ИЗПОЛЗВАНЕ И КОНТРОЛ НА ТРАФИЧНИТЕ ДАННИ ЗА РАЗКРИВАНЕ НА ПРЕСТЪПЛЕНИЯ В ШВЕЙЦАРИЯ

ПРОФ. Д-Р ИЛИН САВОВ
ФАКУЛТЕТ „ПОЛИЦИЯ“, АКАДЕМИЯ НА МИНИСТЕРСТВО НА ВЪТРЕШНИТЕ РАБОТИ

Илин САВОВ *е служител в службите за сигурност в Република България от 2000 г. Защитил е дисертационен труд в Академията на МВР на тема „Взаимодействие и координация между СДОТО и оперативните служби на МВР и ДАНС при прилагане на специални разузнавателни средства”. През 2017 г. придобива академична длъжност „професор” по „Национална сигурност”. Експерт е по проблемите на националната сигурност, оперативно-издирвателните и оперативно-техническите дейности за защита на националната сигурност от посегателства и престъпни прояви. Автор е на студии, научни доклади, статии и учебни пособия свързани с управлението и функционирането на службите за сигурност, трафика на хора, миграционните процеси, използването и контрола на специалните разузнавателни средства и трафични данни в Република България, Европейския съюз и САЩ. Автор е на монографиите „Специални разузнавателни средства” и „Реадмисия и миграционният контрол на чужденци в Република България”, „Организация и управление на прилагането на специалните разузнавателни средства“, „Специфични негласни методи с оперативно-технически профил“. Понастоящем е „професор“ към факултет „Полиция” на Академията на МВР и към факултет „Национална сигурност и отбрана“ на Военна Академия „Г. С. Раковски“.*

Резюме: *В статията се разглежда правната рамка и основните принципи при използването на трафични данни за разкриване на престъпления в Швейцарската конфедерация. Извършен е преглед и оценка върху процедурите относно контрола върху трафичните данни и организацията по реализация на мониторинга. Откроени са органите имащи право да искат прихващането на трафични данни и са изведени някои от предимствата в Швейцарското законодателство във връзка с противодействието на престъпни посегателства.*

Ключови думи: *трафични данни, информация, прокуратура, престъпност, Швейцария, наблюдение, пощенския и телекомуникационен трафик, сигурност*

USE AND CONTROL OF DATA RETENTION FOR CRIME DETECTION IN SWITZERLAND

PROF. DR. ILIN SAVOV
FACULTY „POLICE”, ACADEMY OF THE MINISTRY OF THE INTERIOR

Abstract: *The article discusses the legal framework and basic principles in the use of traffic data for crime detection in the Swiss Confederation. A review and evaluation of the procedures regarding the control over the traffic data and the organization for the implementation of the monitoring was performed. The authorities entitled to request the interception of traffic data have been identified and some of the advantages of Swiss law in combating criminal encroachment have been highlighted.*

Keywords: *data retention, information, prosecution, crime, Switzerland, surveillance, postal and telecommunications data, security*

ВЪВЕДЕНИЕ

С навлизането на съвременните информационни и комуникационни технологии обществата постоянно завишават своите претенции към специализираните държавни структури за адекватна реакция спрямо престъпността и овладяване на негативните причини за появата и вирееното на престъпни поведенчески прояви.

Предполага се, че с разработката и внедряването на системите 5G и 6G ще нарасне значимостта на скоростта и бързината на информационен обмен и трансфери на данни. Това не може да убегне в престъпното мислене, мотивираност и вероятно ще се достигне до прилагане на различните конфигурации на информацията от престъпници и организирани престъпни групи за постигане на техните цели и противозаконни стремления.

Опазването на живота, здравето, основните свободи и неприкосновеност на всеки обществен субект се намира в съдържанието на основните функции и дейности, предоставени законово от държавната власт на специализираните правозащитни държавни органи.

