A magyar büntető eljárás és a digitalizáció

Domokos Andrea*

Életünk digitalizálódott. Így van ez a legális és az illegális szférában egyaránt. A bűnelkövetők Magyarországon és szerte a világban nagy számban használnak digitális eszközöket bűncselekményeik végrehajtására. A kiberbűnözés tipikusan határokon átívelő jellegű, ami egyrészt könnyebb menekülési útvonalat jelent az elkövető számára és nehézséget okoz a bűncselekmények felderítése során. A magyar Büntető Eljárási Kódex is tartalmaz rendelkezéseket az elektronikus kapcsolattartással és az elektronikus adatokat érintő kényszerintézkedésekkel kapcsolatban.

1. A bűnüldözés és a XXI. századi digitalizáció

A büntetőjog, büntető eljárásjog, sőt a büntetés-végrehajtási jog sem marad érintetlen a technikai, technológiai modernizációs folyamatok változásai során. A hivatalos értesítések ügyfélkapura érkeznek, a bankügyeket online intézik. A nyomozóhatóságok valamennyi levélküldeményét (belföldi jogsegély, idézés, stb.) elektronikusan küldik ki.

Vannak olyan társadalomtudósok, akik már veszélyesnek tartják a technológiai fejlődést, állítván, hogy egyoldalúvá teszi a társadalmi rendszereket és a tudományos eredményekkel nem képes lépést tartani a társadalom erkölcsi fejlődése. Fukuyama szerint, „ha egy társadalom szerint »nincs határ« a technológiai fejlődésben, akkor ott valószínűleg semmi másban sincsenek határok, így az egyén viselkedésében sem, s nő a bűnözés, felbomlanak a családok, a szülők nem teljesítik kötelességeiket gyermekeikkel szemben, a szomszédok nem figyelnek egymásra, s a polgárok nem vesznek részt a közéletben."[1]

Ahogy a bűnözők igénybe veszik a rendelkezésre álló új technológiákat, úgy a hatóságoknak is szükségszerűen reagálniuk kell a megváltozott bűnözési formákra. A digitalizáció új eszközeit a bűnüldözőknek, a bíróságoknak és a büntetés-végrehajtásnak is használnia kell.

* Intézetvezető egyetemi tanár, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar.

[1] Francis Fukuyuma: *A nagy szétbomlás*, Budapest, Európa, 2000, 31. o.

A büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be. tv.) a bizonyítás eszközei között szabályozza a tanúvallomást, a terhelt vallomását, a szakvéleményt, a pártfogó felügyelői véleményt, valamint a tárgyi bizonyítási eszköz mellett az elektronikus adatot is (Be. tv. 165. §). A Be. külön fejezetben határozza meg az elektronikus adat fogalmát, amely szerint elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja (Be. tv. 205. § (1) bekezdése). A törvény megfogalmazza, hogy az elektronikus adat – a törvény eltérő rendelkezése hiányában – tárgyi bizonyítási eszköznek tekintendő. Az elektronikus adat jelentősége abban rejlik, hogy mára a bűnügyi nyomozások több mint fele olyan határokon átnyúló kérelmet tartalmaz, amely az elektronikus bizonyítékok (e-mailek, üzenetküldő alkalmazások) elérését célozza.

