Ross*, 456 U.S. 798, 823 (1982).

Магистрати, които изискват от правителството да направи протокол за съдебен анализ, обикновено се позовават върху решението на Върховния съд по делото *Andresen v. Maryland,* 427 U.S. 463 (1976), в което Съдът отбелязва, че когато съдебните заповеди дават право да се изземват документи, „отговорните служители, включително съдебните служители, трябва да внимават и да гарантират, че те се провеждат по начин, който свежда до минимум нарушенията на личното пространство, които не са упоменати в съдебната заповед". Въз основа на *Andresen* е уместно магистратите строго да налагат клаузата за конкретност в компютърни дела, свързани със смесени документи. Въпреки това обаче нищо в *Andresen* не дава право на магистратите да контролират начина, по който съдебната заповед е изпълнена, и такъв контрол е отхвърлен от съда в делата *Dalia* и *Grubbs*. Освен това съдът в *Andresen* признава, че е необходимо да се прегледат „безобидни документи … за да се определи дали те попадат всъщност сред документите, за които има разрешение да бъдат иззети". *Andresen*, 427 U.S. at 482 n.11.

Апелативните съдилища приемат съдебни заповеди за обиск, които не съдържат нито протокол (списък на стъпките, които следователят е длъжен да предприеме, за да започне да проверява компютъра), нито обяснение за липсата на такъв. В *United States v. Giberson,* 527 F.3d 882 (9th Cir. 2008) съдът подкрепя изземване на компютър и последващото му претърсване за конкретно описани документи, въпреки че те са смесени с други файлове, без да изисква никакъв протокол. Становището на съда е, че „потенциалното смесване на материалите не оправдава изключение от засилените процедурни защити за компютри отвъд изискването за основателност в Четвъртата поправка". В *United States v. Hill,* 459 F.3d 966 (9th Cir. 2006) обвиняемият оспорва претърсването на компютъра му с твърдението, освен всичко останало, че съдебната заповед е била невалидна, защото „в нея няма протокол за претърсването, който да ограничи възможността на полицая какво може да проверява, когато претърсва компютъра на обвиняемия". Съдът излиза със становище, че не е бил необходим протокол за обиска и също така не е било необходимо да се обяснява отсъствието на протокол за обиск в заявката за съдебна заповед. Десетият федерален апелативен съд подчертава в *United States v. Brooks*, 427 F.3d 1246 (10th Cir. 2005), че докато съдебните заповеди трябва да описват „с подробности обектите на своето претърсване", методологията, използвана за намирането на тези обекти, няма нужда да бъде описвана: „Този съд никога не е изисквал съдебната заповед да съдържа подробно разработена стратегия на обиска". В *United States v. Khanani*, 502 F.3d 1281, 1290-91 (11th Cir. 2007) Единадесетият федерален апелативен съд отхвърля аргумента, че в съдебната заповед е трябвало да има протокол за обиска, като обръща внимание

на внимателните стъпки, предприети от служителите за съответствие със съдебната заповед. („Докато ние сме съгласни, че може би има случаи, когато методология или стратегия на обиска би била полезна или необходима, отказваме да подкрепим твърдението, че липсата на методология или стратегия на обиска автоматично прави невалидна съдебната заповед."); *United States v. Upham*, 168 F.3d 532, 537 (1st Cir. 1999) („Процесът на съдебна заповед е заинтересуван на първо място да идентифицира какво може да бъде претърсено или иззето – а не как."). Различно е становището на съдиите в *United States v. Payton*,(9th Cir. July 21, 2009) – че претърсването на компютър без изрично разрешение е нарушение на Четвъртата поправка, тъй като нищо в претърсвания дом не е сочело, че документите, попадащи в обсега на съдебната заповед, ще бъдат намерени в компютъра и че съдиите, издаващи съдебни заповеди за претърсване на компютри, „може би трябва да поставят условия за начина и продължителността на такива претърсвания".

Ако стратегията за обиск е описана в съдебната заповед, в нея трябва ясно да се запише, че тази стратегия е илюстрация, а не „спецификация на точния начин, по който съдебната заповед ще бъде изпълнена". *Grubbs, 547 U.S. at 98.* И наистина, един съд излиза със становище „протоколите за обиск и ключовите думи не са „материални" по смисъла на Правило 16(a)(1)(E) и следователно не са откриваеми. *United States v. Fumo, 2007 WL 3232112, at *7 (E.D. Pa. Oct. 30, 2007).*

На последно място, ако магистратът откаже да издаде съдебна заповед, без да включи в нея някои изисквания за нейното изпълнение, и ако служителите на правоохранителните органи решат все пак да я изпълнят, те не трябва да пренебрегват изискванията. Виж *United States v. Brunette*, 76 (D. Maine 1999), (1st Cir. 2001) (правителството не е спазило времевите ограничения за проверка на иззети компютри, въпреки че в съдебната заповед изрично са били вписани такива времеви ограничения).

Разрешение за забавено уведомяване за съдебна заповед

При положение че са изпълнени някои условия, съдът може да издаде така наречените „нелегални" съдебни заповеди, които не изискват от служителите да уведомят по времето на обиска лицето, чиито помещения се претърсват. Нито Четвъртата поправка, нито Правило 41 задължават полицая, който изпълнява съдебна заповед, да представи на собственика копие от съдебната заповед, преди да проведе търсенето. *United States v. Grubbs,* 547 U.S. 90, 98-99 (2006). Освен това според Глава 18, Кодекс на САЩ, параграф 3103а съдът може да разреши забавяне на уведомлението, свързано с изпълнение на съдебна заповед, ако намери „основателна причина" да смята, че представянето на уведомление за изпълнение на съдебната заповед може да има една от неблагоприятните последици, изброени в Глава 18, Кодекс на САЩ, параграф 2705: заплаха за живота или физическата безопасност на даден индивид, бягство от съдебно преследване,

фалшифициране на улики, заплашване на свидетели или други спънки пред провеждането на разследването.

Правоприлагащите органи са длъжни да представят забавеното уведомление в „разумен срок, който не трябва да надхвърля 30 дни след датата на изпълнение на съдебната заповед", или съответно „на по-късна дата, ако фактите по делото оправдават по-дълъг срок на отлагане". Глава 18, Кодекс на САЩ, параграф 3103a(b)(3). Този първоначален период може да бъде удължен „при разумно основание" след „аргументиране на необходимостта от по-нататъшно отлагане"; такива забавяния са „ограничени за период от 90 дни или по-малко, освен в случаите, когато фактите по делото оправдават по-дълъг срок на забавяне". Глава 18, Кодекс на САЩ, параграф 3103a(c).

В раздел 3103a се въвежда разграничение между забавяне на уведомление за обиск и забавяне на уведомление за изземване. И наистина, освен ако съдът не намери „основателна необходимост" за изземване, съдебните заповеди, издадени по този раздел, трябва да забраняват изземване на каквато и да е материална собственост, жична или електронна комуникация или каквато и да е съхранена жична или електронна информация. Според Конгреса, ако следователите са искали да направят нелегални копия на информацията, съдържаща се в компютъра на заподозрения, те са щели предварително да поискат разрешение от съда.

Многократни съдебни заповеди при обиски в мрежата

Служителите трябва да получат многократни съдебни заповеди, ако имат основание да смятат, че търсене в мрежата ще изтегли данни от различни локации.

Магистрат, който се намира в даден съдебен окръг, може да издаде заповед за обиск за „претърсване на собственост ... в границите на окръга" или „претърсване на собственост ... извън границите на окръга, ако собствеността ... е в границите на окръга, когато е поискана заповедта, обаче може да се премести извън окръга преди изтичането на срока на съдебната заповед". Според Правило 41, в дефиницията на „собственост" се включва „информация", а Върховният съд поддържа становището, че „собственост", както е описана в Правило 41 включва нематериална собственост като компютърни данни. Виж *United States v. New York Tel*. Co., 434 U.S. 159, 170 (1977). Въпреки че съдилищата не са заели категорична позиция по въпроса, езикът на Правило 41, в съчетание с тълкуването на Върховния съд за „собственост, може да ограничи търсенето на компютърни данни до данни, които са на територията на окръга по времето на издаването на съдебната заповед.

Териториално ограничение за претърсване на компютърни данни представлява проблем за правоприлагащите органи, тъй като компютърните данни, които се съхраняват в компютърна мрежа, могат да се намират

навсякъде по света. Например полицаи, които претърсват офис в Манхатън по съдебна заповед, издадена от Южния окръг на щата Ню Йорк, могат да седнат на терминала и да стигнат до информация, която се съхранява далеч в компютър, намиращ се в някъде в Ню Джърси, Калифорния, и дори в чужбина. Определен файл, описан в съдебната заповед, може да се намира навсякъде на планетата или може да бъде разпръснат на различни места, в различни окръзи или държави. Още по-лошо, полицаите може да нямат възможност да знаят, когато осъществяват претърсването, дали данните, които изземат, се съхраняват в границите на окръга или извън него. В някои случаи полицаите може и да успеят да разберат къде се намират данните преди претърсването, но в други ще узнаят мястото на съхранение на данните едва след като приключат претърсването.

Когато служителите могат да узнаят преди претърсването, че част от данните или всички данни, описани в съдебната заповед, се съхраняват на друго място, тогава най-уместният начин на действие зависи от това къде се намират те. В случай че данните се съхраняват в две или повече места в САЩ и техните територии, служителите трябва да получат допълнителни съдебни заповеди за всяко място, където се намират данните, за да гарантират точното спазване на Правило 41(а). Например, ако данните се съхраняват в два различни окръга, служителите трябва да вземат съдебни заповеди и от двата окръга.

Когато служителите разберат преди обиска, че част от данните или всичките данни се съхраняват някъде далеч извън САЩ, нещата стават още по-сложни. Съединените щати може би ще трябва да предприемат някакви действия в диапазона от формално уведомяване до официална молба за съдействие от страна на съответната държава. По-нататък, някои държави може би ще възразят срещу опитите на правоприлагащите органи на САЩ да получат достъп до компютри на тяхна територия. Въпреки че според американския служител, който провежда обиск в САЩ в съответствие с валидна съдебна заповед, обискът е вътрешна работа, то други държави могат да имат различно мнение по въпроса. Служителите и прокурорите трябва да се свържат с Международния отдел и да потърсят помощ при решаването на тези сложни въпроси.