В настоящата статия ще насочим вниманието към един важен обществен процес в Швейцарската конфедерация, а именно използването и контролът на трафичните данни във връзка с противодействието на престъпността.

Правен механизъм на контрола на трафичните данни в Швейцария

Както е известно Швейцарска конфедерация е сравнително малка вътрешноконтинентална конфедерация от двадесет и шест кантона в Централна Европа. Площта ѝ е 41 749 km², населението на страната е около 8 милиона души, като се състои от три основни етнолингвистични групи – немска, френска и италианска – и малък процент ретороманско[1] говорещо население. Имигрантите наброяват около 2 милиона. В този смисъл швейцарците нямат единна национална идентичност, а са група от народи, споделящи обща история и ценности като федерализъм, неутралитет и пряка демокрация. Тези особености на Швейцария определят и някои особености в националното законодателство на конфедерацията[2].

Припомням, че в България използването на специалните разузнавателни средства и контрола на трафичните данни са регламентирани в два различни нормативни акта - Закона за СРС и Закона за електронните съобщения. В Швейцария не се прави съществена разлика между тях и основните изисквания, за да се допусни тяхното прилагане, са посочени в Дял 5 „Принудителни мерки“, Глава 8 „Мерки за тайно наблюдение“[3] на НПК[4], и по-специално, в раздел 1 „Наблюдение на пощенския и телекомуникационен трафик“ (Überwachung des Post- und Fernmeldeverkehrs) и Федералния закон за наблюдение на пощите и далекосъобщенията[5].

Съгласно чл. 1 (1) от Федералния закон за наблюдение на пощите и далекосъобщенията се допуска прилагане на мониторинг на пощите и телекомуникациите, когато се извършва:

А) в наказателното производство на Федерацията или на кантон;

Б) за принудително изпълнение на съдебни поръчки по Закона за взаимопомощ на 20 март 1981 г.;

В) като част от търсенето и спасяването на изчезнали лица.

Г) като част от издирването на хора, които са осъдени на лишаване от свобода или срещу които е наложена мярка за неотклонение.;

Д) като част от прилагането на Закона за разузнавателната служба от 25 септември 2015 г.2 (NDG).

Освен това наблюдението може да се използва за информация относно платежните транзакции, която е предмет на Закона за пощенските услуги от 17 декември 2010 г. (PG), като се прилагат разпоредбите относно задължението за предоставяне на доказателства и задължението за предоставяне на информация на орган.

Осигуряването на тези възможности се отнася задължително за всички държавни или частни доставчици на пощенски и телекомуникационни услуги, както и интернет доставчици. Операторите на вътрешни далекосъобщителни мрежи и вътрешни центрове също трябва да се подчинят на тази законова разпоредба.

Интересна е организацията по реализация на този мониторинг и тя се доближава твърде много до практиката в България. Федерацията е създала и поддържа служба за мониторинг на пощите и далекосъобщенията[6] (от тук нататък наричана Службата), която действа в съответствие с член 269 от Наказателно-процесуалния кодекс (StPO).

Тя изпълнява своите функции самостоятелно, работата й се ръководи от инструкции и е подчинена на Федералния департамент по правосъдие и полиция само административно. Службата работи в рамките на своите задължения с лицензионните и надзорни органи в областта на пощенските и телекомуникационни услуги.

Службата има едновременно изпълнителски и контролни функции и изпълнява следните по-важни задачи:

