



# Viktimizáció az online térben Egy nemzetközi kutatás eredményei hazai szemszögből<sup>1</sup>

Victimization in cyberspace – results of a cross-country analysis  
from domestic perspective

---

**Barabás A. Tünde**

Prof. Dr. CSc, igazgató, főtanácsos, tanszékvezető egyetemi tanár  
Országos Kriminológiai Intézet,  
Nemzeti Közszolgálati Egyetem,  
Rendészettudományi Kar  
barabas@okri.hu



**Koplányi Gergely**

statisztikus  
Országos Kriminológiai Intézet  
koplanyi@okri.hu

---

## Absztrakt

**Cél:** Jelen kutatásban három országban (Magyarország, Finnország és az Egyesült Államok) vizsgálták a szerzők a kiberbűncselekmények elkövetéseinek és az áldozattá válásnak a mintázatait.

**Módszertan:** A kutatói team által kidolgozott online kérdőív 2020 áprilisában került felvételre a három országban, a *Qualtrics* kérdőívező rendszer segítségével, reprezentatív mintán. Az adatok elemzése SPSS programcsomaggal történt. A gyakoriságok elemzéséhez khi-négyzet próbát és Fisher-próbát, a középértékek összehasonlításához Mann–Whitney-próbát alkalmaztak. Az egyes áldozattá válási módokra regressziós modellek kerültek felállításra (Bináris Logisztikus Regresszió).

**Megállapítások:** A kutatás eredményei azt mutatják, hogy a technikai eszközök használatának elterjedtségében jóval előrébb tartó Egyesült Államok esetében az online bűncselekmények és az áldozatok száma is szignifikánsan magasabb, mint a két európai országban. A férfiak mindhárom országban nagyobb mértékű online aktivitásról és gyakoribb áldozattá válásról számoltak be a nőkhez képest. Hazánkban számos deliktum esetében a legalacsonyabb mutatók találhatók, hasonló tendenciákat mutatva a finn eredményekkel. Szignifikáns eltérés találtott

---

<sup>1</sup> A nemzetközi kutatói team tagjai Parti Katalin, Thomas Dearden, James Hawdon, Pekka Räsänen, Aki Koivula, Kiss Tibor és Szigeti Akos, akiknek kutatómunkája nélkülözhetetlen volt a cikk elkészüléséhez.

országok szerint az áldozattá válás gyakoriságában is. A magyar mintában az online áldozattá válás nagyobb gyakorisága figyelhető meg az offline cselekményekhez képest. A tanulmány vizsgálja az egyes hagyományos magyarázóelméletek helytállóságát, amelyek között a kontrollelméletek, valamint a rutintevékenység-elmélet kínál magyarázatot ezen a speciálisnak tekinthető, új bűnözési felületen.

**Érték:** A kutatás egy új, eddig kevésbé feltárt területen zajló egyes bűnözési formák sajátosságait vizsgálja és hasonlítja össze a hasonló jellegű offline jogsértésekkel, magyarázatot keresve és ezzel lehetőséget kínálva az új típusú bűncselekmények megelőzési stratégiájának kidolgozásához.

**Kulcsszavak:** kiberbűnözés, viktimizáció, elkövető, magyarázó elméletek

## Abstract

**Aim:** In this research, the Authors examined the patterns of cybercrime perpetration and victimization in three countries (Hungary, Finland, and the United States).

**Methodology:** The online questionnaire developed by the research team was taken in April 2020 in the three countries, with the help of the Qualtrics questionnaire system, on a representative sample. The data were analyzed using the SPSS program package. Chi-square test and Fisher test were used to analyze the frequencies, and Mann–Whitney test was used to compare the mean values. Regression models were set up for each type of victimization (Binary Logistic Regression).

**Findings:** The results of the research show that in the case of the United States, which is far ahead in the prevalence of the use of technical devices, the number of online crimes and victims is significantly higher than in the two European countries. In all three countries, men reported higher levels of online activity and more frequent victimization compared to women. In the case of many delicts, the lowest indicators can be found in our country, showing similar trends to the Finnish results. Authors also found a significant difference in the frequency of victimization by country. In the Hungarian sample, a higher frequency of online victimization can be observed compared to offline acts. The study examines the appropriateness of some traditional explanatory theories, among which the control theories and the routine activity theory offer an explanation on this new special crime surface.