A bűnüldözés speciális területe a kriptovaluták[2] útjának felderítése. A kriptovaluták kiemelten veszélyeztetettek az illegális felhasználás tekintetében. Megjelenésük nagyban megnehezítette a bűncselekmények felderítését. A kriptovaluták esetében nem létezik egységes szabályozás, a világ különböző országai eltérő módon ítélik meg. Nyomozási szempontból kihívás, hogy a számlák, „pénztárcák" anonimak, nem névhez kötöttek. A kibertérben elkövetett bűncselekmények esetében alapvető kriminilisztikai feltétel az IP címek felderítése. Az IP címhez köthető pontos földrajzi hely azonban csak az IP címhez adott országhoz intézett nemzetközi jogsegély keretében ismerhető meg. Továbbá kis mértékű a közvetlen kapcsolódás a cselekmény és az elkövető közt, aki a helyszíntől több ezer kilométerre is tartózkodhat az elkövetés pillanatában. A büntetőeljárás során szükségessé válhat a vagyonelkobzás biztosítása érdekében az üggyel összefüggésbe hozható bitcoin lefoglalása. A lefoglalást a bűncselekményből származó vagyonból vásárolt virtuális fizetési eszköz egészére kell végrehajtani a bitcoin volatilitásának figyelmen kívül hagyásával, ugyanis a Btk. 74. § d) pontja alapján vagyonelkobzást kell elrendelni arra a vagyonra, amely a bűncselekmény elkövetéséből eredő, a bűncselekmény elkövetése során vagy azzal összefüggésben szerzett vagyon helyébe lépett. Ahhoz, hogy ez megvalósuljon, a lefoglalást foganatosító hatóságnak hozzá kell férnie az elkövető tárcájához. Ebben a tárcában találhatóak a privát kulcsok, melyeket meg kell ismerni ahhoz, hogy a bitcoinokat el lehessen küldeni egy új, a hatóság által ellenőrzött címre.

A kriptovaluták területén igen hatékony megoldást kínál a mesterséges alapú megoldások alkalmazása, a neurális hálók képesek megtanulni a nyomozási eszközöket és módszereket, így segítve a hatóságot a munkája során. Az ilyen jellegű berendezések használhatók arra, hogy gyanús pénzügyi műveleteket szűrjenek ki, vagy az interneten keressenek money muling[3] hirdetéseket.

[2] Ld. Cryptocurrencies: A Brief Thematic Review Archived 2017-12-25 at the Wayback Machine. Economics of Networks Journal. Social Science Research Network (SSRN).

[3] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/money-muling , 2019. szeptember 2.

2. Elektronikus kapcsolattartás a magyar büntetőeljárásban

A büntetőeljárásról szóló törvény XXVII. fejezete foglalkozik az elektronikus kapcsolattartással. Létezik kötelező esete és választani is lehet a kapcsolattartás ezen formáját. Az elektronikus kapcsolattartásra köteles büntetőeljárásban részt vevő személy minden beadványt kizárólag elektronikus úton nyújthat be a bírósághoz, az ügyészséghez és a nyomozó hatósághoz, és a bíróság, az ügyészség, illetve a nyomozó hatóság is elektronikus úton kézbesít a részére. Csak akkor mentesül a kötelező elektronikus kapcsolattartás alól, ha elektronikus ügyintézéshez való joga szünetel.

Az elektronikus kapcsolattartás vállalása esetében az eljárás folyamán a büntetőeljárásban részt vevő személy, illetve jogi képviselőnek nem minősülő képviselője köteles a bírósággal, az ügyészséggel és a nyomozó hatósággal a kapcsolatot elektronikus úton tartani. A bíróság, az ügyészség és a nyomozó hatóság is valamennyi ügyiratot elektronikus úton kézbesít a részére.

Ha az elektronikus kapcsolattartásra nem köteles büntetőeljárásban részt vevő személy vagy a jogi képviselőnek nem minősülő képviselője az eljárásban még nem vállalta az elektronikus kapcsolattartást, a bíróság, az ügyészség és a nyomozó hatóság a részére papíralapon történő első kézbesítéssel egyidejűleg tájékoztatja arról, hogy a továbbiakban e törvény rendelkezései szerint vállalhatja az elektronikus kapcsolattartást (Be. tv. 150. §).

Ha a szakértő elektronikus kapcsolattartásra köteles vagy maga vállalja azt, a szakvéleményét és egyéb beadványát elektronikus úton nyújtja be a bírósághoz, az ügyészséghez és a nyomozó hatósághoz és a bíróság, az ügyészség és a nyomozó hatóság is valamennyi ügyiratot elektronikus úton kézbesít a részére (Be. tv. 151. §).

A büntetőeljárás során az Országos Bírósági Hivatal és az egyéb elektronikus ügyintézést biztosító szervek jogosultak az elektronikus úton kapcsolatot tartóknak az elektronikus kapcsolattartás biztosítása céljából hozzájuk érkezett adatainak kezelésére.