- проверява дали мониторинга е активиран от приложимо правонарушение и е разпореден от компетентния орган. При неточни или необосновани условия тя поема контакта с одобряващия орган, преди препращането на информацията на изпълнителния орган.
- нарежда на доставчика на телекомуникационни услуги да предприеме необходимите мерки за мониторинг.
- Приема от доставчиците данните за трафика на наблюдаваното лице, регистрира ги и предавана на заявяващия орган документите и материалните носители на данни.
- Гарантира изпълнението на директните включвания, те не се изпълняват от Службата.
- Получава данните от идентифицирането на абонатите данните за трафика и сметките и ги препраща на заявяващия орган.
- Поставя условия, предвидени за защита на търговска тайна, които са на разположение на одобряващия орган.
- Извършва контрол на разрешената продължителност на наблюдение и определя това при изтичане на срока, ако не е отправено искане за продължение
- Уведомява незабавно органа, дал разрешението, при прекратяване на наблюдението.
- Води статистика за извършваните наблюдения.
- Следи техническото развитие на телекомуникациите.
- Съветва органи и доставчиците на телекомуникационни услуги по технически въпроси, свързани с мониторинга на комуникациите.

Федералния департамент по правосъдие и полиция (FDJP) може да създаде консултативен орган, който включва представители на FDJP, службата, кантоните, правоприлагащите органи, Федералната разузнавателна служба (FIS) и доставчиците на пощенски и телекомуникационни услуги.

Консултативният орган служи за обмен на опит и мнения между по-горе споменатите представители. Той разглежда промените на този закон и разпоредбите за прилагане, както и промените в официалната практика, за да насърчи гладкото прилагане на мониторинга и постоянното по-нататъшно развитие в тази област. Той дава своето становище по проектите за промени и може да дава препоръки по своя инициатива.

FDJP регламентира състава и организацията на консултативния орган и процедурите, които той трябва да спазва.

Продължителността, през която данните, събрани в контекста на наказателното производство, трябва да се съхраняват в системата за обработка, се основава на правилата, които се прилагат за наказателните дела в съответствие с приложимия наказателно-процесуален закон.

Прави впечатление продължителността на съхранение в някои случаи. Данните, събрани като част от изпълнението на искане за взаимна правна помощ, трябва да се съхраняват в системата за обработка толкова дълго, колкото е необходимо за преследваната цел, но не по-дълго от 30 години след края на наблюдението. Същото важи и при случаите за издирване на изчезнало лице, както и при издирването на лице, санкционирано с мярка за лишаване от свобода.

Службата предоставя на следните органи информация за данните в съответствие с членове 21 и 22 от закона при поискване и само за следните цели (чл. 15 параграф 1§:

А). федералните и кантонални власти, които могат да разпореждат или одобряват наблюдение на далекосъобщителния трафик или органите, определени от тях: с цел определяне на услугите и лицата, които ще се наблюдават, и лицата, свързани с тях;

Б). федералната полицейска служба и полицейските власти на кантоните и комуните: с цел изпълнение на полицейски задължения;

В). компетентните федерални и кантонални органи: с цел разглеждане на административно наказателни дела;

Г). Федералната разузнавателна служба с цел изпълнение на задачи съгласно Закона за разузнавателната служба[7] (NDG).

Съгласно чл.21 параграф 1 от Федералния закон за наблюдение на пощите и далекосъобщенията доставчикът на телекомуникационни услуги предоставя на Службата следната информация:

А). Фамилия, собствено име, дата на раждане, адрес и, ако са известни, професия на участника;

Б). адресиращите елементи (чл. 3 букви f и g от Закона за далекосъобщения – Fernmeldegesetz[8])[9];

В). видовете услуги;

Г). допълнителни данни за далекосъобщителни услуги, определени от Федералния съвет; тези данни могат да имат административен или технически характер или да позволяват идентифициране на лица;

Д). за взаимоотношения с клиенти без абонаментни отношения: допълнителна точка за доставка, фамилия и име на лицето, което е доставило средствата, необходими за достъп до телекомуникационната услуга.

Законът предвижда, че доставчиците на телекомуникационни услуги трябва да съхраняват и доставят тези данни с цел идентификация в продължение на 6 месеца.

Федералният съвет (Bundesrat) регламентира начините за използване на информацията и нейното съхранение. Той може да разреши на органите, посочени по-горе, да получат достъп до съществуващите непублични директории.

