KAPITOLA I
POUŽITIE POJMOV

Článok 1
Definície

Na účely tohto dohovoru

a) „počítačový systém“ znamená zariadenie alebo skupinu vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno zariadenie alebo viaceré zariadenia vykonávajú automatizované spracúvanie údajov na základe programu,

b) „počítačové údaje“ znamenajú záznam skutočností, informácií alebo pojmov vo forme, ktorá je vhodná na spracovanie v počítačovom systéme, vrátane programu schopného spôsobiť, že počítačový systém vykoná určitú činnosť,

c) „poskytovateľ služieb“ znamená

i) verejný alebo súkromný subjekt, ktorý poskytuje používateľom svojich služieb možnosť komunikovať prostredníctvom počítačového systému,

ii) iný subjekt, ktorý spracúva alebo uchováva počítačové údaje pre takú komunikačnú službu alebo pre používateľov takej služby,

d) „prevádzkové údaje“ znamenajú počítačové údaje týkajúce sa komunikácie prostredníctvom počítačového systému vytvorené počítačovým systémom, ktorý tvoril súčasť komunikačného reťazca, s uvedením pôvodu, cieľa, trasy, času, dátumu, objemu a trvania komunikácie alebo typu služby, ktorá bola jej podkladom.

K čl. 1

„Počítačový systém“

Počítačový systém je podľa Budapeštianskeho dohovoru zariadenie pozostávajúce z hardvéru a softvéru vyvinutého na automatické spracovanie digitálnych údajov. Môže obsahovať vstupné, výstupné a úložiskové zariadenia. Môže byť samostatný alebo môže byť pripojený v sieti s inými podobnými zariadeniami. Pojem „automatické“ znamená bez priameho ľudského zásahu. Pojem „spracovanie údajov“ znamená, že údaje sú v počítačovom systéme prevádzkované prostredníctvom počítačového programu. Počítačový program je sada pokynov, ktoré môže počítač vykonať na dosiahnutie zamýšľaného výsledku. Počítačový systém sa zvyčajne skladá z rôznych zariadení ako procesor alebo centrálna procesorová jednotka, ako aj periférnych zariadení. Periférne zariadenie je zariadenie, ktoré vykonáva určité špecifické funkcie v interakcii s procesorovou jednotkou, ako je tlačiareň, obrazovka s videom, čítačka/zapisovačka CD alebo iné úložné zariadenie.

Sieť je prepojenie medzi dvoma alebo viacerými počítačovými systémami. Pripojenia môžu byť pozemné (napr. káblové), bezdrôtové (napr. rádiové, infračervené alebo satelitné) alebo oboje. Sieť môže byť geograficky obmedzená na malú oblasť (lokálne siete) alebo sa môže rozprestierať na veľkej ploche (rozsiahle siete), a tieto siete môžu byť navzájom prepojené. Internet je globálna sieť pozostávajúca z mnohých vzájomne prepojených sietí, ktoré používajú rovnaké protokoly. Existujú aj iné typy sietí, či už sú, alebo nie sú pripojené k internetu, a sú schopné komunikovať počítačové údaje medzi

počítačovými systémami. Počítačové systémy môžu byť pripojené k sieti ako koncové body alebo ako prostriedok na uľahčenie komunikácie v sieti.

Počítačový systém predstavuje počítač, fyzický alebo virtuálny, alebo súbor týchto počítačov a akýchkoľvek súčastí a /alebo príslušenstva, dočasne alebo trvalo prepojených alebo súvisiacich a jeden alebo viac z nich obsahuje počítačové programy, počítačové údaje, údaje o obsahu a/alebo prenos údajov v akejkoľvek forme, ktoré vykonávajú funkcie.

„Počítačové údaje“

Definícia počítačových údajov obsahuje pojem „vhodné na spracovanie“. To znamená, že údaje sú vložené v takej forme, aby ich bolo možné priamo spracovať počítačovým systémom. Počítačové údaje, ktoré sa automaticky spracúvajú, sa môžu stať predmetom jedného z trestných činov definovaných v Budapeštianskom dohovore.

Počítačové údaje znamenajú akékoľvek znázornenie faktov, informácií, koncepcií, prvkov, stavu alebo pokynov vo forme vhodnej na komunikáciu, interpretáciu alebo spracovanie v počítačovom programe alebo v časti programu, počítači alebo počítačovom systéme. Počítačové údaje môžu zahŕňať vývojové diagramy, knižnice, adresáre, procesné toky, interné kontroly, metadáta atď.