Когато служителите не знаят и не биха могли да знаят, че данните, които търсят в един окръг, в действителност се намират в друг окръг, доказателството, намерено в другия окръг, обикновено няма да доведе до неговото отхвърляне. Основанията за това са двояки. Първо, съдът може да реши, че служителите, които се намират в даден окръг, претърсват компютър в този окръг и непреднамерено правят така, че невеществена информация да бъде изпратена от втория окръг в първия, са спазили Правило 41(а). Виж *United States v. Ramirez, 112 F.3d 849, 852 (7th Cir. 1997) (Posner, C.J.)* (приема разрешителен режим на териториалните клаузи в Глава III).

Второ, дори ако съдът реши че обискът нарушава Правило 41(а), нарушението няма да доведе до отхвърляне на доказателството, освен в слу-

чай, когато служителите преднамерено и умишлено са нарушили правилото или когато нарушението води до „вреда“ в смисъл, че обискът е нямало изобщо да се проведе или е нямало да бъде толкова „оскърбителен“, ако се е спазвало правилото. Виж *Herring v. United States,* 129 S. Ct. 695, 702 (2009) (изключение се прилага в дела по Четвъртата поправка само в случаите, ако поведението на полицията е „достатъчно преднамерено, така че изключението може значително да го възпре, и достатъчно осъдително, че такова възпиране да си заслужава цената, платена от съдебната система“). Според широко прилагания тест *Burke* съдът обикновено отказва исковете за изземване, когато служителите, които провеждат обиска, не могат да знаят, че нарушават Правило 41, било то правно, или фактически. Виж *Martinez-Zayas*, 857 F.2d at 136 (заключение, че обискът е издържал теста *Burke*, предвид несигурното отношение на закона към това дали поведението нарушава Правило 41(а)“). По подобен начин доказателство, получено при обиск в мрежа, който достига до данни в повече от един окръг, не трябва да доведе до изземване на доказателството, освен ако служителите преднамерено и умишлено са нарушили Правило 41(а) или са причинили щета. Виж *United States v. Trost*, 152 F.3d 715, 722 (7th Cir. 1998) („трудно е да се предвиди нарушение на Правило 41 освен в случаите на грешка, която нарушава клаузата за съдебната заповед в Четвъртата поправка, което би наложило изземване“).

3. АНАЛИЗ НА ДОКАЗАТЕЛСТВАТА

Двуетапен обиск

В голяма част от случаите съдебният анализ на твърдия диск (или друга компютърна медия) изисква твърде много време, за да може да се проведе на място по време на първоначалното осъществяване на обиска. Затова обикновено следователите трябва да изнесат медията за съхранение за анализ навън, за да се определи коя информация съответства на съдебната заповед. Този процес има два етапа: образна диагностика, в която се копира целият твърд диск, и анализ, при който от твърдия диск се подбират документите, които отговарят на съдебната заповед.

Резултат от образната диагностика е създаването на „огледално копие“ на твърдия диск – копие, което „възпроизвежда всеки бит и байт на драйва, включително всички файлове, луфтове и метаданни в същия порядък, в който се появява в оригинала“. *United States v. Vilar,* 2007 WL 1075041.

След образната диагностика започва вторият етап на процеса на съдебния преглед: изследва се копието на твърдия диск и се уточняват данните, които попадат в обсега на съдебната заповед. В случаите на компютърни претърсвания, където целта на анализа извън мястото на обиска е да определи дали информацията, която се съхранява в компютърната медия,

попада в обсега на съдебната заповед, съдът третира съдебния анализ, който се провежда навън, като продължение на обиска, който все още се подчинява на Четвъртата поправка. Виж *United States v. Syphers*, 426 F.3d 461, 468 (1st Cir. 2005) (където съдебният преглед на изъят компютър се нарича „обиск"); *United States v. Mutschelknaus,* 564 F. Supp. 2d 1072, 1076 (D.N.D. 2008) (където съдебният анализ се нарича „последващ обиск"); *United States v. Triumph Capital Group*, Inc., 211 F.R.D. 31, 66 (D. Conn. 2002) (където проверката на копието на твърдия диск се нарича „обиск").

След като изъетият със съдебна заповед компютър е проверен и се определят документите в него, които попадат в обсега на съдебната заповед, последващият анализ на тези документи не би трябвало да намесва Четвъртата поправка. Както обяснява Деветият федерален апелативен съд, „когато даден артикул, който е лично притежание, е законно изъят и претърсен, последващите претърсвания на този артикул, доколкото той остава в непрекъснато и законно притежание на полицията, могат да се проведат без съдебна заповед". *United States v. Turne*r, 28 F.3d 981, 983 (9th Cir. 1994).

Търсене сред смесени документи

Малко компютри са предназначени за една-единствена цел; по-скоро компютрите могат да изпълняват редица функции, като „пощенски услуги, джубоксове, форуми за игри, за срещи, за театрални програми, за дневен график, за пазаруване, виртуални дневници и други". *United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007). Затова почти всеки твърд диск, обект на изследване от правоприлагащите органи, ще съдържа документи, които нямат нищо общо с разследването. Четвъртата поправка обуславя начина, по който следователите могат да търсят сред смесени документи, за да отделят онези документи, които са обект на съдебната заповед.

Върховният съд отбелязва, че при претърсване на смесени документи „сигурно някои безобидни документи ще бъдат проучени поне повърхностно, за да се прецени дали те всъщност са сред онези документи, за които има разрешение да бъдат изъети". *Andresen v. Maryland,* 427 U.S. 463, 482 n.11 (1976). Следователно „отговорните висши чиновници, включително съдебните, трябва да вземат мерки, които да гарантират, че (тези претърсвания) се извършват по начин, който свежда до минимум неупълномощени нахлувания в личното пространство" (пак там).

След допускането в делото *Andresen*, че „безобидни" документи могат да бъдат „бегло" проучени, съдилищата разработиха ръководства за това как служителите да проучват смесени документи, за да намерят документи, които попадат в обсега на съдебната заповед. Водещият процес е *United States v. Heldt*, където се допуска „кратък прочит" на всеки документ и се изисква „прочитът да се прекрати, когато се изясни неприложимостта на съдебната заповед към всеки документ". *United States v. Heldt*, 668

F.2d 1238, 1267 (D.C. Cir. 1982); *United States v. Giannetta*, 909 F.2d 571, 577 (1st Cir. 1990) („полицията може да претърсва ... картотеки, документи и подобни артикули и бегло да прочетат съдържанието им, за да провери дали те попадат сред артикулите, които трябва да бъдат иззети"); *United States v. Ochs*, 595 F.2d 1247, 1258 (2d. Cir. 1979) („известен прочит, обикновено достатъчно кратък"). Ако даден документ е извън обсега на съдебната заповед, обаче независимо от това е уличаващ в някакво престъпление, *Heldt* дава право за „изземването" на този документ само ако по време на този бегъл прочит „уличаващото естество на документа стане очевидно". *Heldt*, 668 F.2d at 1267.

Подобни разсъждения се прилагат и към претърсванията на компютри. Виж *United States v. Khanani*, 502 F.3d 1281, 1290 (11th Cir. 2007) (приема претърсване, в което „компютърният специалист изключва файлове, които няма вероятност да съдържат материали от обсега на съдебната заповед"); *Manno v. Christie*, 2008 WL 4058016 (приема, че е „уместно служителят да прегледа накратко всеки електронен документ, за да реши дали попада сред материалите, упълномощени в съдебната заповед, по същия начин както би могъл да направи, ако претърсва файлове на хартия"); *United States v. Potts,* 559 F. Supp. 2D 1162 (съдебната заповед не упълномощава прекалено широко претърсване, когато дава право на следователя „да претърсва компютъра, като … отваря или преглежда набързо първите няколко страници на такива файлове, за да определи съдържанието им"); *United States v. Fumo,* 2007 WL 3232112 („протоколите за претърсването и ключовите думи не очертават външните граници на законния обиск; точно обратно, поради естеството на компютърните файлове правителството може законно да отвори и набързо да проучи всеки файл, когато претърсва компютър с валидна съдебна заповед"). Когато стане необходимо следователят лично да проучи компютърен файл, за да определи дали той попада в обсега на съдебната заповед, той трябва да предприеме всички необходими стъпки, за да анализира внимателно файла, обаче следователят трябва да прекрати проверката на файла веднага щом се изясни, че съдебната заповед не се отнася до този файл.

Някои по-стари дела като че ли указват, че когато служителите, които извършват обиска, попаднат на смесени документи, те трябва да изземат документите и след това да потърсят допълнително упълномощаване от страна на магистратите, преди да продължат. Например Деветият федерален апелативен съд, когато пише за претърсване на хартиени файлове във време, преди компютърните претърсвания да станат обичайни, намеква, че в „сравнително редки случаи", когато „документите са толкова смесени, че не е възможно да бъдат сортирани на място", правоприлагащият орган „може да избегне нарушаване на правата по Четвъртата поправка, като запечата и задържи документите в очакване на разрешение от магистрата за по-нататъшно претърсване". *United States v. Tamura*, 694 F.2d 591, 595-596 (9th Cir. 1982). Десетият федерален апелативен съд внушава, че същата процедура може да се следва при пре-

търсванията на компютри. Виж *United States v. Carey,* 172 F.3d 1268, 1275 (10th Cir. 1999) („полицаите могат да запечатат или задържат документите в очакване на разрешение от магистрат за условията и ограниченията на по-нататъшното търсене сред документите“). И двата съда впоследствие уточняват, че процедура, в която първоначалната съдебна заповед установява критериите за преглед извън мястото на обиска, е недостатъчна. Виж *United States v. Hay,* 231 F.3d 630, 637 (9th Cir. 2000) (клетвена декларация, която установява „защо е било необходимо да се изземе цялата компютърна система“ и „обосновава изнасянето на цялата система“ с разрешение на магистрат, „обезсмисля *United States v. Tamura*“). *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005) („не сме искали конкретно предварително разрешение в духа на *Carey* при всяко претърсване на компютър“).