A bíróság, az ügyészség és a nyomozó hatóság az elektronikus úton kézbesített ügyiratot minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírással vagy elektronikus bélyegzővel látja el. A bíróság, az ügyészség és a nyomozó hatóság által készített, minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírással vagy elektronikus bélyegzővel ellátott ügyirat közokirat. Aláírás alatt a bíróság, az ügyész és a nyomozó hatóság minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírását vagy elektronikus bélyegzőjét is érteni kell (Be. tv. 158. §).

A büntetőeljárásban részt vevő személy, valamint a bírósági eljárásban az ügyészség indítványozhatja, hogy a bíróság, az ügyészség, illetve a nyomozó hatóság az általa megismerhető ügyirat másolatát elektronikus formában adathordozón vagy az általa megjelölt elektronikus levelezési címre továbbítsa, ha az ügyirat elektronikus formában, elektronikus okiratként, vagy a papíralapú okirat elektronikus másolataként az eljáró bíróságnál, ügyészségnél, illetve nyomozó

hatóságnál rendelkezésre áll. Az ügyirat akkor áll elektronikus formában rendelkezésre, ha a bíróság, az ügyészség, illetve a nyomozó hatóság a papíralapú ügyiratot információs rendszer alkalmazásával szerkesztette meg (Be. tv. 159. §).

3. Elektronikus adatokat érintő kényszerintézkedések a magyar büntetőeljárásban

3.1. Az elektronikus adat lefoglalása. Mind az elektronikus adatot, mind az információs rendszert le lehet foglalni, ezt a kényszerintézkedést úgy kell végrehajtani, hogy az a büntetőeljárás céljából szükségtelen elektronikus adatra lehetőleg ne terjedjen ki, illetve az ilyen elektronikus adatot a lefoglalás a legrövidebb ideig érintse.

Az elektronikus adat lefoglalását az elektronikus adatról másolat készítésével, az elektronikus adat áthelyezésével, az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével, az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával lehet végrehajtani.

A fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, hogy az elektronikus adattal olyan műveletet végeznek, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét megakadályozza.

Az elektronikus adatot tartalmazó információs rendszer vagy adathordozó akkor foglalható le, ha az elkobozható, illetve vagyonelkobzás alá esik, az tárgyi bizonyítási eszközként bír jelentőséggel, vagy a bizonyítás érdekében az abban tárolt, előre meg nem határozható vagy jelentős mennyiségű elektronikus adat átvizsgálására van szükség.

Ha ez az eljárás érdekét nem veszélyezteti, információs rendszer vagy adathordozó lefoglalása esetén az elektronikus adattal rendelkezni jogosult kérésére másolatot kell készíteni az általa megjelölt elektronikus adatról (Be. tv. 315. §).

A bitcoinok megőrzéséhez a lefoglaló hatóságnak készítenie kell egy tárcát és generálnia kell egy publikus kulcsot, amely címként működik. A lefoglalás során erre a címre továbbítják az összeget. Amikor a publikus kulcsot létrehozzák, akkor az megjelenik a blockchain-ben, ugyanúgy, mint ahogy a tranzakció is. A bitcoinok küldéséhez a tárcának csatlakoznia kell az internetre, de a fogadásához lehet a tárca offline állapotban is, mivel a tranzakciót a blockchain-ben rögzítik. A lefoglalt bitcoinok megőrzése során célszerű a kormány által ellenőrzött tárcákat elzártan, offline állapotban tárolni. Később, miután a lefoglalt bitcoinokról mentés készült, a hatóságnak érdemes törölnie saját tárcáját, ahova a bitcoinokat továbbították. A mentésből később minden információt importálni lehet a bitcoin kliensbe, és így bármikor hozzá lehet férni a lefoglalt bitcoinokhoz. A mentést CD-n vagy egy USB eszközön tárolva a hatósági eljárás végéig biztonságba kell helyezni.