„Poskytovateľ služieb“

Pojem „poskytovateľ služieb“ zahŕňa širokú kategóriu osôb, ktoré zohrávajú osobitnú úlohu pri komunikácii alebo spracovaní údajov v počítačových systémoch. Ide o verejné aj súkromné subjekty, ktoré užívateľom umožňujú vzájomnú komunikáciu. Preto nie je dôležité, či používatelia tvoria uzavretú skupinu alebo či poskytovateľ ponúka svoje služby verejnosti, či už bezplatne, alebo za poplatok. Uzavretou skupinou môžu byť napríklad zamestnanci súkromného podniku, ktorým je služba ponúkaná prostredníctvom podnikovej siete.

Pojem „poskytovateľ služieb“ sa vzťahuje aj na tie subjekty, ktoré uchovávajú alebo inak spracúvajú údaje v mene týchto osôb. Ďalej tento výraz zahŕňa subjekty, ktoré ukladajú alebo inak spracúvajú údaje v mene používateľov služieb. Preto poskytovateľ služieb zahŕňa služby poskytované hostiteľskými a ukladacími službami, ako aj služby poskytujúce pripojenie k sieti. Čisto poskytovateľ obsahu (napr. osoba, ktorá uzavrie so spoločnosťou poskytujúcou *hosting* webhostingovú zmluvu) sa však na túto definíciu nevzťahuje, ak tento poskytovateľ obsahu neponúka aj komunikačné služby alebo služby súvisiace so spracovaním údajov.

Poskytovateľom služieb je akýkoľvek verejný alebo súkromný subjekt, ktorý poskytuje používateľom svojej služby schopnosť komunikovať prostredníctvom počítačového programu, počítača, počítačového systému alebo siete, vrátane služieb podporujúcich vývoj alebo využitie počítačových programov a/alebo tvorba, ukladanie, vyhľadávanie, spracovanie, správa a mazanie počítačových údajov, prevádzkových údajov a údajov o obsahu; a/alebo akýkoľvek iný subjekt, ktorý spracúva alebo ukladá počítačové údaje, údaje o obsahu alebo prevádzkové údaje v mene takejto služby alebo používateľov tejto služby.

„Prevádzkové údaje“

Na účely Budapeštianskeho dohovoru sú prevádzkové údaje definované ako kategória počítačových údajov, na ktoré sa vzťahuje osobitný právny režim. Tieto údaje generujú počítače v komunikačnom reťazci s cieľom smerovať komunikáciu od jej pôvodu k cieľu.

HLAVA 1

TRESTNÉ ČINY PROTI DÔVERNOSTI, HODNOVERNOSTI A DOSTUPNOSTI POČÍTAČOVÝCH ÚDAJOV A SYSTÉMOV

K hlave 1

Trestné činy definované v čl. 2 až 6 Budapeštianskeho dohovoru sú určené na ochranu dôvernosti, integrity a dostupnosti počítačových systémov alebo dát a nie na kriminalizáciu legitímnych a bežných činností spojených s dizajnom sietí alebo legitímnych a bežných prevádzkových alebo obchodných praktík.

Článok 2
Nezákonný prístup

Každá strana prijme potrebné legislatívne a iné opatrenia, aby neoprávnený prístup do počítačového systému ako celku alebo do jeho časti bol trestným činom podľa jej vnútroštátneho právneho poriadku, ak bol spáchaný úmyselne. Strana môže trestnosť činu podmieniť tým, že musí byť spáchaný porušením bezpečnostných opatrení s úmyslom získať počítačové údaje alebo s iným nečestným úmyslom, alebo vo vzťahu k počítačovému systému prepojenému s iným počítačovým systémom.

K čl. 2

Od vývoja počítačových sietí boli počítače hackermi na základe svojej schopnosti využívané na trestné účely. V motivácii hackerov existujú značné rozdiely. Hackeri nemusia byť prítomní na mieste činu; musia len obísť ochranu zabezpečujúcu sieť. V mnohých prípadoch nelegálneho prístupu sú bezpečnostné systémy chrániace fyzické umiestnenie sieťového hardvéru sofistikovanejšie ako bezpečnostné systémy chrániace citlivé informácie v sieťach, a to aj v tej istej budove. Nezákonný prístup k počítačovým systémom prekáža počítačovým operátorom v riadení a prevádzke ich systémov. Cieľom ochrany je zachovať integritu počítačových systémov. Je nevyhnutné rozlišovať medzi nezákonným prístupom a následnými trestnými činmi (napr. špionáž údajov), pretože právne ustanovenia majú odlišné zameranie ochrany. Vo väčšine prípadov nie je nelegálny prístup (ak sa zákon snaží chrániť integritu samotného počítačového systému) konečným cieľom, ale skôr prvým krokom k ďalším trestným činom, ako je úprava alebo získanie uložených údajov.