Анализ с използване на съдебен софтуер

При положение че съдебният експерт се опитва да намери данни, съответстващи на съдебната заповед, Четвъртата поправка не ограничава техниките, които експертът използва, за да проучи твърдия диск.

„Компютърното претърсване може да бъде толкова широко, колкото разумно е необходимо, за да се установи местоположението на артикулите, описани в съдебната заповед.“ *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006). Доколкото съдебният експерт се опитва да открие данни, които отговарят на съдебната заповед, Четвъртата поправка не ограничава техниките, които експертът използва. Използването на съдебен софтуер, независимо колко е „сложен“ той, също не нарушава Четвъртата поправка. Виж *United States v. Long*, 425 F.3d 482, 487 (7th Cir. 2005) („невъзможно е да се претърсва компютърен хардуер или софтуер, без да се използва някакъв вид софтуер“, и „фактът, че търсачката е сложна, не е от значение.“)

Дори когато обвиняемият е предприел стъпки, за да скрие улика на твърдия диск, съдебният преглед, който я разкрива, не нарушава разумното очакване за поверителност, доколкото съдебната заповед разрешава претърсване на твърдия диск за тази улика. Например прочитането на изтрити файлове посредством проучване на незаетото място на диска се приема в съда. Виж *United States v. Upham*, 168 F.3d 532, 537 (1st Cir. 1999) („възстановяването от правоприлагащия орган на незаконни изображения след опит за тяхното унищожаване не е по-различно от декодирането на шифровано съобщение, законно прихванато, или слепването на скъсаните части на случайна бележка“).

Промени в насоката на разследването и необходимост от нови съдебни заповеди

Даден компютър може да участва в редица типове престъпления, така че твърдият диск на компютъра може да съдържа улики за различни престъпления. Въпреки това обаче, когато служителят претърсва компютъра със съдебна заповед, често пъти съдебната заповед разрешава претърсване на компютъра само за търсене на улики за определено престъпление. Ако служителят попадне на улика за престъпление, което не е упоменато в съдебната заповед, би било предпазна мярка от негова страна да получи втора съдебна заповед. В *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999) детективите получават съдебна заповед да претърсят компютъра на обвиняемия за улики за продажба на наркотици. Докато осъществява претърсването в полицейското управление, детективът разкрива снимки с детска порнография. Тогава детективите зарязват „търсенето на свързана с наркотиците улика“ и вместо това претърсват целия твърд диск за улики за детска порнография. Десетият федерален апелативен съд отхвърля детската порнография със становището, че търсенето на улики за детска порнография излиза извън първоначалния обсег на съдебната заповед. Може да се направи сравнение между делата *Carey* и *United States v. Walser*, 275 F.3d 981, 986-87 (10th Cir. 2001) (поддържа претърсването, когато полицаят със съдебна заповед да претърси компютър за улики за търговия с наркотици открива детска порнография в компютъра, преустановява претърсването и след това се обръща към магистратите за втора съдебна заповед за търсене на улики за детска порнография) и *Gray*, 78 F. Supp. 2d at 530-31 (поддържа претърсването, когато служител се натъква на детска порнография в хода на търсене на улики за хакерска дейност и след това иска втора съдебна заповед, за да претърси компютъра за детска порнография).

Впоследствие Десетият апелативен съд определя *Carey* като „просто подкрепящ твърдението, че правоприлагането не може да надхвърля обсега на съдебната заповед отвъд нейното първоначално основание“. *United States v. Grimmett*, 439 F.3d 1263, 1268 (10th Cir. 2006). По нататък *Grimmett* насочва анализа не към субективното намерение на служителя, а към онова, което съдебната заповед оправдава. Видимо, фокусът на *Carey* върху субективното намерение на служителя отразява един в някаква степен остарял възглед за Четвъртата поправка. Върховният съд отказва да разгледа субективното намерение на служителя и вместо това се съсредоточава върху това дали обстоятелствата, разгледани обективно, оправдават поведението на служителя. Виж също така Brigham City v. Stuart, 547 U.S. 398, 404 (2006) („Дадено действие е „основателно“ според Четвъртата поправка независимо от душевното състояние на съответния служител, доколкото обстоятелствата, обективно погледнато, оправдават действието.“).

Въз основа на тези прецеденти редица съдилища посочват, че субективното намерение на служителя по време на изпълнение на съдебна заповед не може да определи дали обискът надхвърля обсега на съдебната

заповед и нарушава Четвъртата поправка. Виж *United States v. Van Dreel*, 155 F.3d 902, 905 (7th Cir. 1998) („щом съществува достатъчно основание и е била издадена законна съдебна заповед, субективното намерение на служител при провеждането на обиска няма връзка със случая"); *United States v. Ewai*n, 88 F.3d 689, 694 (9th Cir. 1996). Според тези дела правилното разследване е дали, погледнато обективно, обискът, който служителите са провели, в действителност съответства на съдебната заповед, която са получили. Субективното намерение на служителя или „няма връзка" *Van Dreel*, 155 F.3d at 905, или е само един фактор, определящ становището „дали полицията е свела обиска си до разрешеното в съдебната заповед*". Ewain*, 88 F.3d at 694.

Въз основа на обективния стандарт за поведението на служителите възниква вътрешно напрежение между *Carey* и дела като *Hill, 322 F. Supp. 2d at 1090,* където се признава че „няма начин да се знае какво има в даден файл, преди да се проучи съдържанието му". Този факт, в съчетание с принципа, че „даден контейнер, който може да съдържа обект на търсене, разрешен със съдебна заповед, може да бъде отворен незабавно", *United States v. Ross*, 456 U.S. 798, 823 (1982), навежда на мисълта, че не би трябвало да бъде необходимо да се търси втора съдебна заповед след откриването на улика за друго престъпление. Въпреки това обаче, тъй като *Carey* не е отменено, остава препоръчително да се търси втора съдебна заповед при откриване на друго престъпление, което не е упоменато в първоначалната съдебна заповед.

Разрешени времеви срокове за проучване на иззета медия

Нито Четвъртата поправка, нито Правило 41 налагат някакво специално ограничение върху срока за провеждане на съдебното проучване от правителството. Правителството обикновено може да задържи изземания компютър и да проучи съдържанието му по внимателен и обмислен начин, подчинявайки се единствено на изискването за разумност в Четвъртата поправка, а разумността на търсенето на правителството се обуславя от това дали възможната причина за претърсването е изчезнала. Отсъствието на специфична времева рамка за съдебното проучване се потвърждава от нова поправка в Правило 41(е), която се очаква да влезе в сила през декември 2009:

Съдебна заповед по Правило 41(е)(2)(А) може да даде разрешение за изземване на електронна медия за съхранение или изземването или копирането на електронно съхранена информация. Освен ако специфично не е упоменато друго, съдебната заповед дава право за последващ преглед на медията или на информацията в съответствие със съдебната заповед. Времето за изпълнение на съдебната заповед в Правило 41(е)(2)(А) и (f)(1)(А) се отнася до изземването или копирането на място на информацията

от медията, а не до по-късното копиране и проучване извън мястото на обиска.

Съдебните състави на различните съдилища са единодушни, че нито Четвъртата поправка, нито Правило 41 поставят изрично ограничения върху времетраенето на който и да е съдебен анализ и са разрешавали съдебните анализи да започнат месеци след като следователите изземат компютър или данни.

Четвъртата поправка изисква съдебният анализ на компютъра да се проведе в рамките на разумен срок. Виж *United States v. Mutschelknaus*, 564 F. Supp. 2d 1072, 1077 (D.N.D. 2008) („Федералните правила за наказателна процедура не изискват съдебният анализ на компютри или други електронни съоръжения да се проведе в определен период от време. Всяко последващо претърсване само трябва да се проведе в рамките на разумен срок."); *Burns,* 2008 WL 4542990, at 8 („Забавянето във времето трябва да бъде разумно, но няма конституционна горна граница за разумност."). Когато преценява разумния срок за съдебен анализ, съдът може да вземе предвид, че анализът на компютър е труден и продължителен процес. Виж *Triumph Capital Group, Inc*., 211 F.R.D. at 66 (срокът за завършване на претърсването е разумен и „претърсванията на компютър не са и не могат да бъдат обект на каквото и да е строго времево ограничение, тъй като са свързани с много повече информация, отколкото обикновеното проучване на документи, изискват по-голяма подготовка и повече внимание при изпълнението").

Важно е да се подчертае, че съдът обикновено се отнася към изчезването на достатъчното основание като основен критерий за „разумността" на срока на проучването според Четвъртата поправка. Например в *United States v. Syphers*, 426 F.3d 461 (1st Cir. 2005) Първият федерален апелативен съд заявява, че Четвъртата поправка „не съдържа изисквания за това кога ще се случи обискът или претърсването, нито за неговата продължителност, но предупреждава, че „неразумното забавяне на изпълнението на съдебната заповед, което води до изчезване на достатъчното основание, ще направи незаконна съдебната заповед". Трябва да се отбележи обаче, че изчезването на достатъчното основание е малко вероятно в случаите на претърсване на компютър, тъй като уликата е „замразена във времето", когато медията за съхранение е копирана или иззета.

Обаче някои съдии възприемат различен възглед по въпроса и отказват да подпишат съдебни заповеди за обиск, които разрешават изземване на компютри, освен в случаите, когато правителството проведе съдебното проучване в кратък период от време, например тридесет дни. Някои съдии налагат още по-кратки времеви срокове като седем дни, а други налагат изрични срокове във времето, когато служителите подават молба за съдебна заповед за изземване на компютър от действащ бизнес. В подкрепа на тези ограничения някои магистрати изразяват загриженост, че може би е конституционно „неразумно" по Четвъртата поправка правителството

да лишава индивидите от техните компютри, освен за кратък период от време.