**Value:** The research examines and compares the characteristics of certain forms of crime in a new, under-explored area with similar types of offline offences, seeking explanations and thus offering an opportunity to develop a strategy for the prevention of new types of crime.

**Keywords:** cybercrime, victimization, offender, crime theories

## Bevezetés

A 21. században egyre nagyobb szerepet kapnak életünkben az online térben zajló társas interakciók, folyamatosan növekszik az itt eltöltött idő. A 2020-as COVID–19-járvánnyal ez a folyamat felerősödött, a személyes és szakmai élet is egyre inkább a virtuális térbe tevődött át. Ezzel párhuzamosan az online bűncselekmények és így az áldozatok száma is folyamatosan növekszik ([URL1](#)); mi több, a virtuális térben elkövetett átverések és adatlopások egyre változatosabb formái alakulnak ki.

A kiberbűnözés vizsgálata az elmúlt három évtizedben egyre nagyobb teret nyert kriminológiai szempontból is ([Varga, 2021](#)).

A kutatás egy nemzetközi összehasonlító vizsgálat az online és offline áldozattá válás és egyes kiberbűncselekmények elkövetésének témakörében.<sup>2</sup> Hipotézisünk szerint, amennyiben érthetőbbé válnak a kiberbűncselekmények elkövetőinek motivációi, a deviáns viselkedésüket alakító tényezők, az online térben elkövetett bűncselekmények számának növekedő tendenciája is megfordítható.

## Elméleti keret

A bűncselekmények és a bizonytalanságérzet csökkentését célzó stratégiák egyik legfontosabb kérdése, hogy kik válnak áldozattá, vannak-e meghatározható demográfiai és szociokulturális jellemzőik. Eltérően alakul a viktimizáció az egyes bűncselekménytípusok szerint is.

Egy adott társadalomban élők bizonytalanságérzete megragadható makrotársadalmi, antropológiai szempontból, és személyes, demográfiai tényezők mentén is. A személyes tényezők viszonylatában egyes kutatások hangsúlyozzák a fiatalok gyakoribb viktimizációját, mivel többször járnak el otthonról és találkoznak idegenekkel. A kisgyermekes családok tagjai kisebb valószínűséggel lesznek áldozatok (különösen vagyoni elleni cselekmények esetében), mert több időt tartózkodnak az otthonukban ([Kerecsi, 2005](#)). Egyes elméletek szerint a nők a hivatalos statisztikai adatokhoz képest jóval gyakrabban válnak áldozattá, azonban ezt félelemből, szégyenérzetük miatt, vagy kiszolgáltatott helyzetükből adódóan nem jelentik a hatóságoknak. Különösen igaz ez a szexuális, valamint a családon belüli sérelmek esetében ([Virág, 2005](#)).

---

2 A kutatás a Jean Monnet Center of Excellence, Collage Center for European Union, Transatlantic, and Trans-European Space Studies (CEUTTSS) támogatásával valósult meg, a Virginia Tech College of Liberal Arts and Human Sciences (CLAHS), a University of Turku Faculty of Social Sciences, valamint a Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Kriminológia Tanszéke részvételével.

A látenciakutatások eredményein alapul az a megállapítás, hogy általánosságban is többen válnak áldozattá, mint az a hatóságok számára ismertté válik, azonban különböző okokból; így a hatóságokkal szembeni bizalmatlanság vagy a félelem, vagy éppenséggel a sérelem csekély volta miatt nem jelentik azt (Barabás, 2004; 2015). A sértetté válás mértéke eltérően alakul a vidék és a városi környezet vonatkozásában, és akár egy városban, különböző körzeteken belül is (Barabás, 2018).

Mindehhez képest az online tér a bűncselekmények elkövetésének és elszívésének olyan, a korábban megismertekhez képest speciális területe, amely működéséből adódóan – de feltételezhetően más okokból (is) – szerepet játszik abban, ki válik elkövetővé vagy áldozattá, miközben az alap bűnözésmagyarázó elméletek is igaznak bizonyulnak. Jelen kutatásban hat szociológiai elmélet magyarázóerejét vizsgáltuk egyes kiberbűncselekmények elszívésére/elkövetésére vonatkozóan, amelyek a következők:

- az önkontroll szerepe – általános bűnözésemélet (General Theory of Crime) (Gottfredson & Hirschi, 1990);
- a rutintevékenység-elmélet (Routine Activities Theory, RAT) (Cohen & Felson, 1979);
- az általános feszültségelmélet (General Strain Theory) (Agnew, 1992);
- az intézményi anomiaelmélet (Institutional Anomie Theory) (Messner & Rosenfeld, 1994);
- a differenciális asszociációs elmélet (Differential Association Theory) (Sutherland, 1937; 1947); valamint
- a szociális tanuláselméleti modell (Social Learning) (Akers, 1998).