Analýza rôznych prístupov ku kriminalizácii nelegálneho prístupu k počítačom na vnútroštátnej úrovni ukazuje, že prijaté ustanovenia niekedy zamieňajú nelegálny prístup s následnými trestnými činmi alebo sa usilujú obmedziť kriminalizáciu nelegálneho prístupu iba k závažným porušeniam. Niektoré krajiny kriminalizujú jednoduchý prístup, zatiaľ čo iné obmedzujú kriminalizáciu iba na trestné činy, pri ktorých je prístup do systému chránený bezpečnostnými opatreniami alebo pri ktorých má páchateľ nezákonné úmysly, alebo pri ktorých boli získané, upravené alebo poškodené údaje. Ostatné krajiny netrestajú samotný prístup, ale iba následné trestné činy. Odporcovia kriminalizácie nelegálneho prístupu sa odvolávajú na situácie, v ktorých nevzniklo žiadne nebezpečenstvo alebo ak *hacking* viedol k odhaleniu medzier v bezpečnosti cieľových počítačových systémov.

Pojem „prístup“ nešpecifikuje určité komunikačné prostriedky, ale je otvorený ďalšiemu technickému rozvoju. Zahŕňa všetky prostriedky vstupu do iného počítačového systému vrátane útokov na internet, ako aj nelegálny prístup k bezdrôtovým sieťam. Toto sa vzťahuje aj na neoprávnený prístup k počítačom, ktoré nie sú pripojené k žiadnej sieti. Tento široký prístup znamená, že nelegálny prístup sa nevzťahuje iba na budúci technický vývoj, ale týka sa aj tajných údajov, ku ktorým majú prístup zamestnanci. Druhá veta čl. 2 Budapeštianskeho dohovoru ponúka možnosť obmedziť kriminalizáciu nezákonného prístupu prostredníctvom siete. Nezákonné činy a chránené systémy sú teda definované spôsobom, ktorý zostáva otvorený ďalšiemu vývoju.

Prístup k počítaču možno podľa čl. 2 Budapeštianskeho dohovoru stíhať, iba ak k nemu dôjde „neoprávnene“. Prístup do systému umožňujúceho voľný a otvorený prístup verejnosti alebo prístup do systému so súhlasom vlastníka alebo iného držiteľa práv nenapĺňa túto požiadavku. Správcovia sietí a bezpečnostné spoločnosti, ktoré testujú ochranu počítačových systémov s cieľom zistiť možné medzery v bezpečnostných opatreniach, si dávajú pozor na riziko kriminalizácie pri nelegálnom prístupe. Napriek skutočnosti, že títo odborníci vo všeobecnosti pracujú na základe súhlasu, je potrebné zdôrazniť, že testovanie alebo ochrana bezpečnosti počítačového systému autorizovaného vlastníkom alebo prevádzkovateľom, sú v súlade právom. Skutočnosť, že obeť trestného činu poskytla páchateľovi heslo alebo podobný prístupový kód, nevyhnutne neznamená, že páchateľ potom pri prístupe do počítačového systému obete konal zákonne. Ak páchateľ presvedčil obeť, aby poskytla heslo alebo prístupový kód pomocou úspešného prístupu v oblasti sociálneho inžinierstva, je potrebné overiť, či sa povolenie vydané obeťou vzťahuje na čin, ktorý páchateľ spáchal. Spravidla to tak nie je a páchateľ preto koná neoprávnene.

„Nezákonný prístup“ v zmysle čl. 2 Budapeštianskeho dohovoru sa týka základných princípov ako je dôvernosť, integrita a dostupnosť počítačových systémov a údajov. Samotné neoprávnené vniknutie („hacknutie“) by malo byť v zásade samo osebe nezákonné. Takéto prieniky môžu umožniť prístup k dôverným údajom (vrátane hesiel, informácií o cieľovom systéme) a k použitiu systému bez platieb alebo dokonca môžu nabádať hackerov k páchaniu nebezpečnejších foriem počítačových trestných činov, ako sú počítačové podvody alebo útoky.

Najefektívnejším prostriedkom na zabránenie neoprávnenému prístupu je samozrejme zavedenie a vývoj účinných bezpečnostných opatrení. Komplexná reakcia však musí zahŕňať aj hrozbu a použitie trestnoprávnych opatrení. Zákaz prístupu môže poskytnúť ďalšiu ochranu systému a údajom ako takým, a to už v rannom štádiu pred už skôr opísanými nebezpečenstvami.