A Be. tv. 308. § (3) bekezdés szerint lefoglalni az ingó dolgot, a számlapénzt, az elektronikus pénzt vagy az elektronikus adatot lehet. A kódex a zárolást is lehetővé teszi, ugyanis a 324. § (2) bekezdés b) pontja alapján zár alá vétel rendelhető el a

számlapénz mellett az elektronikus pénzre is. Azonban az elektronikus pénz és virtuális valuta nem azonos, és még csak nem is hasonló fogalmak. A Be. sokszor igencsak általános értelmű normáit a belügyminiszter irányítása alá tartozó nyomozó hatóságok nyomozásának részletes szabályairól és a nyomozási cselekmények jegyzőkönyv helyett más módon való rögzítésének szabályairól szóló 23/2003. BM-IM együttes rendelet (a továbbiakban: Nyor.) részletezte. A zár alá vétel és lefoglalás mikéntjét az új Nyor. határozhatja meg.

3.2. Elektronikus adat megőrzésére kötelezés. A bűncselekmény felderítése, illetve a bizonyítás érdekében elektronikus adat megőrzésére kötelezést lehet elrendelni. A bíróság, az ügyészség vagy a nyomozó hatóság rendeli el. Az elektronikus adat megőrzésére kötelezés az elektronikus adat birtokosának, feldolgozójának, illetve kezelőjének az elektronikus adat feletti rendelkezési jogát korlátozza.

Az elektronikus adat megőrzésére kötelezést akkor lehet elrendelni, ha az bizonyítási eszköz felderítéséhez, bizonyítási eszköz biztosításához, illetve a gyanúsított kilétének vagy tényleges tartózkodási helyének a megállapításához szükséges.

A megőrzésre kötelezett a határozat vele történő közlésének időpontjától köteles a határozatban megjelölt elektronikus adatot változatlanul megőrizni és – szükség esetén más adatállománytól elkülönítve – biztosítani annak biztonságos tárolását. A megőrzésre kötelezett köteles az elektronikus adat megváltoztatását, törlését, megsemmisülését, továbbítását, az elektronikus adatról másolat jogosulatlan készítését vagy az ahhoz való jogosulatlan hozzáférést megakadályozni.

Ha az elektronikus adat eredeti helyen történő megőrzése az érintettnek az elektronikus adat feldolgozásával, kezelésével, tárolásával vagy továbbításával kapcsolatos tevékenységét jelentősen akadályozná, az elrendelő engedélyével az elektronikus adat megőrzéséről annak más információs rendszerbe vagy adathordozóra történő átmásolásával gondoskodhat. Az átmásolást követően a megőrzésre kötelezést elrendelő az eredeti elektronikus adatot tartalmazó információs rendszerre vagy adathordozóra a korlátozásokat részlegesen vagy teljesen feloldhatja.

Ahhoz az elektronikus adathoz, amelyet a megőrzésre kötelezés érint, a kényszerintézkedés tartama alatt kizárólag a bíróság, az ügyészség vagy a nyomozó hatóság, valamint a megőrzésre kötelezést elrendelő engedélyével a megőrzésre kötelezett jogosult hozzáférni. Arról az elektronikus adatról, amelyet a megőrzésre kötelezés érint, a megőrzésre kötelezett az intézkedés tartama alatt csak az elrendelő engedélyével adhat más részére tájékoztatást.

A megőrzésre kötelezett köteles haladéktalanul tájékoztatni a megőrzésre kötelezést elrendelőt, ha a megőrzésre kötelezéssel érintett elektronikus adatot jogosulatlanul megváltoztatták, törölték, megsemmisítették, továbbították, átmásolták, megismerték, vagy ezek megkísérlésére utaló jelet észlelt.

Az elektronikus adat megőrzésére kötelezést követően a megőrzésre kötelezést elrendelő haladéktalanul megkezdi az elektronikus adatok átvizsgálását. Az átvizsgálás eredményeként a megőrzésre kötelezést elrendelő dönt a lefoglalás

végrehajtása más módjának az elrendeléséről vagy a megőrzésre kötelezést megszünteti.

A megőrzésre kötelezés legfeljebb három hónapig tart. A megőrzésre kötelezés megszűnik, ha a büntetőeljárást befejezték. A büntetőeljárás befejezéséről a megőrzésre kötelezettet tájékoztatni kell (Be. tv. 316. §).