Прокурорите трябва да се съпротивляват на такива ограничения. Законът не дава изрично право на магистратите да издават съдебни заповеди, които налагат времеви ограничения върху проучването от правоприлагащите органи на иззета улика, и правото на магистратите да налагат такива ограничения може да се постави под въпрос, особено в светлината на предстоящата поправка в Правило 41, че времето за изпълнението на съдебната заповед „се отнася до изземването и копирането на място на медията или на информацията, а не към което и да е последващо копиране или преглед извън мястото на обиска". Както Върховният съд препоръчва в едно по-ранно дело, правилният подход е магистратите да издадат съдебна заповед въз основа на съществуването на достатъчно основание, а след това да оставят страните впоследствие да оспорват конституционните въпроси. Виж *Ex Parte United States*, 287 U.S. 241, 250 (1932) („Отказът на съда да издаде съдебна заповед … е по същество отказ да се допусне процесът по делото да започне и е почти отказ да се разреши прилагането на закона.").

Най-малко един съдебен състав е излязъл с позицията, че отхвърляне на улика е допустимо, когато правителството не успее да спази наложените от съда ограничения върху времевия период за преглед на иззети компютри. В *United States v. Brunette*, 76 F. Supp. 2d 30 (D. Me. 1999) съдията разрешава на служителите да изземат компютри на заподозрян в детска порнография при условие, че служителите ги претърсят за улика „в рамките на 30 дни". Служителите извършват обиска пет дни по-късно и изземат няколко компютри. Няколко дни преди изтичането на тридесетдневния период правителството подава молба и получава тридесетдневно удължаване на времето за преглед. След това служителите преглеждат всички с изключение на един от изземите компютри в рамките на удължения период и намират стотици снимки с детска порнография. Обаче служителите започват да преглеждат последния компютър два дни след изтичане на удължения период. Обвиняемият подава иск за отхвърляне на снимките, открити в последния компютър, с аргумента, че претърсване отвъд шестдесетдневния период нарушава условията на съдебната заповед и последвалата наредба за удължаване. Съдът приема иска, като заявява, че „защото правителството не е спазило изискванията на съдебната заповед и последвалата наредба, всяка информация, получена от компютъра, се отхвърля".

Резултатът в *Brunette* има малко основание както по Правило 41, така и по Четвъртата поправка. Дори ако приемем, че магистратът има право да налага времеви ограничения върху съдебната проверка, изглежда неуместно да наложи отхвърляне заради нарушения на такива условия, когато подобни нарушения на самото Правило 41 нямат такова последствие. Може да направим сравнение между *Brunette* и *United States v. Twenty-Two Thousand, Two Hundred Eighty Seven Dollars* ($22,287.00), *U.S. Currency, 709*

F.2d 442, 448 (6th Cir. 1983) (където съдът отказва отхвърляне в случай, когато полицаите са започнали обиска „малко след 10 вечерта", въпреки че Правило 41 постановява, че всички обиски трябва да се провеждат между 6 сутринта и 10 часа вечерта.) По подобен начин Четвъртата поправка изисква само разумност и съдиите отхвърлят искове, основани върху твърдения за забавяне като разгледаните по-горе.

Съдържание на Правило 41(f) - опис, заведен в съда

Полицаите трябва да попълват описи с квитанции, които само упоменават какви хардуерни устройства са били иззети.

Правило 41(f) изисква полицаят, който изпълнява съдебната заповед, да „подготви и провери опис на изземаните собственост" и „да върне съдебната заповед заедно с копие от описа на магистрата, подписал съдебната заповед". Понастоящем „правилата не определят задължително ниво на конкретност за описи на иззети артикули", а дали даден опис е достатъчно конкретен, е въпрос на факти. Когато се изземват документи, не е задължително в описа да се изброява всеки един от тях. Такава „специфика и конкретност не се изисква дори при крайно тълкуване на Правило 41" в светлината на изискването му описът „бързо" да бъде заведен при магистрата.

Затова в компютърните дела полицаите обикновено съставят описи с обратни квитанции, които само посочват информацията или хардуерните устройства, които са иззети, като например „огледално копие на Maxtor 500 гигабайта твърд диск". Този подход е възприет от новата поправка на Правило 41(f), която изрично казва, че „в случай, свързан с изземване на електронна медия за съхранение или копиране на електронно съхранявана информация, описът може да се ограничи до описание на физическата медия за съхранение, която е била иззета или копирана".

Съдилищата също поддържат становището, че когато правителството изземе документи или данни, като даде на обвиняемия „копие от всичко, което е било иззето", това „премахва необходимостта от подробен опис"; *United States v. Ogden*, 2008 WL 2247074, at **13 (W.D. Tenn. May 28, 2008)* (отказва иск за отхвърляне въз основа на липса на своевременен опис на претърсване на компютър, „защото обвиняемият е имал достъп до изземаните файлове, познавал е лично тези файлове и му е бил предоставен списък на файловете"). Осигуряването на обвиняемите на „достъп" до книжни документи, иззети от офиса, също „премахва необходимостта от по-подробен опис" освен онзи, който просто посочва кои картотеки са били иззети.

4. ПРЕДИЗВИКАТЕЛСТВА ПРЕД ПРОВЕЖДАНЕТО НА ОБИСК

Предизвикателства, свързани с „явно незачитане“

Понякога защитата се опитва да използва изземването на носители за съхранение на информация или смесена информация като основа за подаване на иск за отхвърляне на всички улики, получени при обиска. За да бъде овъзмезден с крайното средство на пълната супресия, обвиняемият трябва да докаже, че изземването на допълнителни материали доказва, че служителите са изпълнявали съдебната заповед при „явно незачитане на условията в нея”. Виж *United States v. Khanani, 502 F.3d 1281, 1289 (11th Cir. 2007)*; *United States v. Le,* 173 F.3d 1258, 1269 (10th Cir. 1999); *United States v. Matia*s, 836 F.2d 744, 747-48 (2d Cir. 1988). Даден обиск е извършен при „явно незачитане“ на условията, когато полицаите толкова грубо са надхвърлили обсега на съдебната заповед по време на изпълнението, че законният обиск изглежда само претекст за своеволно претърсване на частната собственост на обекта. Виж *United States v. Liu*, 239 F.3d 138 (2d Cir. 2000); *United States v. Foster*, 100 F.3d 846, 851 (10th Cir. 1996); *United States v. Young,* 877 F.2d 1099, 1105-06 (1st Cir. 1989).

Поради причини от практическо и техническо естество служителите, извършващи претърсвания на компютри, често пъти трябва да изземват хардуер или файлове освен онези, описани в съдебната заповед. Адвокатите по защитата понякога се опитват да докажат, че с изземването на повече от конкретните компютърни файлове, изброени в съдебната заповед, полицаите са проявили „явно незачитане“ към мандата, даден им от съдебната заповед.

Прокурорите могат най-добре да отговорят на исковете за „явно незачитане“, като покажат, че всяко изземване на собственост, която не е упомената в съдебната заповед, е резултат от добронамерен отговор към възникнали фактически трудности, а не е опит да се претърси произволно собствеността на обвиняемия под прикритието на ограничена съдебна заповед. Съдът приема практическите трудности, с които се сблъскват служителите, когато претърсват компютър в търсене на определени файлове, и обикновено одобрява претърсване извън мястото на обиска независимо от случаите на изземване на допълнителна собственост. Виж *United States v. Hill*, 459 F.3d 966, 974-75 (9th Cir. 2006) („полицаите ще трябва да проверят всеки един от може би хилядите файлове на диска – процес, който може да отнеме часове наред и дори дни“); *Davis v. Gracey,* 111 F.3d 1472, 1280 (10th Cir. 1997) (отбелязва „очевидните трудности при разделянето на съдържанието на електронен носител на информация (търсено като улика) от компютърния хардуер (иззет) по време на обиска“); *Henson*, 848 F.2d at 1383-84 („Не мислим, че е разумно да задължаваме полицаите да преглеждат големи масиви документи, намерени в офиса на обвиняемия, за да отделят онези няколко от тях, които не попадат

в обсега на съдебната заповед."); *United States v. Scott-Emuakpor*, 2000 WL 288443, at *7 (W.D. Mich. Jan. 25, 2000) (отбелязват се „специфичните проблеми, свързани с претърсването на компютъризирани документи", които оправдават обискиране извън мястото на обиска); *Gawrysiak*, 972 F. Supp. at 866 („Мандатът на Четвъртата поправка за разумност не изисква от полицая да прекара дни наред на мястото на обиска да преглежда екраните на компютрите, за да установи точно кои документи могат да се копират според съдебната заповед."); *United States v. Sissler*, 1991 WL 239000, at *4 (W.D. *Mich. Jan*. 25, 1991) („Полицаите не са били задължени да проверят компютъра и дисковете в къщата, тъй като пароли и други устройства за сигурност често се използват, за да се защити информацията, която се съхранява в тях. Очевидно на полицаите е било разрешено да ги изнесат от къщата, за да може компютърният специалист да се опита „да разбие" тези предохранителни мерки, процес, който изисква време и усилия. Както изземването на документи, и изземването на компютърния хардуер и софтуер е било мотивирано от съображения за практичност. Следователно тяхното изземване не представлява „явно незачитане" на ограниченията, записани в съдебната заповед"). Виж също *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) („Не е лесна задача да се претърси пълен харддиск и да се прегледа цялата информация, която се съдържа в него. Протоколът показва, че самият механизъм на търсенето на снимков материал, проведен впоследствие извън мястото на обиска, не е позволявал това да се направи на място."); *United States v. Lamb,* 945 F. Supp. 441, 462 (N.D.N.Y. 1996) („Ако някои файлове със снимки се съхраняват във вътрешния харддиск на компютъра, изнасянето на компютъра в офис или лаборатория на ФБР изглежда единственият възможен начин да се провери съдържанието му.").

Искове за връщане на собственост

Член 41(g) дава право на „ощетеното" лице да подаде иск за връщане на собствеността. Този член е от особено значение при дела, свързани с претърсването на компютри, тъй като дава възможност на собствениците на иззето компютърно устройство да заведат иск за връщане на устройството, преди да бъде предявено обвинението. В някои случаи обвиняемите завеждат такива искове, тъй като смятат, че изземването нарушава Четвъртата поправка. Ако това е така, компютърът следва да бъде върнат.