„Prístup“ zahŕňa vstup do celého alebo ktorejkoľvek časti počítačového systému (hardvér, jeho komponenty, uložené údaje, adresáre, údaje o prevádzke a obsahu). Nezahŕňa však iba zasielanie e-mailových správ alebo súborov do tohto systému. „Prístup“ zahŕňa vstup do iného počítačového systému, ktorý je pripojený cez verejné telekomunikačné siete, alebo k počítačovému systému v tej istej sieti, ako je LAN (lokálna sieť) alebo intranet v rámci organizácie.

Výsledkom použitia špecifických technických nástrojov môže byť prístup (podľa čl. 2 Budapeštianskeho dohovoru) realizovaný napríklad na webovú stránku, priamo alebo prostredníctvom hypertextových odkazov vrátane priamych odkazov alebo použitia „*cookies*“ alebo „robotov“ na vyhľadanie a získanie informácií. Samotné použitie takýchto nástrojov neznamená konanie *per se* „bez oprávnenia“. Údržba verejnej webovej stránky

predpokladá súhlas vlastníka webovej stránky s tým, že k nej môže mať prístup ktorýkoľvek iný používateľ webovej stránky. Uplatňovanie štandardných nástrojov ustanovených v bežne používaných komunikačných protokoloch a programoch nie je samo osebe „bez oprávnenia".

Článok 3
Nezákonné zachytenie údajov

Každá strana prijme potrebné legislatívne a iné opatrenia, aby neoprávnené zachytávanie neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v rámci tohto systému vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje také počítačové údaje vykonané technickými prostriedkami, bolo trestným činom podľa jej vnútroštátneho právneho poriadku, ak bolo spáchané úmyselne. Strana môže trestnosť činu podmieniť tým, že musí byť spáchaný s nečestným úmyslom alebo vo vzťahu k počítačovému systému prepojenému s iným počítačovým systémom.

K čl. 3

Používanie IKT sprevádza niekoľko rizík súvisiacich s bezpečnosťou prenosu informácií. Na rozdiel od klasických operácií zahŕňajú procesy prenosu dát cez internet množstvo poskytovateľov a rôznych miest, kde je možné proces prenosu dát zachytiť. Najslabšou stránkou zachytávania údajov zostáva používateľ, a to najmä používatelia súkromných domácich počítačov, ktorí sú často nedostatočne chránení pred vonkajšími útokmi. Pretože páchatelia sa vždy zameriavajú na najslabšie miesto, riziko útokov na súkromných používateľov je veľké.

Nové sieťové technológie (napr. „bezdrôtová sieť LAN") ponúkajú niekoľko výhod prístupu na internet, napríklad nastavenie bezdrôtovej siete v súkromnom dome umožňuje rodinám pripojiť sa k internetu odkiaľkoľvek v danom okruhu, bez potreby káblového pripojenia. Popularitu tejto technológie a výsledný komfort však sprevádzajú vážne riziká pre bezpečnosť siete. Ak je k dispozícii nechránená bezdrôtová sieť, páchatelia sa môžu prihlásiť do tejto siete a použiť ju na trestné účely bez potreby prístupu do budovy. Vo väčšine prípadov nedostatok ochrany vyplýva z nedostatku vedomostí o tom, ako nakonfigurovať ochranné opatrenia. V minulosti sa páchatelia sústreďovali najmä na obchodné siete pre nelegálne zachytávanie údajov. Zachytenie podnikovej komunikácie pravdepodobne poskytlo užitočné informácie ako zachytenie údajov prenesených v súkromných sieťach. Zvyšujúci sa počet krádeží identity súkromných osobných údajov naznačuje, že zameranie páchateľov sa mení.

Uplatniteľnosť čl. 3 Budapeštianskeho dohovoru sa obmedzuje na zachytávanie prenosov realizovaných technickými opatreniami. Ako už bolo skôr uvedené, otázka, či toto ustanovenie upravuje nelegálny prístup k informáciám uloženým na pevnom disku, je kontroverzná a často diskutovaná. Toto ustanovenie sa vo všeobecnosti vzťahuje iba na zachytávanie prenosov - prístup k uloženým informáciám sem nepatrí. Skutočnosť, že o použití tohto ustanovenia sa diskutuje aj v prípadoch, keď sa páchateľ fyzicky dostane k samostatnému počítačovému systému, čiastočne vyplýva zo skutočnosti, že Budapeštiansky dohovor neobsahuje ustanovenie týkajúce sa špionáže údajov. Dôvodová správa

predovšetkým poukazuje na to, že ustanovenie sa týka komunikačných procesov prebiehajúcich v počítačovom systéme. Stále však zostáva otvorená otázka, či by sa ustanovenie malo uplatňovať iba v prípadoch, keď obete zasielajú údaje, ktoré potom zachytia páchatelia, alebo či by sa malo uplatniť aj vtedy, keď páchateľ ovláda počítač. Druhý bod súvisí s kriminalizáciou nelegálneho získavania počítačových údajov.