3.3. Felhívás az elektronikus adat önkéntes eltávolítása érdekében. A Be. tv. lehetőséget biztosít az önkéntes eltávolításra az eljárás gyorsítása érdekében. Ha a büntetőeljárás érdekeit nem sérti, az ügyészség vagy a nyomozó hatóság az elektronikus adat ideiglenes hozzáférhetetlenné tételének elrendelését megelőzően felhívhatja az elektronikus adat önkéntes eltávolítása érdekében a sajtószabadságról és a médiatartalmak alapvető szabályairól szóló törvény szerinti azon médiatartalom-szolgáltatót, illetve azon tárhelyszolgáltatót vagy tárhelyszolgáltatást is végző közvetítő szolgáltatót, amelyik képes megakadályozni az elektronikus adathoz való hozzáférést (Be. tv. 338. §).

Az elektronikus adat ideiglenes hozzáférhetetlenné tételét a bíróság rendeli el. Az elektronikus adat ideiglenes hozzáférhetetlenné tétele az elektronikus hírközlő hálózat útján közzétett adat feletti rendelkezési jog ideiglenes korlátozása és az adathoz való hozzáférés ideiglenes megakadályozása. Akkor lehet elrendelni, ha az eljárás olyan közvádra üldözendő bűncselekmény miatt folyik, amellyel kapcsolatban elektronikus adat végleges hozzáférhetetlenné tételének van helye, és az a bűncselekmény megszakítása érdekében szükséges.

Az elektronikus adat ideiglenes hozzáférhetetlenné tétele elrendelhető az elektronikus adat ideiglenes eltávolításával, vagy az elektronikus adathoz való hozzáférés ideiglenes megakadályozásával. Az elektronikus adat ideiglenes hozzáférhetetlenné tételének teljesítésére kötelezett tájékoztatja a felhasználókat a tartalom eltávolításának vagy a tartalomhoz hozzáférés megakadályozásának a jogalapjáról. A tájékoztatás tartalmát külön jogszabály határozza meg. Az elektronikus adat ideiglenes eltávolítása és az elektronikus adat megőrzésére kötelezés együttesen is elrendelhető (Be. tv. 335. §).

3.4. Az elektronikus adat ideiglenes eltávolítása. Az elektronikus adat ideiglenes eltávolítására az érintett elektronikus adatot kezelő, az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvényben meghatározott tárhelyszolgáltatót, illetve tárhelyszolgáltatást is végző közvetítő szolgáltatót kell kötelezni. Az eltávolításra kötelezett a határozat vele történő közlését követő egy munkanapon belül köteles az elektronikus adat ideiglenes eltávolítására.

Az elektronikus adat ideiglenes eltávolításáról és az elektronikus adat visszaállításáról szóló határozatot az eltávolításra kötelezettel haladéktalanul közölni kell, amely a határozat vele történő közlésétől számított egy munkanapon belül köteles az elektronikus adat visszaállítására.

A bíróság hivatalból vagy az ügyészség indítványára az eltávolításra kötelezettet az elektronikus adat ideiglenes eltávolítására vagy visszaállítására vonatkozó kötelezettség elmulasztása miatt rendbírsággal sújthatja (Be. tv. 336. §).

3.5. Az elektronikus adathoz való hozzáférés ideiglenes megakadályozása. A kábítószer-kereskedelem, kóros szenvedélykeltés, kábítószer készítésének elősegítése, kábítószer-prekurzorral visszaélés, új pszichoaktív anyaggal visszaélés, gyermekpornográfia, állam elleni bűncselekmény, terrorcselekmény, terrorizmus finanszírozása vagy háborús uszítás miatt folyamatban lévő büntetőeljárásban a bíróság elrendeli a felsorolt bűncselekménnyel összefüggő elektronikus adathoz való hozzáférés ideiglenes megakadályozását. Erre akkor kerül sor, ha az eltávolításra kötelezett az elektronikus adat ideiglenes eltávolítására vonatkozó kötelezettséget nem teljesítette, az elektronikus adat ideiglenes eltávolítására vonatkozóan a külföldi hatóság jogsegély iránti megkeresése a megkeresés bíróság általi kibocsátásától számított harminc napon belül nem vezetett eredményre, az eltávolításra kötelezett azonosítása lehetetlen vagy aránytalan nehézséggel járna, vagy az elektronikus adat ideiglenes eltávolítására vonatkozóan a külföldi hatóság jogsegély iránti megkeresésétől eredmény nem várható vagy a megkeresés aránytalan nehézséggel járna.