Член 41(g) също така дава право на собствениците да подадат иск за възвръщане на тяхната собственост, когато изземването е законно, но ищецът е „ощетен от това, че правителството продължително време е във владение на неговата собственост". Мултифункционалността на компютъра понякога е основание за искове въз основа на член 41(g). Например заподозрян, който се разследва за хакерство, може да заведе иск за това, че трябва да си получи обратно компютъра, за да си попълни данъчната декларация или да си провери имейла. По подобен начин фирма, заподозряна

в измама, може да подаде иск за връщане на оборудването с аргумента, че ако то не бъде върнато, бизнесът ще пострада.

Собствениците на законно иззет компютър трябва да преодолеят редица пречки, преди съдът да разпореди на правителството да върне устройството. Първо, собственикът трябва да убеди съда, че трябва да разгледа безпристрастно неговия иск. Виж *Floyd v. United State*s, 860 F.2d 999, 1003 (10th Cir. 1988) („Член 41(е) следва да се прилага внимателно и въздържано."). Въпреки че съдебните стандарти са доста различни в различните съдилища, повечето ще потвърдят валидността на заведен по член 41(g) иск само в случай, че ищецът докаже, че: (1) лишаването от собствеността му нанася „необратима щета" и (2) че в противен случай ищецът е лишен от безпристрастността на закона. Виж *In re Search of Kitty's East*, 905 F.2d 1367, 137071 (10th Cir. 1990). Ако ищецът покрие тези елементи, съдът ще разгледа основанията на иска и изземата собственост ще бъде върната само в случай, че продължителното ѝ задържане от страна на правителството причинява необратима щета. Виж *Ramsden,* 2 F.3d at 326. Това изисква съдът да прецени и да направи избор между интереса на правителството да задържи собствеността срещу интереса на собственика да си я възвърне. Виж *United States v. Premises Known* as *608 Taylor Ave.*, 584 F.2d 1297, 1304 (3d Cir. 1978).

В случай че Съединените щати имат нужда от собствеността в процеса на разследване или наказателно производство, задържането на собствеността обикновено е основателно. Обаче ако законните интереси на Съединените щати могат да бъдат защитени дори ако собствеността бъде върната, продължителното ѝ задържане би било неоснователно.

Исковe за връщане на законно иззети компютри са успешни само в редки случаи. Първо, съдът обикновено отказва да се произнесе по иска, ако правителството е предоставило на собственика електронно копие на изземите компютърни файлове. Виж, *e.g., In re Search of 5444 Westheimer Road, 2006 WL 1881370, at *2 (S.D. Tex. Jul. 6, 2006)* (отхвърляне на иск за връщане на собственост преди завеждане на наказателно дело, когато правителството е предоставило копие от изземите компютърни данни); *re Search Warrant Executed February 1, 1995, 1995 WL 406276, at *2 (S.D.N.Y. Jul. 7, 1995)* (заключение, че собственикът на изземия компютър не може да претендира за необратима щета, когато правителството му е предложило да копира съдържащите се в него файлове); виж също *Standard Drywall, Inc. v. United States*, 668 F.2d 156, 157 n.2. (2d Cir. 1982) („Ние поставяме под въпрос дали при отсъствието на изземването на уникална собственост или привилегировани документи страната може да докаже необратима щета (основание за съдопроизводство) в случай, когато правителството или предоставя на страната копия от изземите документи, или връща оригиналите и представя копията пред съда.").

Второ, съдът обикновено решава, че интересът на правителството към компютърното устройство е по-голям от този на обвиняемия в слу-

чай, когато е в ход наказателно производство или процедура за конфискация. Виж *United States v. Stowe*, *1996 WL 467238, at *1-3 (N.D. Ill. Aug. 15, 1996)* (продължителното задържане на компютър след изтичането на 18 месеца е основателно, когато правителството твърди, че разследването е в ход, а обвиняемият не е успял да предостави убедителен аргумент в полза на връщането му); *the Matter of Search Warrant for K-Sports Imports, Inc., 163 F.R.D. 594, 597 (C.D. Cal. 1995)* (където се отхвърля иск за връщане на компютърни документи поради предстояща процедура по конфискация); виж също *Johnson v. United States*, *971 F. Supp. 862, 868 (D.N.J. 1997)* (където се отхвърля иск на банка по Правило 41(е) за връщане на компютърни дискове с мотива, че банката не е вече действаща). Ако обаче правителството не възнамерява да използва компютъра в по-нататъшни производства, той трябва да бъде върнат. Виж *United States v. Moore, 188 F.3d 516, 1999 WL 650568, at *6 (9th Cir. Aug. 25, 1999)* (където се нарежда компютърът да бъде върнат, тъй като „необходимостта правителството да задържи компютъра, за да го използва в следващо производство, сега изглежда малко вероятна); *K-Sports Imports, Inc.*, *163 F.R.D. at 597.* Нещо повече, съдът може да одобри иск по Правило 41(g) в случай, че обвиняемият не може да води бизнеса си без компютърното съоръжение, а правителството може да работи напълно успешно с копия от изземите файлове

5. ПРАВНИ ОГРАНИЧЕНИЯ ЗА ИЗПОЛЗВАНЕ НА СЪДЕБНА ЗАПОВЕД ЗА ПРЕТЪРСВАНЕ

Обикновено, доколкото са спазени правилните процедури, правителството може да извърши обиск срещу всеки индивид – включително и такива, които не са заподозрени в престъпление – ако има достатъчно основание да смята, че обискът ще разкрие контрабанда или улика за престъпление. Виж *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978); *Warden v. Hayden*, 387 U.S. 294, 309 (1967). И все пак в някои случаи Конгресът и главният прокурор са наложили ограничения върху ситуациите, в които следователите могат да използват съдебна заповед за обиск, за да получат улики. Три от тези ограничения са особено приложими в сферата на компютърните претърсвания.

Журналисти и автори. Закон за защита на поверителността

Когато служителите имат основание да смятат, че обискът ще доведе до изземване на материали, свързани с дейности по Първата поправка, като издателска дейност или публикуване на материали в интернет, те трябва да вземат под внимание действието на Закона за защита на поверителността (ЗЗП). Всеки федерален компютърен обиск, свързан със ЗЗП, трябва да бъде разрешен от Департамента по правосъдие.

Съгласно ЗЗП правоприлагащите органи трябва да предприемат специални стъпки, когато планират обиск, който според служителите може да доведе до изземване на материали, свързани със свободата на словото. Федералните обиски, свързани с ЗЗП, следва да бъдат предварително одобрени от заместник-помощника на главния прокурор на Криминалния отдел. Звеното за компютърни престъпления и интелектуална собственост е контактна точка за всички такива обиски, свързани с компютри.

а) кратка история на Закона за защита на поверителността

Когато се опитваме да дешифрираме непроницаемия текст на ЗЗП, може би е полезно да разберем контекста, в който е бил приет. Преди решението на Върховния съд по делото *Warden v. Hayden*, 387 U.S. 294, 309 (1967) правоприлагащите органи не са можели да получат съдебна заповед за претърсване и изземване на „обикновено доказателство“ за престъпление. Съдебните заповеди са били разрешени само за изземване на контрабанда, предмети или плодове на престъплението. Виж *Boyd v. United States*, 116 U.S. 616 (1886). В делото *Hayden* Върховният съд обръща курса и излиза със становището, че Четвъртата поправка позволява на правителството да получи заповед за обиск, за да изземе обикновено доказателство. Това решение на съда задава основата за сблъсъка между правоприлагащите органи и пресата. Тъй като журналистите и репортерите често се натъкват на престъпна дейност по време на разработване на материалите си, те притежават „обикновено доказателство“ за престъпление, което може да се окаже полезно при криминалните разследвания. Като освобождава Четвъртата поправка от рестриктивния режим на *Boyd,* становището по делото *Hayden* създава възможност правоприлагащите органи да използват съдебни заповеди за обиск, насочени към пресата за изземване на улики за престъпление, събрани в процеса на проучване и публикуване на журналистически материали.

Много скоро такъв обиск се провежда. На 12 април 1971 Окръжният съд на Санта Клара, Калифорния, получава съдебна заповед за претърсване на офиса на „Станфорд Дейли”, студентския вестник на университета „Станфорд”. Окръжната прокуратура разследва кръвопролитен сблъсък между полицията и демонстранти в университетската болница три дни по-рано. Вестник „Станфорд Дейли” отразил инцидента и пуснал специално издание със снимки от сблъсъка. Смятайки, че вестникът разполага с още снимки от инцидента, които могат да помогнат да бъдат идентифицирани демонстрантите, полицията получава съдебна заповед и изпраща четирима полицаи да обискират офиса на вестника в търсене на още доказателства в помощ на разследването. Полицаите не откриват нищо. Месец по-късно обаче редакторите на „Станфорд Дейли” завеждат гражданско дело срещу полицията с аргумента, че обискът е нарушил техните права по Първата и Четвъртата поправка. Накрая делото стига до Върховния съд и в *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), Съдът отхвърля претенциите на вестника. Въпреки че отбелязва, че „Четвъртата поправка не предо-

твратява, нито препоръчва усилията от страна на законодателната или изпълнителна власт да издигнат извънконституционални защити“ срещу претърсване на пресата, Съдът постановява, че нито Четвъртата, нито Първата поправка забраняват такъв обиск.

Конгресът гласува ЗЗП през 1980 г. в отговор на делото *Stanford Daily.* Според Доклада на Сената ЗЗП осигурява на „пресата и на някои други лица, които не са заподозрени в извършване на престъпление, защити, каквито Четвъртата поправка не предоставя“. Законът има за цел да даде на издателите известни законни права, които да възпрепятстват правоохранителните органи да ги вземат на прицел само защото те често събират „обикновени доказателства“ за престъпление. Както посочва законодателната история:

Предназначението на този закон е да ограничи обиска на материали, притежавани от лица, занимаващи се с дейности по Първата поправка, за които няма подозрение за участие в престъпната дейност, във връзка с която тези материали се търсят, както и да не ограничава възможността на правозащитните служители да претърсват и изземват материали от лицата, заподозрени в извършване на разследваното престъпление.