Cieľom čl. 3 Budapeštianskeho dohovoru je teda chrániť právo na súkromie pri dátovej komunikácii. Trestný čin predstavuje rovnaké porušenie súkromia komunikácie ako tradičné zachytávanie a zaznamenávanie ústnych telefonických rozhovorov medzi osobami. Právo na súkromie je zakotvené v čl. 8 EDĽP. Trestný čin ustanovený v čl. 3 Budapeštianskeho dohovoru uplatňuje túto zásadu na všetky formy elektronického prenosu údajov, či už telefonicky, faxom, e-mailom, alebo prostredníctvom prenosu súborov.

Zachytávanie „technickými prostriedkami" sa týka monitorovania alebo sledovania obsahu komunikácií, získavania obsahu údajov buď priamo, prostredníctvom prístupu a používania počítačového systému, alebo nepriamo, pomocou elektronického zachytávania. Zachytávanie môže zahŕňať aj nahrávanie. Technické prostriedky zahŕňajú technické zariadenia pripojené k prenosovým linkám, ako aj zariadenia na zhromažďovanie a zaznamenávanie bezdrôtovej komunikácie. Môžu zahŕňať použitie softvéru, hesiel a kódov.

Trestný čin sa týka „neverejného" prenosu počítačových údajov. Pojem „neverejný" kvalifikuje povahu procesu prenosu (komunikácie), a nie povahu prenášaných údajov. Pojem „neverejný" preto sám osebe nevylučuje komunikáciu prostredníctvom verejných sietí. Komunikácia zamestnancov, tiež na obchodné účely, ktorá predstavuje „neverejný prenos počítačových údajov", je tiež chránená proti neoprávnenému zachytávaniu podľa čl. 3 Budapeštianskeho dohovoru (rozsudok ESĽP z 25. júna 1997 vo veci *Halford proti Veľkej Británii*, sťažnosť č. 20605/92).

Komunikácia vo forme prenosu počítačových údajov sa môže uskutočňovať vo vnútri jedného počítačového systému, medzi dvoma počítačovými systémami patriacimi tej istej osobe, dvoma počítačmi navzájom komunikujúcimi alebo počítačom a osobou (napr. prostredníctvom klávesnice).

Pojem „prenos" zahŕňa všetky dátové prenosy, či už telefonické, faxové, e-mailové, alebo súborové. Trestný čin definovaný v čl. 3 Budapeštianskeho dohovoru sa vzťahuje iba na neverejné prenosy. Prenos je „neverejný", ak je proces prenosu dôverný. Dôležitým prvkom na rozlíšenie medzi verejným a neverejným prenosom nie je povaha prenášaných údajov, ale povaha samotného procesu prenosu. Aj prenos verejne prístupných informácií možno považovať za trestný, ak majú strany zapojené do prenosu v úmysle utajiť obsah svojej komunikácie. Používanie verejných sietí nevylučuje „neverejnú" komunikáciu.

Zachytávanie komunikácie môže byť stíhané podľa čl. 3 Budapeštianskeho dohovoru, iba ak k nemu dôjde „neoprávnene". Medzi súbor príkladov, ktoré sa nevykonávajú neoprávnene, patria napríklad opatrenia na základe pokynov alebo na základe oprávnenia účastníkov prenosu, autorizované testovacie alebo ochranné činnosti odsúhlasené účastníkmi a zachytávanie údajov na základe ustanovení trestného práva alebo v záujme národnej bezpečnosti. Ďalším problémom je otázka, či by používanie súborov *cookies* viedlo k trestným sankciám na základe čl. 3 Budapeštianskeho dohovoru. Na tomto mieste je potrebné upozorniť na tú skutočnosť, že bežné obchodné praktiky (napr. súbory *cookies*) sa nepovažujú za neoprávnené zachytávanie.