A bíróság a határozatával az elektronikus hírközlési szolgáltatókat kötelezi az elektronikus adathoz való hozzáférés ideiglenes megakadályozására.

A bíróság az elektronikus adathoz való hozzáférés ideiglenes megakadályozásának elrendelését haladéktalanul közli a Nemzeti Média- és Hírközlési Hatósággal (a továbbiakban: NMHH), amely a kényszerintézkedés végrehajtását szervezi és ellenőrzi.

Az NMHH az elektronikus adathoz való hozzáférés ideiglenes megakadályozására vonatkozó kötelezettséget bevezeti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisába, ezzel egyidejűleg a bíróság határozatáról elektronikus úton haladéktalanul tájékoztatja az elektronikus hírközlési szolgáltatókat, amelyek a tájékoztatástól számított egy munkanapon belül kötelesek az elektronikus adathoz való hozzáférés ideiglenes megakadályozására. Ha valamely elektronikus hírközlési szolgáltató a kötelezettséget nem teljesíti, az NMHH erről haladéktalanul tájékoztatja a bíróságot.

Az elektronikus adathoz való hozzáférés ideiglenes megakadályozása a büntetőeljárás jogerős befejezésével megszűnik (Be. tv. 337. §).

4. Az elektronikus adat végleges hozzáférhetetlenné tétele

Immár szankcióként is szerepel a Büntető Törvénykönyvben az elektronikus hírközlő hálózaton közzétett adatoknak a végleges hozzáférhetetlenné tétele. A magyar törvényi szabályozás a 2011/93/EU irányelv 25. cikkének tesz eleget, amikor ezt az új büntetőjogi szankciót bevezeti.

Az Európai Parlament és Tanács irányelvében határozta meg a teendőket a gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalak ellen.[4] Az interneten

[4] 2011. december 13-i 2011/93/EU IRÁNYELVE a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi

megvalósítható bűncselekményeket igyekszik megelőzni, illetve a tiltott adattartalomhoz való hozzáférést igyekszik megakadályozni. Ilyen adatok például a tiltott pornográf felvételek. Ezen adatok végleges hozzáférhetetlenné tétele megakadályozhatja a bűncselekmény, bűncselekmények továbbélését a net világában. A bíróság Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése (Btk. 385. §), illetve Gyermekpornográfia (Btk. 204. §) elkövetése esetén alkalmazza az új szankciót.

Ez a fajta büntetőjogi szankció az elkobzáshoz hasonlatos, amely intézkedést – többek között - annak a dolognak az esetében kell alkalmazni, amely bűncselekmény elkövetése útján jött létre.

Azzal szemben is alkalmazható, aki büntetőjogilag nem vonható felelősségre (gyermekkor, kóros elmeállapot miatt). Míg büntetés csak azzal az elkövetővel szemben szabható ki, aki büntethető, azaz büntetőeljárásban büntetőjogi felelősségre vonható, addig egyes intézkedéseknek nem feltétele, hogy akivel szemben alkalmazzák, büntethető is legyen.

Kötelező a véglegesen hozzáférhetetlenné tétel, amikor az elektronikus hírközlő hálózaton közzétett adat hozzáférhetővé tétele vagy közzététele bűncselekményt valósít meg, amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy amely bűncselekmény elkövetése útján jött létre. Amennyiben internetes tartalom útján valósul meg a rágalmazás (Btk. 226. §), illetve a becsületsértés (Btk. 227. §), akkor is kötelező.