Ако е извършено престъпление в Интернет, доставчика на интернет е длъжен да предостави на компетентния орган цялата информация, което дава възможност за идентифициране на извършителя. Ако има достатъчно индикации, че заплаха за вътрешна или външна сигурност се извършва или е била извършена чрез Интернет, доставчиците на телекомуникационни услуги са длъжни да предоставят на услугата цялата информация, която позволява идентифицирането на авторството или произхода.

Федералният съвет определя коя информация доставчиците на телекомуникационни услуги трябва да съхраняват и предоставят с цел идентификация по време на взаимоотношенията с клиентите и в продължение на 6 месеца след приключването им. Той регулира формата и съхранението на исканията за информация. Предоставянето на информация или мониторинг е стандартизирано. Федералният съвет предвижда, че доставчиците на телекомуникационни услуги трябва да съхраняват и доставят някои от тези данни с цел идентификация в продължение на ***6 месеца***. Доставчиците на телекомуникационни услуги трябва да предоставят на Службата допълнителна информация, с която разполагат. Федералният съвет може да задължи доставчиците на вторични комуникационни услуги, които предлагат услуги от голямо икономическо значение или за голям брой потребители, да запазят и доставят цялата или част от информацията, която те трябва да предоставят.

Федералният закон за наблюдение на пощите и далекосъобщенията регламентира също задълженията на доставчиците на телекомуникационни услуги:

- От доставчика на телекомуникационни услуги при поискване се изисква да бъдат изпратени на Службата данните за трафика на съобщенията и за идентификацията на абоната и сметките на наблюдаваното лице. Той също така трябва да предостави необходимата информация за извършването на мониторинг. Федералният съвет може да освободи доставчиците на телекомуникационни услуги от определени законови задължения само ако те предлагат услуги с малко икономическо значение или в образователния сектор.
- Когато при наблюдаваните телекомуникационни услуги са включени няколко доставчици, то Службата избира един доставчик на услугата, който е отговорен за администриране работата по заявката или може да извърши мониторинга с най-малко техническо усилие. Всички участващи доставчици са длъжни да предоставят своите данни на отговорния доставчик. Обезщетението, предвидено в член 38 на закона и за което ще стане дума след малко, се заплащат на изпълняващия доставчик. Разпределението на средствата между страните е отговорност на доставчиците.
- Доставчиците са длъжни да пазят информацията на необходимите данни за идентифициране на абоната и данните за трафика и сметките в продължение на шест месеца.
- Те осигуряват необходимите абонатни иден-

тификаторите и данни за трафика и сметките на наблюдаваното лице възможно най-бързо, когато това е възможно, в реално време.

- Доставчиците гарантират съответствие на съобщението с данните, посочени в член 21, параграф 1. Тези данни могат да се доставят на Службата по електронен път.
- Доставчиците трябва да съхраняват след получаване на искане най-малко шест месеца информация за връзките на клиентите в съответствие с член 21, а така също случаите, когато лицата не са осъществили връзка с клиент чрез мобилни телефони.
- Федералният съвет определя останалите подробности. Ако е необходимо, може да се предвиди, че предаването на съобщението се извършва безплатно и денонощно.
- Операторите на вътрешните далекосъобщителни мрежи и вътрешни центрове трябва да имат лица, отговорни за достъпа до предоставяните услуги и даване на необходимата информация.

Необходимостта от оборудване за наблюдение се поема от доставчиците на пощенски и телекомуникационни услуги. Поради това в Швейцария е решено на издаващия орган за описаната информация да се направи адекватна компенсация за разходите на всяко наблюдение. Федералният съвет регламентира компенсирането и определя таксите за направените служебни разходи от доставчиците. Поръчващият орган плаща такса, състояща се от:

а. такса за изпълнение на услугата;

б. обезщетението за услугите на задължените да сътрудничат.