Aby mohla byť stanovená trestná zodpovednosť, musí byť nezákonné zachytávanie spáchané „úmyselne" a „bez oprávnenia". Skutok je opodstatnený napríklad vtedy, ak má

KAPITOLA III
MEDZINÁRODNÁ SPOLUPRÁCA

Ku kapitole III

Kapitola III Budapeštianskeho dohovoru obsahuje niekoľko ustanovení týkajúcich sa extradície a vzájomnej právnej pomoci. Táto kapitola poskytuje právny rámec pre medzinárodnú spoluprácu so všeobecnými a konkrétnymi opatreniami vrátane povinnosti krajín spolupracovať v čo najväčšom rozsahu. Vyšetrovanie jedného prípadu počítačovej kriminality často zahŕňa systémy trestného súdnictva v rôznych krajinách, čo si vyžaduje intenzívnu medzinárodnú spoluprácu.

Oddiel 1
Všeobecné zásady

K oddielu 1

Počítačová kriminalita je do veľkej miery nadnárodnou trestnou činnosťou. V rámci medzinárodnej spolupráce sú nevyhnutné aj neodkladné opatrenia potrebné na uchovanie údajov. Bez výraznej spolupráce medzi národmi a prijatia nových stratégií zostanú orgány činné v trestnom konaní pozadu a budú bojovať proti zločinu 21. storočia pomocou nástrojov z 19. storočia. Počítačová kriminalita si vyžaduje zvýšenie spolupráce medzi štátmi a vyžaduje efektívnejšie vyšetrovacie metódy. Budapeštiansky dohovor sa v čl. 23 až 35 zaoberá zvyšujúcim sa významom medzinárodnej spolupráce.

HLAVA 1

VŠEOBECNÉ ZÁSADY TÝKAJÚCE SA MEDZINÁRODNEJ SPOLUPRÁCE

K hlave 1

V hlave 1 tejto kapitoly Budapeštianskeho dohovoru sú definované tri všeobecné zásady týkajúce sa medzinárodnej spolupráce pri vyšetrovaní počítačovej kriminality.

Článok 23
Všeobecné zásady týkajúce sa medzinárodnej spolupráce

Strany spolupracujú v súlade s ustanoveniami tejto kapitoly a s použitím príslušných medzinárodných nástrojov na medzinárodnú spoluprácu v trestných veciach, dojednaní prijatých na základe vzorového zákona alebo vzájomnosti a vnútroštátnych zákonov v čo najväčšom rozsahu na účely vyšetrovania alebo konania o trestných činoch súvisiacich s počítačovými systémami a údajmi alebo na zhromažďovanie dôkazov o trestnom čine v elektronickej forme.

K čl. 23

Význam medzinárodnej spolupráce pri vyšetrovaní počítačovej kriminality vychádza z poskytovaní spolupráce v čo najväčšom rozsahu. V čl. 23 Budapeštianskeho dohovoru sú ustanovené tri všeobecné zásady týkajúce sa medzinárodnej spolupráce podľa kapitoly III Budapeštianskeho dohovoru. V čl. 23 Budapeštianskeho dohovoru sa uvádza, že všeobecné zásady sa neuplatňujú iba pri vyšetrovaní v oblasti počítačovej kriminality, ale aj pri akomkoľvek vyšetrovaní, pri ktorom je potrebné zhromažďovať dôkazy v elektronickej podobe. Týka sa to vyšetrovania počítačovej kriminality, ako aj vyšetrovania v tradičných prípadoch. Ak podozrivý z vraždy použil e-mailovú službu v zahraničí, čl. 23 Budapeštianskeho dohovoru by sa použil, pokiaľ ide o vyšetrovania, ktoré sú potrebné, pokiaľ ide o údaje uložené hostiteľským poskytovateľom. Ustanovenia týkajúce sa medzinárodnej spolupráce nenahrádzajú ustanovenia medzinárodných dohôd o vzájomnej právnej pomoci a vydávaní ani príslušné ustanovenia vnútroštátneho práva týkajúce sa medzinárodnej spolupráce.

Spolupráca sa má rozšíriť na všetky trestné činy súvisiace s počítačovými systémami a údajmi [t. j. na trestné činy uvedené v čl. 14 ods. 2 písm. a) a b) Budapeštianskeho dohovoru], ako aj na zhromažďovanie dôkazov v elektronickej podobe o trestnom čine. To znamená, že ak je trestný čin spáchaný pomocou počítačového systému, alebo ak trestný čin nespáchaný pomocou počítačového systému (napr. vražda) zahŕňa elektronické dôkazy, uplatňujú sa ustanovenia kapitoly III Budapeštianskeho dohovoru. Je však potrebné poznamenať, že čl. 24 (extradícia), čl. 33 (vzájomná pomoc pri zhromažďovaní prevádzkových údajov v reálnom čase) a čl. 34 (vzájomná pomoc pri zachytávaní údajov o obsahu) Budapeštianskeho dohovoru umožňujú zmluvným stranám ustanoviť iný rozsah uplatňovania týchto opatrení.