5. Európai, nemzetközi lépések

Európában létrejött az e-igazságügyi portál, amely elektronikus ügyfélkapuként kíván működni az igazságügy területén és azt a célt szolgálja, hogy EU-szerte megkönnyítse az igazságügyi rendszerekkel kapcsolatos információkeresést és az igazságszolgáltatáshoz való hozzáférést.[5]

„Egységes digitális kapu" kialakítását is elhatározták, amely biztosítja a hozzáférést az információkhoz, eljárásokhoz, valamint segítségnyújtó és problémamegoldó szolgáltatásokhoz az Európai Unió tagállamai számára.[6]

Európában hozták létre az E-CODEX-et, az internetes adatcserén alapuló e-igazságügyi kommunikációt. Célja a határokon átnyúló igazságügyi együttműködés elősegítése, jellemzője, hogy a jog és az informatika határán helyezkedik el. A

kerethatározat felváltásáról 25. cikk Eszerint a tagállamok megteszik a szükséges intézkedéseket a gyermekpornográfiát tartalmazó vagy azt terjesztő, a területükön üzemeltetett weboldalak azonnali eltávolításának biztosítására, valamint törekednek a területükön kívül üzemeltetett hasonló weboldalak eltávolítására. A tagállamok intézkedéseket tehetnek a gyermekpornográfiát tartalmazó vagy azt terjesztő, a területükön található internetfelhasználókat célzó weboldalakhoz való hozzáférés meggátolására. Ezen intézkedéseket eljárások keretében kell meghatározni, és megfelelő biztosítékokat kell nyújtaniuk, különösen annak biztosítása érdekében, hogy a korlátozás arra korlátozódjon, ami szükséges és arányos, valamint, hogy a felhasználókat tájékoztassák a korlátozás okáról.

[5] https://e-justice.europa.eu/home.do , 2019. október 1.

[6] Az Európai Parlament és a Tanács (EU) 2018/1724 rendelete (2018. október 2.)

projektben az azonosításra, elektronikus kézbesítésre, elektronikus formanyomtatványokra vonatkozó informatikai jellegű alcsoportok mellett a jogi alcsoport is kiemelkedő szerepet tölt be az e-law európai tanácsi munka során.[7]

Az Európai Unió Bizottsága közleményt adott ki a mesterséges intelligenciával (MI) kapcsolatos együttműködésről. 2018 áprilisában Norvégia és a tagállamok együttműködési nyilatkozatot írtak alá a Digitális Napon. Közös fellépést szorgalmaztak az MI kutatása, alkalmazása és jogi szabályozása területén. A tagállamok feladatul kapták, hogy alakítsanak ki saját nemzeti stratégiát a mesterséges intelligenciával kapcsolatosan 2019-ben.[8]

Az Europol, az Eurojust és az EJN (Európai Igazságügyi Hálózat)[9] közös projektje a SIRIUS[10], amely az elektronikus bizonyítékok határokon átnyúló hozzáférését hivatott elősegíteni. Ladislav Hamran[11] az Eurojust elnöke javaslatot terjesztett elő a digitális büntető igazságszolgáltatásra vonatkozóan, indoklása szerint a határokon átnyúló bűncselekmények felderítése, bizonyítása akkor lehetséges, ha az európai rendészeti szervek is lépést tartanak a digitalizációval. Európa biztonságosabbá tétele érdekében az Európai Unió az elmúlt években határozott lépéseket tett a bűnüldöző szervek, a határőrök és a migrációs tisztviselők által használt információs rendszerek korszerűsítésére. Ennek következtében lehetőség nyílt a bűnüldözés szempontjából fontos információk azonnali cseréjére. Az új rendszerek képesek lesznek „beszélni" egymással, egyúttal biztonságosak lesznek, számos garancia van beépítve a rendszerbe, amely megakadályozza, hogy illetéktelenek férjenek hozzá az elektronikus bűnügyi adatokhoz.

2019-ben az Európa Tanács tárgyalásokat kezdeményezett az Amerikai Egyesült Államokkal az elektronikus bizonyítékok határokon átnyúló hozzáféréséről.[12]

Emailek, szöveges üzenetek, fényképek, videók, előfizetői adatok, online fiókok adatai minősülhetnek elektronikus bizonyítékoknak, ezek azonban akár az elkövető, akár a sértett tartózkodási helyétől távol levő szervereken lehetnek. Emiatt kell megoldást találni az elektronikus bizonyítékokhoz való gyors és hatékony hozzáférés tekintetében. Ez az egyedüli módja mind az EU-n belül, mind nemzetközi szinten a terrorizmus és a szervezett bűnözés elleni hatékony küzdelemnek. Cél az elektronikus bizonyítékok megszerzési folyamatának gyorsítása, illetve az elektronikus bizonyítékokhoz való hozzáférés kapcsán a jelenleg még fennálló nyomozási akadályok elhárítása.[13]

A mesterséges intelligenciának is nagy szerepe lehet a büntető igazságszolgáltatásban, bűnüldözésben, bűnmegelőzésben. A Predpol az open data

---

[7] e-CODEX (e-Justice Communication via Online Data Exchange) https://www.e-codex.eu/about , 2019. október 2.