Tekintettel arra, hogy mind a jelenlegi, mind pedig a korábbi kutatások elsősorban a rutintevékenység-, valamint az önkontroll-elmélet magyarázóelvéivel találtak jelentősebb összefüggést a kiberbűncselekmények esetében, ezért a következőkben az adatok elemzése során erre a két elméletre támaszkodunk.

A rutintevékenység-elmélet alapfeltevése az, hogy a bűncselekmény bekövetkezéséhez térben és időben egy motivált elkövetőnek, egy megfelelő célpontnak és egy alkalmas védelem hiányának kell egybeesnie (Cohen & Felson, 1979). A motivált elkövető jelenléte általában adott, akár offline, akár online térről van szó. A célpont megfelelősége és az alkalmas védelem szerepe és jelenléte az online környezetben azonban a hagyományos bűnözéshez képest némileg módosított megközelítést igényel (Näsi, Danielsson & Kaakinen, 2023). A kutatás során fontos szempontként vettük figyelembe ezért azt, hogy mennyi időt tölt a válaszadó online felület előtt (mennyire tekinthető internet- vagy éppenséggel játékfüggőnek, vagy a közösségimédia-felületek túlzott használójának). Emellett vizsgáltuk azt is, vajon a kérdezett milyen PC-ismeretekkel

rendelkezik, feltételezve, hogy a kevésbé tapasztalt felhasználó alkalmasabb célpontot jelent a bűnelkövetők számára. Továbbá, hogy alkalmaz-e olyan biztonsági eszközöket, mint a tűzfal, illetve megfelelő vírusirtó használata, vagy akár a webkamera lefedése.

Az online aktivitáson és rutinokon túl kevés tanulmány vizsgálta az önkontroll és a kiberviktimizáció közötti összefüggést. Whitty (2019) tanulmánya szerint az online rutinok mellett az impulzivitás, valamint a szenzációkereső és addiktív viselkedés skáláján magas pontszámot elérő személyeknél (az idősebb életkorral együtt) magasabb a csalás miatt áldozattá válás kockázata. Bossler és Holt (2010), valamint Reyns és Fisher (2018) tanulmányai gyenge kapcsolatot találtak az alacsony önkontroll és a kiberviktimizáció között, bár Holt és Bossler tanulmánya (2008) kapcsolatot talált az alacsony önkontroll és a rosszindulatú szoftverek áldozattá válása között, van Wilsem (2011) pedig hasonló összefüggést talált az online hackelés és zaklatás áldozattá válása tekintetében (összegzi Nási et al., 2023).

## Módszertan

### *A kutatási minta*

Az online térben történő áldozattá válással és elkövetéssel kapcsolatos kérdőív 2020 áprilisában három országban; az Egyesült Államokban, Magyarországon és Finnországban került felvételre, a *Qualtrics* kérdőívező rendszer segítségével, reprezentatív mintán. A hiányos esetek kiszűrése után 4212 fő került a mintába. Az 1. számú táblázat a minta nemek és országok szerinti megoszlását ábrázolja.

### 1. számú táblázat

*Nemi megoszlás országok szerint*

Ország	A kérdezett neme			Összesen
	nő	férfi	egyéb / nem válaszolt	
Egyesült Államok	691	686	24	1401
	49,3%	49,0%	1,7%	100%
Finnország	732	627	31	1390
	52,7%	45,1%	2,2%	100%
Magyarország	708	688	25	1421
	49,8%	48,4%	1,8%	100%
Összesen	2131	2001	80	4212
	50,6%	47,5%	1,9%	100%

*Forrás:* A szerzők saját szerkesztése.