Spolupráca sa nakoniec musí uskutočňovať v súlade s ustanoveniami tejto kapitoly a prostredníctvom uplatňovania príslušných medzinárodných dohôd o medzinárodnej spolupráci v trestných veciach. Ustanovenia kapitoly III Budapeštianskeho dohovoru nenahrádzajú ustanovenia medzinárodných dohôd o vzájomnej právnej pomoci alebo príslušné ustanovenia vnútroštátneho práva týkajúce sa medzinárodnej spolupráce. Táto základná zásada je výslovne posilnená v čl. 24 (extradícia), čl. 25 (všeobecné zásady týkajúce sa vzájomnej pomoci), čl. 26 (spontánne informácie), čl. 27 (postupy vzťahujúce sa na žiadosti o vzájomnú pomoc v prípade, keď neexistujú použiteľné medzinárodné dohody), čl. 28 (dôvernosť a obmedzenie použitia), čl. 31 (vzájomná pomoc týkajúca sa prístupu k uloženým počítačovým údajom), čl. 33 (vzájomná pomoc pri zhromažďovaní prevádzkových údajov v reálnom čase) a čl. 34 (vzájomná pomoc týkajúca sa zachytenia obsahových údajov) Budapeštianskeho dohovoru.

HLAVA 2

ZÁSADY TÝKAJÚCE SA EXTRADÍCIE

K hlave 2

Vydávanie štátnych príslušníkov zostáva jedným z najťažších aspektov medzinárodnej spolupráce. Žiadosti o vydanie veľmi často vedú ku konfliktu medzi potrebou ochrany občana a potrebou podpory prebiehajúceho vyšetrovania. V čl. 24 Budapeštianskeho

dohovoru sa vymedzujú zásady vydávania. Na rozdiel od čl. 23 Budapeštianskeho dohovoru sa ustanovenie obmedzuje na trestné činy uvedené v Budapeštianskom dohovore a neuplatňuje sa na prípady menšej závažnosti (pozbavenie osobnej slobody na obdobie menej ako 1 rok).

Článok 24
Extradícia

1.

a) Tento článok sa použije na vydanie medzi stranami pre trestné činy vymedzené podľa článkov 2 až 11 tohto dohovoru za predpokladu, že podľa právnych poriadkov oboch dotknutých strán za ne možno uložiť trest odňatia slobody alebo ochranné opatrenie s hornou hranicou najmenej jeden rok alebo prísnejší trest.

b) Ak sa podľa dojednania prijatého na základe vzorového zákona alebo vzájomnosti, alebo extradičnej zmluvy vrátane Európskeho dohovoru o vydávaní (ETS č. 24), ktoré sa dajú použiť medzi dvoma alebo viacerými stranami, má uplatniť iný minimálny trest, použije sa minimálny trest ustanovený takým dojednaním alebo zmluvou.

2. Trestné činy uvedené v odseku 1 sa považujú za extradičné trestné činy v každej extradičnej zmluve, ktorou sú navzájom viazané. Strany sa zaväzujú zahrnúť také trestné činy ako extradičné do každej extradičnej zmluvy, ktorú medzi sebou uzatvoria.

3. Ak strana, ktorá podmieňuje vydanie existenciou zmluvy, dostane žiadosť o vydanie od inej strany, s ktorou nemá uzatvorenú extradičnú zmluvu, môže považovať tento dohovor za právny základ na vydanie vo vzťahu ku každému trestnému činu uvedenému v odseku 1.

4. Strany, ktoré nepodmieňujú vydanie existenciou zmluvy, uznávajú medzi sebou trestné činy uvedené v odseku 1 za extradičné trestné činy.

5. Vydanie podlieha podmienkam ustanoveným právnym poriadkom dožiadanej strany alebo použiteľnými extradičnými zmluvami vrátane dôvodov, na ktorých základe môže dožiadaná strana odmietnuť vydanie.

6. Ak sa vydanie za trestný čin uvedený v odseku 1 odmietne výlučne z dôvodu štátneho občianstva vyžiadanej osoby alebo z dôvodu, že dožiadaná strana zastáva názor, že má právomoc konať o trestnom čine, dožiadaná strana predloží prípad na žiadosť dožadujúcej strany svojim príslušným orgánom na účely trestného stíhania a v primeranej lehote podá správu o konečnom výsledku dožadujúcej strane. Tieto orgány prijmú rozhodnutie a vedú vyšetrovanie a konanie rovnakým spôsobom ako v prípade trestných činov porovnateľnej povahy podľa právneho poriadku tejto strany.