[8] „A mesterséges intelligenciáról szóló összehangolt terv" 2018. december 7.

[9] European Judicial Network

[10] http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx , 2019. október 2.

[11] Eurojust's Annual Report 2018 Combatting crime and terrorism via digital justice Brussels, 2 April 2019 http://eurojust.europa.eu/press/PressReleases/Pages/2019/2019-04-02.aspx , 2019. október 3.

[12] Brussels, 5.2.2019 COM(2019) 70 final

[13] https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf, 2019. október 3.

és a mesterséges intelligencia használatával képes megjósolni, hogy mikor és hol kerül sor bűncselekményre. A múltbeli bűncselekményekre vonatkozó meglévő adatok elemzésével jelzik előre a várható bűnözést. Az USÁ-ban már több városban működik a Predpol-rendszer. Los Angelesben próbálták ki először és az algoritmus mintákat dolgozott ki a „hotspotok" azonosítására, ahol meghatározott bűncselekmények várhatók a jövőben. Durhamban (Egyesült Királyság) szintén ezt a módszert használják a bűnmegelőzésre. A Harm Assessment Risk Tool (Hart) program öt éves bűnügyi adatok alapján jósolja meg, hogy a bűnelkövetők milyen szintű kockázatot jelentenek.[14]

A mesterséges intelligencia és a robotika volt a fő kérdésköre az UNICRI Mesterséges Intelligencia Központja és az Interpol ülésének is.[15] A rendőrségek számára rendelkezésre álló digitális lehetőségekről, egyúttal a kockázatokról is szóltak, hangsúlyozva, hogy a mesterséges intelligencia és a robotika használata nem jövőbeli lehetőség, hanem a jelen valósága.[16]

6. Összegző gondolatok

A bűnüldözés során az informatika speciális terület, melyhez külön szakértelem szükséges. A bűnüldözők hiányzó ismereteit nem mindig lehet szakértő igénybevételével pótolni, hiszen már az adatgyűjtés folyamatában, illetve az összes nyomozati cselekmény során szakszerűen kell eljárni. Az informatikai jártasságban való elmaradás különösen az idősebb generációk esetében jellemző, orvosolandó hiányosság. A bűncselekmények jelentős része megvalósítható a kibertérben is. Az internet egyrészt új bűncselekmények megjelenését hozta el, másrészt a már létező bűncselekmények leltek általa új helyszínre.[17] Kérdésként merül fel, hogy miként reagáljon a törvényalkotó a kiberbűnözésre. Elegendő, ha a Büntető Törvénykönyvben külön nevesítve vannak a közvetlenül a cybercrime körébe tartozó cselekmények (pl. a Btk. XLIII. fejezetében szereplő tiltott adatszerzés és információs rendszer elleni bűncselekmények), a hagyományos bűncselekmények (pl. a kiskorúval való kapcsolattartás akadályozása) és azok, amelyek a hagyományos világban és a virtuális térben egyaránt megvalósíthatóak (pl. zsarolás, rágalmazás, zaklatás)? Szükséges-e a büntetőjogban a proaktív hozzáállás? Megvalósítható-e egyáltalán az alkotmányos alapelvek megtartásával a jövőben keletkező káros magatartások előzetes védelme?

[14] https://www.europeandataportal.eu/en/highlights/ai-and-open-data-crucial-combination, 2019. október 5.
[15] Hága, 2019. március 21.
[16] http://www.unicri.it/news/article/Centre_Artificial_Intelligence_Robotics , 2019. október 3.
[17] Ld. részletesen Nagy Zoltán András: *Bűncselekmények számítógépes környezetben*, Budapest, Ad librum, 2009.