При разследване на престъпления във фазата на досъдебното производство съгласно чл. 269, параграф 1 от НПК на Швейцария, прокуратурата може да наблюдава пощенския и далекосъобщителен трафик, ако:

А). съществуват сериозни подозрения, че е извършено престъпление от вида на тези, подробно изброени в параграф 2 на същия този член;

Б). сериозността на престъплението оправдава това наблюдение;

В). всички предишни действия по разследването са били неуспешни или разследването би било невъзможно или нецелесъобразно затруднено.

В алинея 2 на чл. 269, подобно на ФРГ, са подробно посочени престъпленията, при които се допуска наблюдение на пощенския и далекосъобщителен трафик, като се отчитат изискванията на Наказателния кодекс[10], Федералния закон за чужденците и интеграцията[11], Федералния закон относно приемане на Хагската конвенция за защита на децата при международно осиновяване[12], Закона за военните материали[13], Закона за ядрената енергия[14], Закона за наркотичните упойващи средства[15], Закона за опазване на околната среда[16], Закона за контрол на стоките[17], Закона за насърчаване на спорта[18], Закона за пазарната финансова инфраструктура[19], Закон за оръжията[20], Закон за терапевтичните продукти[21] и Закон за хазарта[22].

Ако оценката на престъпление, подлежащо на военна юрисдикция, се прехвърли под гражданска юрисдикция, наблюдението на пощенския и телекомуникационния трафик също може да бъде разпоредено да преследва престъпленията, изброени в чл. 70, параграф 2 от Военно-наказателното производство[23] от 23 март 1979 г.

Пощенски и телекомуникационен трафик може да бъде наблюдаван на следните лица:

А). на обвиняемият;

Б). на трета страна, ако въз основа на определени факти трябва да се приеме, че:

1. обвиняемият използва пощенския адрес или телекомуникационната услуга на третото лице, или
2. третата страна получава съобщения, специфични за обвиняемия, или препраща съобщения от него на друго лице.

При наблюдение на лице, принадлежащо към професионална група, посочена в членове 170–173[24], информацията, която не е свързана с предмета на разследването и причината, поради която това лице се наблюдава, трябва да бъде премахната под ръководството на съд . Органите на реда не трябва да получават познания за професионални тайни. Отделените данни трябва да бъдат унищожени незабавно; те не трябва да бъдат оценявани.

Наблюдението на пощенския и телекомуникационния трафик изисква задължително одобрение от съда. По изключение, ако лицето използва няколко телекомуникационни терминала, по които осъществява трафик, съда може да издаде общо разрешение, без това да е необходимо за

всеки отделен случай, т.е. дава се общ лиценз (Rahmenbewilligung). Прокуратурата трябва да предоставя ежемесечно информация и при завършване на наблюдението доклад за одобрение на приложените мерки. Ако се изисква прилагане на мерки, непредвидени в общото разрешение или защитени съобразно режима за търговска тайна, то се изисква отново одобрението на съда.

Прокурорът може да поиска данни за трафика, сметките или за идентифициране на потребителя когато е налице сериозно подозрение за извършено престъпление по чл.179 от НК и когато са изпълнени условията на член 269, параграф 1, букви B и C, и по-специално за:

А) кога и с кои лица или връзки наблюдаваното лице от пощенския и телекомуникационния трафик има или е имало свързвания;

Б) данните за трафика или сметките.

Режимът изисква задължителното одобрение на тези мерки от съда. Независимо от продължителността на наблюдението, информацията за данните от трафика не може да бъде за време, по-голямо от шест месеца назад от датата на поискването.