7.

a) Každá strana oznámi pri podpise alebo pri ukladaní svojej ratifikačnej listiny, listiny o prijatí, schválení alebo o prístupe generálnemu tajomníkovi Rady Európy názov a adresu každého orgánu zodpovedného za zasielanie alebo

prijímanie žiadostí o vydanie alebo za predbežnú väzbu v prípade, ak neexistuje zmluva.

b) Generálny tajomník zriadi a aktualizuje register orgánov takto určených stranami. Každá strana priebežne zabezpečuje správnosť jednotlivých údajov v registri.

K čl. 24

Pre vyšetrovanie počítačovej kriminality sú najdôležitejšími formálnymi mechanizmami podporujúcimi medzinárodnú spoluprácu vzájomná právna pomoc a extradícia. Ostatné mechanizmy, ako napríklad konfiškácia výnosov z trestnej činnosti a vymáhanie majetku, sú v praxi menej významné. Okrem formálnych mechanizmov existujú neformálne spôsoby spolupráce, ako napríklad výmena spravodajských informácií medzi orgánmi činnými v trestnom konaní v rôznych krajinách.

Úspešná koordinácia operácie „Baltico" súvisela s organizovanou cezhraničnou trestnou činnosťou páchateľov. Prostredníctvom Eurojustu (Agentúra EÚ pre justičnú spoluprácu v trestných veciach) a Europolu (Európsky policajný úrad) sa vykonali koordinačné stretnutia v Taliansku a v Holandsku za účasti zástupcov dotknutých členských štátov. Účelom koordinačných stretnutí bolo dosiahnutie vzájomného porozumenia rozsahu stíhaných trestných vecí v zainteresovaných členských štátoch. Na základe výsledkov stretnutí bolo rozhodnuté, že na vedenie jednotného vyšetrovania a trestného stíhania bude príslušné Taliansko.

Pozitívny konflikt jurisdikcií môže za určitých okolností vyústiť do tzv. prekážky *ne bis in idem*, najmä keď na vyšetrovanie a trestné stíhanie trestných činov je oprávnených viac jurisdikcií. V tomto prípade býva trestné stíhanie vedené paralelne vo viacerých štátoch. Členský štát aplikujúci princíp legality nemôže nevykonať trestné stíhanie trestného činu, ktorý spadá do jeho jurisdikcie. V tomto prípade v záujme vyriešenia konfliktu jurisdikcií je potrebné nájsť dôvod na odovzdanie trestného stíhania do druhého štátu. Problém nastáva v prípade, keď členský štát kombinuje princíp teritoriality s princípom aktívnej personality, napríklad ak členský štát trestne stíha vlastných občanov za trestný čin spáchaný na území iného štátu.

Subjektívna teritorialita môže slúžiť ako prekážka vydaniu tak, že sa pojednávanie umiestni tam, kde došlo k rozšíreniu ktorejkoľvek kľúčovej zložky trestného činu, bez ohľadu na to, či je účinok badateľný niekde inde. Naopak, objektívna teritorialita umožňuje štátu uplatniť si jurisdikciu extrateritoriálne. Vzťah medzi extradíciou a zákonmi o ľudských právach sa zakladá na vzájomnej dôvere, že justičné systémy v každej zúčastnenej jurisdikcii fungujú podľa spoločne dohodnutých štandardov. Uplatňovanie medzinárodných záruk v oblasti ľudských práv môže byť tiež ťažké dosiahnuť na domácich súdoch. Preto mechanizmy spravodlivého procesu na vnútroštátnej úrovni, zohrávajú dôležitú úlohu pri ochrane práv jednotlivca.

V čl. 24 ods. 1 Budapeštianskeho dohovoru sa uvádza, že povinnosť vydania sa vzťahuje iba na trestné činy ustanovené v súlade s čl. 2 až 11 Budapeštianskeho dohovoru, ktoré sú podľa právnych predpisov oboch strán dotknuté odňatím slobody na obdobie najmenej jedného roka alebo viac. Podľa Budapeštianskeho dohovoru môžu strany potrestať niektoré z trestných činov relatívne krátkym maximálnym časom (napr. čl. 2 a čl. 4). V súlade s tým bola dosiahnutá dohoda o všeobecnej požiadavke, aby k extradícii mohlo dôjsť, ak trest, ktorý možno uložiť za trestný čin, sa vzťahuje sa trest odňatia slobody najmenej