б) обхват на Закона за защита на поверителността

С някои изключения, според ЗЗП е незаконно държавният служител да „претърсва или изземва“ материали, когато:

> а) материалите са „работен продукт“, подготвени, произведени, създадени с очакване да станат обществено достояние“, Глава 42, Кодекс на САЩ, параграф 2000aa-7(b)(1);
>
> б) материалите включват „мисловните впечатления, заключения или теории на своя създател”, Глава 42, Кодекс на САЩ, параграф 2000aa-7(b)(3), 2000aa(a); и
>
> в) материалите се притежават с цел да станат обществено достояние от лице, за което „има основание да се смята, че има за цел да разпространи в обществото“ някаква форма на „публична комуникация“, Глава 42, Кодекс на САЩ, параграф 2000aa-7(b)(3), 2000aa(a);
>
> или
>
> а) материалите са „документални материали“, които съдържат „информация“, Глава 42, Кодекс на САЩ, параграф 2000aa-7(a); и
>
> б) материалите са притежание на лице „във връзка с намерението да разпространи в обществото“ някаква форма на „публична комуникация“. Глава 42, Кодекс на САЩ, параграф 2000aa(b), 2000aa-7(a).

В такива случаи правителството е длъжно да използва призовка или друг задължителен процес вместо съдебна заповед за обиск, освен в случаите, когато действа изключение в ЗЗП.

Спектърът на приложение на ЗЗП е широк. Той не се ограничава само до журналисти: на него се позовава издател на ролеви игри, виж *Steve Jackson Games, Inc. v. Secret Service*, 816 F. Supp. 432 (W.D. Тех. 1993), и издател на „интернет базиран вестник", въпреки че претенциите на последния са отхвърлени на друго основание. Виж *Mink v. Suthers,* 482 F.3d 1244, 1257-58 (10th Cir. 2007).

Законът за защита на поверителността има няколко важни изключения:

Контрабанда. ЗЗП е неприложим към „контрабанда, облаги от престъпление или към притежавани по престъпен начин неща или собственост, определена за или използвана като средство за извършване на криминално престъпление". Глава 42 Кодекс на САЩ, параграф 2000аа-7(а), (b).

Заподозрян в престъпление. ЗЗП не се прилага в случай, когато има „вероятно основание да се смята, че лицето, притежаващо такива материали, е извършило или в момента извършва углавното престъпление, към което се отнасят материалите", въпреки че законът постановява ново изключение на изключението при дадени обстоятелства, където самото престъпление „се състои в приемането, притежаването, предаването или задържането" на въпросните материали. Виж Глава 42, Кодекс на САЩ, параграф 2000аа(а)(1), 2000аа(b)(1); *Guest v. Leis,* 255 F.3d 325, 342 (6th Cir. 2001); *DePugh v. Sutton,* 917 F. Supp. 690, 696 (W.D. Mo. 1996) („ЗЗП недвусмислено дава право на правителството да не се съобрази с изискванията на закона в тези случаи, в които лицето, заподозряно в престъпление, притежава документи, свързани с престъплението"). Материалите могат „да имат връзка" с престъпление дори когато тези връзки са някак далечни. Например в казуса *S.H.A.R.K. v. Metro Parks Serving Summit County,* 499 F.3d 553 (6th Cir. 2007), активисти на движение за защита на животните поставили скрити камери по дървета, за да заснемат планирано убийство на див елен. Свалянето (и изземването) на тези камери не нарушават ЗЗП, защото камерите, на първо място, са свързани с престъплението влизане в чужда територия, необходимо, за да бъдат поставени там.

Спешност. ЗЗП не действа в случай, че има основание да се смята, че незабавното изземване на такива материали е необходимо за предотвратяване на смърт или тежка телесна повреда. Виж Глава 42, Кодекс на САЩ, параграф 2000аа(а)(2), 2000аа(b)(2).

Призовката ще бъде неадекватна. ЗЗП не се прилага при претърсването или изземването на „документални материали" по смисъла на параграф параграф 2000аа-7(а), ако призовката се е оказала неадекватна или има

основание да се смята, че призовката няма да доведе до предоставянето на материалите, виж Глава 42, Кодекс на САЩ, параграф 2000aa(b)(3)-(4). Един съд излиза със становището, че това изключение е изпълнено, когато уличаваща видеокасета е притежание на лице, което е приятел на лицето, което видеокасетата уличава. Виж *Berglund v. City of Maplewood*, 173 F. Supp. 2d 935, 949-50 (D. Minn. 2001).

Важно е да се отбележи, че тези изключения са изключения само по отношение на ЗЗП, а не по отношение на защитите, предоставени от Четвъртата поправка изобщо. Когато се прилага изключение по ЗЗП, това означава само, че правителството може да поиска съдебна заповед – а не че правителството може да осъществи обиск без съдебна заповед. Виж *DePugh v. Sutton*, 917 F. Supp. 690, 696 (W.D. Mo. 1996).

Нарушения на ЗЗП не водят до отхвърляне на уликата, но могат да доведат до искове за граждански обезщетения, заведени срещу върховния орган, чиито служители или чиновници са осъществили обиска. *Davis v. Gracey,* 111 F.3d 1472, 1482 (10th Cir. 1997) (където се отхвърля обвинението срещу общински чиновници в личното им качество, тъй като такива дела следва да бъдат възбудени само срещу „правителствена единица", освен ако правителствената единица не се е отказала от върховния си имунитет). Ако държавни служители или чиновници нарушат ЗЗП, а държавата не се откаже от върховния си имунитет и следователно не може да бъде страна по дело, индивидуалните държавни служители или чиновници могат да бъдат подведени под отговорност в рамките на и според правомощията на поста си, като им се предостави добросъвестна защита. Виж, параграф 2000aa-6(a)(2),(b).

в) приложение на ЗЗП при претърсване и изземване на компютри

Въпроси, свързани със ЗЗП, възникват често в компютърни дела поради две причини, които е било трудно да бъдат предвидени през 1980 г., когато Конгресът приема закона. Първо, използването на персонални компютри за издателска дейност и интернет разширява невероятно обхвата на това кой „участва в дейности по Първата поправка". Днес всеки, който има компютър и достъп до интернет, може да бъде издател, който притежава защитени по ЗЗП материали в компютъра си.

Втората причина, поради която възникват проблеми със ЗЗП във връзка с компютърни дела, е, че езикът на закона не отхвърля категорично понасянето на отговорност при случайни изземвания на защитени от ЗЗП материали и такива могат да възникнат, когато служителите търсят и изземат съхранявана в компютъра контрабанда или улика за престъпление, които са смесени със защитени по ЗЗП материали. Например разследвания, водени за незаконни бизнеси, които публикуват снимки с детска порнография в интернет, разкриват, че такива бизнеси често пъти поддържат други издателски материали (като порнография за възрастни), които може да

бъдат защитени по ЗЗП. Изземването на компютъра заради пропагандата по необходимост води до изземване на защитените по ЗЗП материали, тъй като контрабандата е смесена със защитени по ЗЗП материали на компютрите в този бизнес. Ако ЗЗП се интерпретира като забраняващ такива изземвания, законът не само ще възпрепятства правоприлагащите органи да се прицелват в невинни издатели, но също и ще забрани претърсването и изземването на компютъра на заподозрян в углавно престъпление, ако в него се съдържат защитени по ЗЗП материали, дори и случайно.

Законодателната история и текстът на ЗЗП показва, че вероятно Конгресът е смятал ЗЗП да се прилага само в случаите, когато правоприлагащите органи преднамерено се насочват към материал по Първата поправка, свързан с престъпление, както в *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978). Например „изключението за заподозрян" сваля отговорността по ЗЗП, когато „съществува основателна причина да се смята, че лицето, притежаващо такива материали, е извършило или извършва углавното престъпление, с което са свързани материалите", Глава 42, Кодекс на САЩ., параграф 2000aa(a)(1), параграф 2000aa(b)(1). Този текст показва, че Конгресът е смятал, че защитени по ЗЗП материали непременно ще бъдат свързани с углавно престъпление, когато следователите се насочват към тези материали като улика. Обаче когато служителите по съвместителство изземат защитени по ЗЗП материали, тъй като те са смесени в компютъра с други материали, които с право са мишена на правоприлагащите органи, защитените по ЗЗП материали могат изобщо да не са свързани с някакво престъпление. Например защитени по ЗЗП материали могат да бъде градинарски вестник, който случайно се намира на същия твърд диск заедно с детска порнография или документи за измамна схема.

Шестият федерален апелативен съд се произнася категорично, че случайното изземване на защитени по ЗЗП материали, смесени в компютъра на заподозрения с улики за престъпление, не възбужда отговорност по ЗЗП. Процесът *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001) е свързан с две дела срещу офиса на шерифа на окръг Хамилтън, щата Охайо. Делата са заведени след изземването на два сървъра, използвани да поддържат пощенски кутии, заподозрени, че съдържат улики и контрабанда, свързана с разврат, телефонно подслушване, детска порнография, кражба на кредитни карти и софтуерно пиратство. Шестият апелативен съд отбелязва, че „когато полицията извършва претърсване със съдебна заповед на компютър за документи, често пъти е трудно или дори невъзможно (особено при липса на сътрудничество от страна на собственика) да се отделят углавните материали от други „безобидни" материали в компютъра" на мястото на обиска. Поради тези прагматични съображения Съдът отхвърля вменяването на отговорност по ЗЗП при случайни изземвания; в противен случай ЗЗП „в много случаи ще пречи на полицията да изземе улики, намиращи се в компютъра". Вместо това Съдът излиза със становище, че „когато защитени материали са смесени в компютъра на заподозрения с

криминална улика, която не е защитена от закона, ние няма да повдигнем отговорност по ЗЗП за изземването на защитени от ЗЗП материали". Въпреки това обаче Съдът предупреждава, че независимо от това, че случайното изземване на свързан със ЗЗП работен продукт или документни материали не нарушава Закона, то последващото претърсване на такъв материал вероятно ще бъде забранено.