Тъй като изискванията на чл. 269 бяха вече изяснени, ще се спрем накратко на чл. 179 от НК на Швейцария. Става дума за следните престъпни деяния:

- Отваряне без разрешение на затворено писмено или предадено съобщение с цел запознаване със съдържанието му, независимо, че адресата е друг, и съхраняване, предаване или използване на тази информация. Наказанието за това деяние е глоба;
- Слушане на чужд непубличен разговор без съгласието на всички участващи чрез подслушвателно устройство или звукозапис. Използване на тази информация, включително и чрез предаването ѝ на трети лица. Притежаване на запис, за който лицето знае, че е получен чрез престъпно деяние, съхранение и предаване на този записа на трети страни. Наказанието за тези деяния е лишаване от свобода до три години или глоба;
- Правене на звукозапис от събеседник в непубличен разговор без знанието и съгласието на участващите в разговора. Притежаване или съхранение на звукозапис, за което лицето знае, че е получен в нарушение на първото условие, прави оценка в интерес на трета страна или предава съдържанието за получаване на информация. Предвиденото наказание е лишаване от свобода до една година или глоба;
- Наблюдение без разрешение и правене на запис на материален носител на резултатите от това наблюдение на секретни райони или на публично недостъпни факти в личната област. Познание за неправомерни действия на други лица в тази област. Притежаване на запис, получен чрез неправомерно деяние, съхранение и предаване на трети лица. Предвиденото наказание е лишаване от свобода до три години или глоба.

В Швейцария никой не може да бъде обвинен в извършване на престъпление, ако той като събеседник или участник в краен телекомуникационен разговор в срок от една седмица подпомогне или съдейства на службите за сигурност или съобщи за подобна информация, получена при сключване на търговски сделки, подписване на договори, за които има съмнения, че се базират на информация, получена чрез по-горе описаните престъпни деяния. Допълнително условие, обаче, е лицето да не е криминално проявено.

Данните за трафика могат да бъдат поискани още при:

- Маркетинг и спекулативна препродажба на подслушване, аудио и видеозапис, например, когато някой произвежда, внася, изнася, придобива, съхранява, притежава, допълнително създава чрез други трансфери, продава, дава под наем или рекламира технически устройства за прихващане и нерегламентирано правене на звуко- и видеозапис и когато тези устройства са в употреба наказанието е лишаване от свобода до три години или глоба. Ако нарушителят действа в интерес на трето лице, при условията на трета страна, знае за извършваното престъпление и то е предотвратено без негови постъпки, то той получава наказание като основен извършител. Ако третото лице е юридическо лице, общо или командитно дружество или едноличен търговец, параграф 1, определящ наказанията, се прилага по отношение на тези лица, които са съдействали за това или е трябвало да съдействат.

- Неправилно използване на телекомуникационно оборудване, например, умишлено или поради небрежност допусне неправомерно използване на телекомуникационните инсталации за СОТ;
- Събиране на информация за защитени лични данни или лични профили, които не са общодостъпни, като при поискване наказанието е до три години лишаване от свобода или парична глоба.

Прави впечатление, че право за получаване на информация за трафичните данни разследващите органи имат при престъпни деяния, наказанията за които са значително по-малки, отколкото в нашата страна. За някои от тях те дори са символични, например, при неправилното използване на телекомуникационно оборудване наказанието може да бъде само глоба или порицание (в оригинала Buße – покаяние).

Прокуратурата трябва в срок от 24 часа след организиране на наблюдението или поява на необходимостта от информация за данни за трафика да подаде в наказателната колегия на съда (Zwangsmassnahmengericht)| следните документи: описание на извършените до момента действия, мотивите и необходимите за одобрение процесуални документи. Съдът се произнася в рамките на пет дни от организирането на наблюдението или искането за информация и може да даде разрешение временно или под условие, да поиска допълване на информацията или извършването на допълнителни следствени действия. При необходимост съдът може да отговори незабавно на прокурора и на службата за наблюдение на пощенските и телекомуникационните услуги в съответствие с член 2 от Федералния закон от 6 октомври 2000 г. за наблюдение на пощите и телекомуникациите. В разрешението се посочва изрично дали:

- Трябва да се предвиди възможност за защита на търговската тайна;
- Е допустимо директното свързване;

Съдът издала своето разрешение за не повече от ***3 месеца***. Разрешението може да бъде един или повече пъти удължено, но всеки път с не повече от 3 месеца. Ако е необходимо удължаване, прокуратурата преди края на разрешения период трябва да изпрати мотивирано искане за подновяване.