## Eredmények

### *Online és offline áldozattá válás – nemek szerinti eltérés*

Az áldozattá válási blokkban a kérdést megelőző 12 hónapra vonatkozóan kérdeztük meg a résztvevőket arról, hogy áldozattá váltak-e különféle online átverésekben és cselekményekben (e-mail csalások, adatokkal visszaélés, ismeretlen számlatranzakciók, számítógépes vírusok, kéretlen online hozzászólások), illetve nem a kibertérben elkövetett cselekményekben (igazolvány, bankkártya ellopása, kéretlen személyes hozzászólások, személyes tulajdon rongálása). A 2. számú táblázat a fentiek közül bármilyen módon (legalább egyszer) áldozattá váltak nemek szerinti megoszlását tartalmazza.

### **2. számú táblázat**

*Online és offline áldozattá válás nemek szerint*

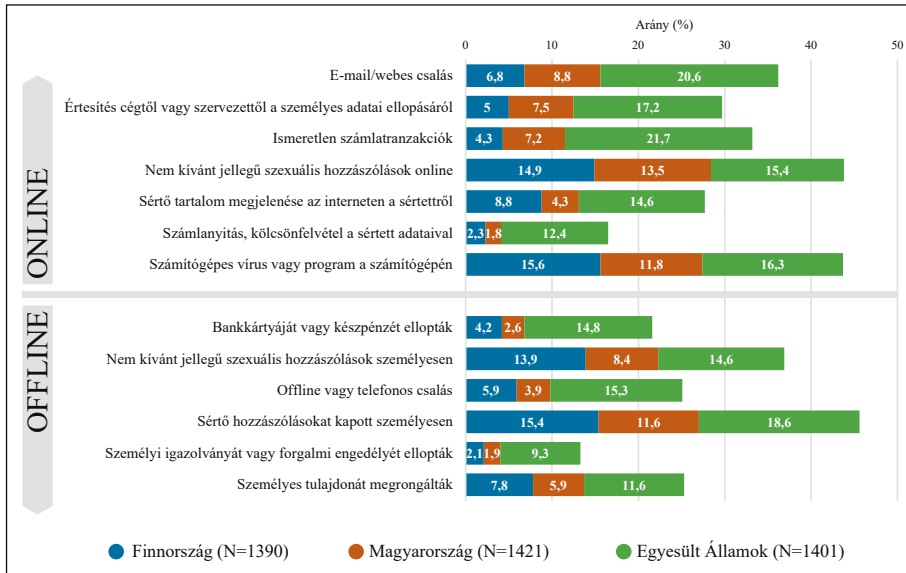
	Nem vált áldozattá	Áldozattá vált	Nem válaszolt	Összesen
<b>Online áldozattá válás</b>				
Nő	1371	698	62	2131
	<b>64,30%</b>	<b>32,80%</b>	<b>2,90%</b>	<b>100%</b>
Férfi	1198	734	69	2001
	<b>59,90%</b>	<b>36,70%</b>	<b>3,40%</b>	<b>100%</b>
Összesen	2569	1432	131	4132
	<b>62,20%</b>	<b>34,70%</b>	<b>3,20%</b>	<b>100%</b>
<b>Offline áldozattá válás</b>				
Nő	1488	583	60	2131
	<b>69,80%</b>	<b>27,40%</b>	<b>2,80%</b>	<b>100%</b>
Férfi	1432	513	56	2001
	<b>71,60%</b>	<b>25,60%</b>	<b>2,80%</b>	<b>100%</b>
Összesen	2920	1096	116	4132
	<b>70,70%</b>	<b>26,50%</b>	<b>2,80%</b>	<b>100%</b>

*Forrás:* A szerzők saját szerkesztése.

Az online áldozattá válás esetében a nemek közötti eltérés szignifikáns a khinégyszet próba alapján ( $\chi^2=7,873$ ;  $p<0,01$ ), a férfiak a nőkhöz képest szignifikánsan gyakrabban váltak áldozattá az online cselekmények esetében.

## 1. számú ábra

Online és offline áldozatok aránya országok szerinti bontásban



Forrás: A szerzők saját szerkesztése.

Az online és offline áldozattá válási gyakoriságokat országonkénti bontásban vizsgálva azt találjuk, hogy minden cselekményforma szignifikánsan gyakrabban fordult elő az Egyesült Államokban a khi-négyzet próba alapján ( $p < 0,01$ ), a „Nem kívánt jellegű szexuális hozzászólások online” kivételével, ahol nem volt számottevő különbség az országok szerint.