Решението на Шестия федерален апелативен съд по делото *Guest* потвърждава, че изключението за заподозрения действа според замисъла на законодателите: да ограничи обхвата на защитата по ЗЗП до „журналисти и някои други лица, които не са заподозрени в извършване на престъпление". В този дух има редица съдебни решения, които интерпретират по-широко фразата „с което са свързани материалите" в изключението за заподозрения, когато възникне случай на непреднамерено изземване на смесени материали. Виж *United States v. Hunter*, 13 F. Supp. 2d 574, 582 (D. Vt. 1998) (заключава, че материалите за седмичен правен вестник, публикуван от обвиняемия от неговата правна кантора, „са свързани" с предполагаемото му участие в трафика с наркотици на негов клиент, когато първият е бил непреднамерено иззет при търсенето на улики за последния. Виж също *S.H.A.R.K*. v. *Metro Parks Serving Summit County*, 499 F.3d 553, 567 (6th Cir. 2007) (изземване на видеокамери, поставени от незаконно проникнали лица, не е в нарушение на ЗЗП, тъй като камерите са свързани с престъплението незаконно проникване); *Carpa v. Smith*, 2000 WL 189678, at *1 (9th Cir. Feb. 15, 2000) („Законът за защита на поверителността ... е неприложим към заподозрени в престъпление.").

Становището на Шестия федерален апелативен съд в *Guest* не се занимава с проблема за смесените материали, когато собственикът на иззетия компютър не е заподозрян. В единственото досега публикувано решение по този въпрос окръжен съд подвежда щатските Сикрет Сървис под отговорност за непреднамерено изземване на защитени по ЗЗП материали. Виж *Steve Jackson Games, Inc. v. Secret Service*, 816 F. Supp. 432 (W.D. Tex. 1993). „Стийв Джаксън Геймс" ООД (СДГ) първоначално публикува ролеви игри, но също така оперирал мрежа от тринадесет компютъра, с които предоставя на клиентите си електронна поща, информация за продуктите на СДГ и предстоящи публикации. Тъй като смятали, че системният администратор на компютрите на СДГ е съхранил в тях улика за престъпление, Сикрет Сървис получили съдебна заповед и иззели два от тринадесетте компютъра, свързани в мрежата, както и други материали. Сикрет Сървис разбрали, че изземените компютри съдържат издателски материали, едва след претърсването. Въпреки това обаче Сикрет Сървис върнали компютрите месеци по-късно, като в нито един момент не смятали, че самото СДГ е замесено в разследваното престъпление.

Окръжният съд по делото *Steve Jackson Games* решава, че Сикрет Сервис нарушават ЗЗП; за жалост е трудно да се очертаят основанията на съда. Например в становището не се посочва точно кои от материалите, иззети от Сикрет Сървис, са защитени от ЗЗП; вместо това съдът се задоволява

да изброи изземата собственост и да заключи, че някои защитени от ЗЗП материали „били получени" по време на обиска. По подобен начин съдът отбелязва, че обискът на СДГ и първоначалното изземване на собственост не нарушава ЗЗП, обаче продължителното задържане на собствеността след установяване на издателския статут на СДГ е истинският източник на нарушение на ЗЗП – нещо, с което самият закон, изглежда, не се занимава. Съдът също така намеква, че решението би могло да бъде различно, ако Сикрет Сървис са направили „копия от цялата иззета информация" и са върнали хардуера във възможно най-кратък срок, но не отговаря дали в такъв случай резултатът е щял да бъде различен.

Случайното изземване на защитени по ЗЗП материали от компютър на незаподозряно лице продължава да бъде несигурна материя в правото, отчасти защото дела, свързани със ЗЗП, рядко се оспорват. На практика служителите могат да избегнат изземването на защитени по ЗЗП материали от компютър на незаподозряно лице, като използват призовка или действат съобразно Закона за съхранената комуникация (ЗСК), за да изискат от него да предостави търсената информация. До днес никой друг съд не е възприел същия подход към ЗЗП, както съдът по делото *Steve Jackson Games.* Виж *State v. One (1) Pioneer CD-ROM Changer, 891 P.2d 600, 607 (Okla. App. 1994)* (където се оспорва аргументът в *Steve Jackson Games*, че изземването на компютърно устройство може да наруши ЗЗП само защото съоръжението „също така съдържа или е използвано за разпространяване на потенциални „документни материали"). Нещо повече, дори съдилищата в последна сметка да откажат да ограничат ЗЗП до случаите, в които правоприлагащите органи преднамерено изземат от незаподозряно лице материал по Първата поправка, който е обикновено доказателство за престъпление, съдът може да заключи, че други изключения в ЗЗП като „контрабанда или плодове на престъпление" може да се тълкуват също толкова широко, както съдът по делото *Guest* тълкува изключението за заподозрения.

Малкото федерални съдилища, които са решавали дела, заведени по ЗЗП, са отхвърляли претенциите на ищците без достатъчен съдържателен анализ. Виж *Davis v. Gracey*, *111 F.3d 1472, 1482 (10th Cir. 1997)* (прекратява поради липса на компетентност дело по ЗЗП, неправомерно заведено срещу общински чиновници в тяхното лично качество); *Berglund v. City of Maplewood,* 173 F. Supp. 2d 935, 949-50 (D. Minn. 2001) (становище, че изземването от страна на полицията на видеокасета на обвиняемия попада под изключенията „заподозрян в престъпление" и „унищожаване на улики" в ЗЗП, тъй като касетата е можело да съдържа доказателство за неправомерното поведение на заподозрения); *DePugh v. Sutton,* 917 F. Supp. 690, 696-97 (W.D. Mo. 1996) (отхвърля позоваването на ЗЗП за изземване на материали с детска порнография, тъй като има основателна причина да се смята, че лицето, притежаващо материалите, е извършило углавното престъпление, за което се отнасят материалите); *Powell v. Tordoff,* 911 F. Supp. 1184, 1189-90 (N.D. Iowa 1995) (отхвърля иск по ЗЗП с аргумента, че

ищецът няма компетентност да оспорва обиск и изземване по Четвъртата поправка). Виж също *Lambert v. Polk County*, 723 F. Supp. 128, 132 (S.D. Iowa 1989) (отхвърля иск, заведен по ЗЗП, след като полицията изземва видеокасета, тъй като полицаите не са можели основателно да предполагат, че собственикът на касетата е имал за цел да направи материала обществено достояние).

Юридически привилегировани документи

Служителите трябва да бъдат особено внимателни, когато планират претърсване на компютър, което може да доведе до изземване на юридически привилегировани документи като медицински епикризи и кореспонденция между клиент и адвокат. Два въпроса трябва да бъдат взети под внимание. Първо, служителите трябва да са сигурни, че обискът няма да наруши наредбите на главния прокурор, свързани с получаване на поверителна информация от незаинтересовани трети страни. Второ, служителите трябва да разработят стратегия за преглед на изземите в резултат на претърсването компютърни файлове, така че да не допуснат нарушаване на каквато и да е привилегия.

а) наредби на главния прокурор, свързани с обиск на незаинтересовани трети страни юристи, лекари и духовници

Служителите трябва да бъдат особено внимателни, ако възнамеряват да претърсят офиса на лекар, адвокат или член на духовенството, срещу които не е повдигнато обвинение за участие в разследваното престъпление. По поръчение на Конгреса главният прокурор издаде указания за федералните служители, които искат да получат документни материали от такива незаинтересовани трети страни. Виж Глава 42, Кодекс на САЩ, параграф 2000аа-11(а); 28 C.F.R., параграф 59.4(b). Според тези правила федералните служители на правоприлагащите органи не трябва да използват съдебна заповед за обиск с цел да получат документни материали, за които се смята, че са частно притежание на незаинтересована трета страна лекар, юрист или духовник в случай, когато търсеният материал или онзи, който вероятно ще бъде прегледан при изпълнение на съдебната заповед, съдържа поверителна информация за пациенти, клиенти или енориаши. Правилото допуска изключение само в някои случаи. Съдебна заповед може да бъде използвана, ако прилагането на не толкова крайни мерки би застрашило достъпността или полезността на търсените материали; достъпът до документните материали е от изключителна важност за разследването; и изпълнението на съдебната заповед е препоръчано от прокурора и е одобрено от съответния заместник-помощник главен прокурор.

б) стратегии за преглеждане на привилегировани компютърни файлове

Служители, които възнамеряват да извършат обиск, който може да доведе до изземване на юридически привилегировани документи, трябва да разработят стратегия за изключване на привилегированите файлове и трябва да опишат тази стратегия в клетвената декларация.

Когато служителите изземат компютър, който съдържа юридически привилегировани файлове, доверена трета страна трябва да прегледа компютъра и да определи кои файлове съдържат привилегировани материали. След като прегледа материалите, третата страна ще предостави онези материали, които не са привилегировани, на екипа разследващи. Предпочитаните практики за определяне кой да прегледа файловете са различни в различните съдилища. Най-общо казано обаче, има три възможности. Първо, самият съд може да прегледа материалите на закрито заседание *in camera*. Второ, председателстващият съдия може да вмени на неутрална трета страна, известна като „специален майстор", задачата да прегледа файловете. Трето, екип от прокурори или служители, които не работят по делото, могат да образуват „филтърен екип", за да подпомогнат извършването на обиска и последващия преглед на файловете. „Филтърният екип" издига така наречената „етична стена" между уликата и прокурорския екип, като допуска само непривилегировани файлове да прескочат стената.