Прокуратурата трябва да прекрати наблюдението поради следните причини:

- Първоначалните условия вече не се изпълняват; или
- Разрешението или продължаването на срока се откаже.

Прокурорът уведомява съда за причините, предизвикали приключване на наблюдението.

Ако при наблюдение на други престъпления се получат доказателства, касаещи обвиняемото лице, прокуратурата може да ги използва, ако е възможно тяхното отнасяне към разследваното престъпление.

Извън наказателното производство наблюдението на телекомуникациите трябва да бъде ограничено само до абонатната идентификация и пренос на данни, като целта е да се намери изчезнало лице. Тези данни могат да бъдат консултирани (прегледани) от неучастваща трета страна.

Получаването на информация за едно лице в този случай е възможно при следните условия:

- Полицията е установила, че местоположението на лицето е неизвестно; и
- Налице са спешни индикации за сериозни заплахи относно неговото здраве или живота му.

Трябва да се изтъкне, че членове 274-279 от Наказателно процесуалния кодекс, част от които вече бяха разгледани, се прилагат съответно и за тази процедура. Става дума преди всичко за начина по получаване на разрешение, условията за прекратяване на наблюдението, използване на резултатите и т.н. Кантоните определят издаващия орган, органът по одобряването и възивния орган. Режимът трябва да бъдат одобрени от съдебен орган.

ЗАКЛЮЧЕНИЕ

В заключение трябва да се посочи как един относително малък нормативен акт може да регулира такава чувствителна тема, каквато е надзора на пощенския и телекомуникационен трафик. Федералният закон за наблюдението на пощите и далекосъобщенията се състои само от 47 члена, включително заключителните и преходни разпоредби, но успява да обхване най-важните въпроси от обхвата и организация на мониторинга, основните задачи, които изпълнява службата по

наблюдение на пощенския трафик и далекосъобщенията, вида на информацията и компетентните органи, които имат право да искат и получават тази информация, задълженията на доставчиците, както и въпросите, които трябва да бъдат решавани от федералните и кантонални власти.

Независимо от факта, че Швейцария не е член на ЕС, но законодателството на страната спазва европейските принципи за защита правата на човека и основните свободи.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. *Закон за електронните съобщения - Обн. ДВ. бр.41 от 22 Май 2007г.,....доп. ДВ. бр.28 от 24 Март 2020г., изм. ДВ. бр.44 от 13 Май 2020г., изм. и доп. ДВ. бр.51 от 5 Юни 2020г., доп. ДВ. бр.62 от 14 Юли 2020г., изм. ДВ. бр.69 от 4 Август 2020г.*
2. *Bundesgesetz vom 22. Juni 2001 zum Haager Adoptionsübereinkommen und über Massnahmen zum Schutz des Kindes bei internationalen Adoptionen: Artikel 24;*
3. *Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 18. März 2016 (Stand am 1. März 2018)*
4. *Fernmeldegesetz (FMG) vom 30. April 1997 (Stand am 1. März 2018)*
5. *Kernenergiegesetz vom 21. März 2003: Artikel 88 Absätze 1 und 2, 89 Absätze 1 und 2 und 90 Absatz 1;*
6. *Militärstrafprozess (MStP) vom 23. März 1979 (Stand am 1. Februar 2020)*
7. *Umweltschutzgesetz vom 7. Oktober 1983: Artikel 60 Absatz 1 Buchstaben g–i sowie m und o;*
8. *Schweizerische Strafprozessordnung (Strafprozessordnung, StPO) vom 5. Oktober 2007 (Stand am1. Februar 2020)*

1 Говори се само от 35 000 души и според някои лингвисти в основата му лежи древния простонароден латински език. Става един от четирите национални езика в Швейцария през 1938 заедно с немски, френски и италиански език.

2 Конфедерацията е съюз на суверенни държави, които запазват много по-голяма самостоятелност, отколкото при федерацията. При конфедерацията местните органи имат много висока самостоятелност спрямо националните. Обикновено конфедералното правителство е натоварено с ограничен кръг дейности, като отбрана, външна политика, външна търговия и обща парична единица. Швейцария е федерална държава, единствена по своята същност, която е добила своето федерално управление, след като е била конфедерация. Това е причината, поради която е запазила наименованието конфедерация.

3 8. Kapitel: Geheime Überwachungsmassnahmen

4 Schweizerische Strafprozessordnung (Strafprozessordnung, StPO) vom 5. Oktober 2007 (Stand am1. Februar 2020)

5 Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 18. März 2016 (Stand am 1. März 2018)

6 Dienst für die Überwachung des Post- und Fernmeldeverkehrs

7 Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz, NDG) vom 25. September 2015 (Stand am 24. März 2020)

8 Fernmeldegesetz (FMG) vom 30. April 1997 (Stand am 1. März 2018)

9 Art. 3 Begriffe - F. Адресиращи елементи: комуникационни параметри и елементи за номериране като кодове, телефонни номера и кратки номера;

Art. 3 Begriffe - G.Комуникационни параметри: елементи за идентифициране на лица, компютърни процеси, машини, устройства или телекомуникационни системи, които участват в телекомуникационен комуникационен процес;

10 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (Stand am 1. Januar 2017)

11 Bundesgesetz vom 16. Dezember 2005 über die Ausländer - und Integrationsgesetz: Artikel 116 Absatz 3 und 118 Absatz 3;

12 Bundesgesetz vom 22. Juni 2001 zum Haager Adoptionsübereinkommen und über Massnahmen zum Schutz des Kindes bei internationalen Adoptionen: Artikel 24;

13 Kriegsmaterialgesetz vom 13. Dezember 1996: Artikel 33 Absatz 2 und 34–35b;

14 Kernenergiegesetz vom 21. März 2003: Artikel 88 Absätze 1 und 2, 89 Absätze 1 und 2 und 90 Absatz 1;

15 Betäubungsmittelgesetz vom 3. Oktober 1951: Artikel 19 Absatz 2 sowie 20 Absatz 2;

16 Umweltschutzgesetz vom 7. Oktober 1983: Artikel 60 Absatz 1 Buchstaben g–i sowie m und o;

17 Güterkontrollgesetz vom 13. Dezember 1996: Artikel 14 Absatz 2;

18 Sportförderungsgesetz vom 17. Juni 2011: Artikel 22 Absatz 2;

19 Finanzmarktinfrastrukturgesetz vom 19. Juni 2015: Artikel 154 und 155.

20 Waffengesetz vom 20. Juni 19971: Artikel 33 Absatz 3;

21 Heilmittelgesetz vom 15. Dezember 20002: Artikel 86 Absätze 2 und 3;

22 Geldspielgesetz vom 29. September 2017: Artikel 130 Absatz 2 für die Straftaten nach Artikel 130 Absatz 1 Buchstabe a.

23 Militärstrafprozess (MStP) vom 23. März 1979 (Stand am 1. Februar 2020)

24 Чл. 170 - Държавните служители и членовете на публичните власти.; чл. 171 - 1 Духовници, адвокати, защитници, нотариуси, патентни адвокати, лекари, зъболекари, фармацевти, психолози и техните асистенти ; чл.172 - Лицата, които се занимават професионално с публикуването на информация в редакционния раздел на периодично появяващ се носител, както и техните помощни лица; чл. 173 - Всеки, който трябва да поддържа професионална тайна съгласно една от подробно изброени разпоредби.