Тъй като в един-единствен компютър могат да се съхраняват милиони файлове, съдиите в изключително редки случаи предприемат *in camera* прегледи. Вместо това обичайно се избира между филтърен екип и специален майстор. Повечето прокурори предпочитат да използват филтърен екип, ако съдът разреши. Филтърният екип обикновено може да прегледа изземите компютърни файлове в сравнително кратък срок, докато на специалните майстори прегледът понякога отнема няколко години. От друга страна, някои съдилища изразяват притеснения по отношение на филтърните екипи. Виж *Grand Jury Subpoenas*, 454 F.3d 511, 522-23 (6th Cir. 2006) (одобрява използването на филтърни екипи във връзка със съдебни заповеди, но ги отхвърля във връзка с призовки на голямото жури); *United States v. Neill*, 952 F. Supp. 834, 841 (D.D.C. 1997); *United States v. Hunter*, 13 F. Supp. 2d 574, 583 n.2 (D. Vt. 1998) (преглед, осъществен от магистрат или специален майстор, „може да е за предпочитане" пред използването на филтърен екип.

Въпреки че не съществува единствен стандарт, съдийската практика показва, че обикновено улика, получена от филтърен екип, е приемлива само ако правителството покаже, че процедурите надлежно са защитавали правата на обвиняемия и няма нанесена щета. Един подход за ограничаване на количеството на потенциално привилегировани документи е защитникът да прегледа направеното от филтърния екип, за да определи онези документи, за които защитата ще пледира за привилегия. Така

идентифицираните файлове, които нямат отношение към разследването, няма нужда да бъдат оспорвани. Въпреки че такъв подход може би не е подходящ във всички случаи, магистратите могат да оценят факта, че на защитата е предоставена възможност да идентифицира потенциални искове, преди материалът да бъде предоставен на прокурорския състав.

При необичайни обстоятелства съдът може да заключи, че филтърният екип няма да бъде адекватен, и да назначи специален майстор да прегледа материалите. Виж *United States v. Abbell*, 914 F. Supp. 519 (S.D. Fla. 1995); *DeMassa v. Nunez*, 747 F.2d 1283 (9th Cir. 1984). Във всеки случай овластеният проверяващ положително ще се нуждае от неутрален технически експерт, който да помага в сортирането, идентифицирането и анализирането на дигиталната улика за процеса на прегледа.

Други незаинтересовани трети страни

Освен конкретните ограничения за използването на съдебна заповед за обиск за получаване на информация от незаинтересовани издатели, юристи, лекари и духовници, политиката на Департамента по правосъдие подкрепя използването на призовка или други не толкова натрапчиви средства, за да се сдобие с улика от незаинтересовани трети страни, освен когато използването на тези не толкова натрапчиви средства чувствително заплашва достъпността или полезността на търсените материали. Освен в спешни случаи, заявката за такава съдебна заповед трябва да бъде разрешена от представител на правителството. Важно е да се отбележи обаче, че несъобразяването с тази политика „може да не бъде оспорвано и съдът може да не повдигне този въпрос като основание за премахване или изключване на улика“. 28 C.F.R., параграф 59.5(b).

Доставчици на комуникационни услуги

Когато се предполага, че обискът може да доведе до случайно изземване на мрежови акаунти, принадлежащи на невинни трети страни, служителите трябва да предприемат всичко необходимо, за да защитят непокътнатостта на акаунтите на третите страни.

Една категория незаинтересована трета страна, често срещана в компютърен контекст, са доставчиците на интернет услуги. Законът за съхраненитe комуникации (ЗСК) регулира достъпа на правоприлагащите органи до съдържанието на електронни комуникации, съхранявани от трети страни – доставчици на услуги. В повечето случаи правоприлагащите органи трябва да използват клаузите за задължителен процес в параграф 2703, за да убедят доставчик на услуги да разкрие информация; когато е възможно, правоприлагащите органи трябва да избягват физическото изпълнение на съдебна заповед за обиск по член 41 върху доставчик на интернет услуги. Когато служителите на правоприлагащите органи изпълняват заповед за обиск по член 41 по отношение на доставчик на

интернет услуги и изземат акаунти на клиенти и абонати, тези клиенти и абонати могат да заведат граждански дела с аргумента, че обискът е в нарушение на ЗСК. Освен това ЗСК има наказателна клауза, която забранява неупълномощения достъп до електронни или жични комуникации на „електронно съхранение". Виж Глава 8, Кодекс на САЩ, параграф 2701.

Текстът на ЗСК като че не вменява гражданска отговорност за претърсвания и изземвания, извършени съобразно валидни съдебни заповеди за обиск по Правило 41: ЗСК изрично разрешава достъпа на правителството до съхранени комуникации при наличието на съдебна заповед, издадена според Федералните правила за наказателна процедура, виж Глава 18, Кодекс на САЩ, параграф 2703(a), (b), (c)(1)(A); *Davis v. Gracey,* 111 F.3d 1472, 1483 (10th Cir. 1997), а наказателната забрана на параграф 2701 е неприложима, когато достъпът е разрешен по параграф 2703. Въпреки това *Steve Jackson Games, Inc. v. Secret Service,* 816 F. Supp. 432 (W.D. Tex. 1993) повдига опасението, че обискът, извършен съобразно валидна съдебна заповед, би могъл да наруши ЗСК. Окръжният съд в *Steve Jackson Games* подвежда Сикрет Сървис под отговорност, след като служителите изземват, преглеждат и (в някои случаи) унищожават съхранени електронни комуникации, иззети въз основа на валидна съдебна заповед за обиск. Становището на съда, изглежда, се корени в погрешното схващане, че ЗСК изисква също така заповедите за обиск да бъдат съобразени и с Глава 18, Кодекс на САЩ, параграф 2703(d), както и с различните бележки в параграф 2703. Всъщност ЗСК ясно посочва, че параграф 2703(d) и бележките в параграф 2703 се прилагат само когато правоприлагащите органи не са издействали съдебна заповед.[1] Нещо повече, добронамереното позоваване на съдебна заповед, съдебно разпореждане или законно разрешение представлява безспорна защита срещу нарушение на ЗСК.

Най-добрият баланс между резултата в *Steve Jackson Games* и категоричността на ЗСК може да се постигне, когато служителите, които осъществяват претърсвания на интернет доставчици и други трети страни, съхраняващи жични или електронни комуникации, действат крайно предпазливо. При всяко претърсване на компютър служителите трябва да се опитват да избягват неупълномощени вмешателства в личното пространство и в това отношение претърсванията на доставчици на услуги не са по-различни. Виж *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) („отговорните длъжностни лица, включително съдебните длъжностни лица, трябва да гарантират, че обиските се провеждат по начин, който свежда до минимум неупълномощени вмешателства в личното

1 Това посочва фундаменталната разлика, пренебрегната в Steve Jackson Games: разликата между съдебна заповед за обиск, издадена по Правило 41, осъществена чрез физическо претърсване и съдебна заповед за обиск, издадена по ЗСК, която правоприлагащите органи извършват, като задължават доставчик на електронна комуникационна услуга или отдалечен компютърен сервиз да разкрият съдържанието на мрежовия акаунт на абоната. Въпреки че и двете са заповеди за обиск, на практика те са различни. Разликата е особено важна, когато съдът реши, че е нарушен ЗСК, и трябва да определи мярката, тъй като законът не дава право за конфискация за неконституционни нарушения на ЗСК.

пространство“). В повечето случаи следователите се опитват да избегнат масирано претърсване и изземване на компютрите на доставчика, като вместо това разчитат на задължителния процес, съответстващ на ЗСК. Когато следователите нямат друг избор, освен да осъществят обиска, както когато доставчикът няма способност или воля да се подчини на задължителния процес или е заподозрян в участие в престъпно деяние, самите служители трябва да претърсят компютрите на доставчика. Тъй като всеки компютър на доставчика може да съдържа записи, свързани с потребители, които са напълно непричастни към наказателното разследване, може би би било уместно да се разработят специални процедури, за да се защитят интересите за неприкосновеност на личното пространство на тези потребители. Например служителите могат да информират магистрата в клетвената декларация към съдебната заповед за обиск, че те ще предприемат мерки да осигурят поверителността на акаунтите, и да не ги подлагат на човешка проверка. Запазване на непокътнатостта на акаунтите на невинни лица при липсата на основания да се смята, че в акаунтите на тези лица може да се съхранява улика за престъпление, би трябвало да задоволи опасенията, изразени в *Steve Jackson Games.* В този порядък може да се направи сравнение между *Steve Jackson Games, 816 F. Supp. At 441* (където се възбужда отговорност по ЗСК, когато служителите четат лична кореспонденция на потребители, които са свързани с престъплението, „и по такъв начин са изтрили или унищожили кореспонденция, било то умишлено или случайно“) с *Gracey*, *111 F.3d at 1483* (отказва да вмени отговорност по ЗСК при обиск, при който „ищците не твърдят, че служителите са се опитали да получат достъп и да прочетат изпетите имейли, а служителите отричат да са имали какъвто и да е интерес да постъпят така“).

ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

ДП - Департамента по правосъдие
Department of Justice (DOJ)

ЗЗП – Закон за защита на поверителността
PPA – Privacy Protection Act

ЗНЧР – Закон за наблюдение на чуждо разузнаване
FISA – Foreign Intelligence Surveillance Act

ИМВ – Имиграционни и митнически власти
ICE – Immigration and Customs Enforcement

КСБТ – Консултативен съвет за борба срещу тероризма
ATAC – Anti-Terrorism Advisory Council

КСНС – Киберспециалисти по национална сигурност
NSCS – National Security Cyber Specialists

МГЗ – Митническа и гранична защита
CBP – Customs and Border Protection

ОНС – Отдел за национална сигурност на ДП
National Security Division (NSD)

ПРПП – подслушване, регистрация, прихващане и проследяване
PRTT – Pen Register and Trap and Trace

СБТ – Сектор за борба срещу тероризма
Counterterrorism Section (CTS)

СВПП – Споразумение за взаимна правна помощ
MLAT – Mutual Legal Assistance Treaty

СК – Сектор за контраразузнаване
CES – Counterespionage Section

СМС – Служба за международно сътрудничество
OIA – Office of International Affairs

СНЧР – Съд за наблюдение на чуждо разузнаване
FISA – Foreign Intelligence Surveillance Court

ФБР – Федерално бюро за разследване
FBI – Federal Bureau Investigation

ISBN 9789542914464