### Áldozattá válás a magyar mintában

A kutatás magyar résztvevőivel kapcsolatban tehát megállapítható, hogy mindegyik cselekmény esetében kevesebb az online és offline áldozattá válások aránya az amerikai mintához képest. A magyar mintában az online áldozattá válás nagyobb gyakorisága figyelhető meg az offline cselekményekhez képest (30,7–21%). Ez összefüggésben lehet azzal, hogy maga a kérdezés a COVID–19-járványt követően zajlott, és az előző év eseményeire kérdezett rá.

Az online áldozattá válási formák közül a leggyakoribb cselekmény a nem kívánt jellegű szexuális hozzászólás (13,5%), ezt követi a számítógépes vírus vagy program (11,8%) és az e-mail, webes csalások (8,8%). A magyar résztvevők körében az offline áldozattá válás formái közül a személyes sértő hozzászólások

fordultak elő legnagyobb arányban (11,6%), valamint a személyes jellegű nem kívánt szexuális hozzászólások (8,4), és a tulajdon megrongálása (5,9%).

### 3. számú táblázat

Magyar áldozatok nemi és életkori megoszlásában

Áldozattá válás a magyar mintán	Áldozat neme			Áldozat kora			
	Nő (%)	Férfi (%)	p.	18–25 éves (%)	26–59 éves (%)	60+ éves (%)	p.
<b>Online cselekmények</b>							
E-mail/webes csalás	7,6	10,1	N.S.	7,8	7,2	12,6	<0,01
Számlanyitás, kölcsönfelvétel a sértett adataival	1,6	2,2	N.S.	1,4	2,0	1,9	N.S.
Ismeretlen számlatranzakciók	5,6	9,1	<0,05	4,3	6,7	10,2	<0,05
Értesítés cégtől vagy szervezettől a személyes adatai ellopásáról	4,6	11,0	<0,01	4,3	7,3	9,7	N.S.
Sértő tartalom megjelenése az interneten a sértettől	4,5	4,2	N.S.	7,1	4,0	4,3	N.S.
Nem kívánt jellegű szexuális hozzászólások online	13,1	14,9	N.S.	17,9	13,0	14,8	N.S.
Számítógépes vírus vagy program a számítógépén	10,5	13,8	<0,1	9,9	11,9	14,1	N.S.
<b>Offline cselekmények</b>							
Offline vagy telefonos csalás	2,9	5,1	<0,05	4,3	3,9	4,0	N.S.
Személyigazolványát vagy forgalmi engedélyét ellopták	2,2	1,8	N.S.	2,9	2,3	1,1	N.S.
Bankkártyáját vagy készpénzét ellopták	2,2	3,0	N.S.	4,3	3,1	1,3	N.S.
Sértő hozzászólásokat kapott személyesen	12,1	12,1	N.S.	21,6	11,7	9,2	<0,05
Nem kívánt jellegű szexuális hozzászólások személyesen	10,3	7,0	<0,05	17,9	7,9	7,0	<0,05
Személyes tulajdonát megrongálták	5,2	6,9	N.S.	5,0	8,1	2,2	<0,05
Statisztikai próba	Fisher-próba			Khi-négyzet próba			

*Forrás:* A szerzők saját szerkesztése.

Szignifikáns eltérések tapasztalhatóak a magyar válaszadók körében az egyes online és offline áldozattá válási módok esetében, az áldozat neme és életkora szerint is. Az eredményeket a fenti, 3. számú táblázat foglalja össze.

Az ismeretlen számlatranzakciók szignifikánsan nagyobb arányban fordultak elő az időskorú férfiak esetében, a férfiak továbbá gyakrabban estek áldozatul álcéges, álszolgáltató általi személyes adatlopási kísérletnek a nőkhöz képest. Az e-mail/webes csalások áldozatai között nagyobb arányban voltak az időskorúak (60 éves vagy idősebb). Az offline cselekmények esetében elmondható,



hogy az offline, vagy telefonos csalás áldozatai nagyobb arányban férfiak, míg a nem kívánt jellegű személyes szexuális hozzászólások áldozatai nagyobb arányban nők. Ezen két cselekmény esetében a fiatal felnőtt korosztály a legveszélyeztetettebb. A személyes tulajdon megrongálása a felnőtt (26–59 éves) korcsoportot szignifikánsan nagyobb mértékben érintette a fiatal felnőtt és idős korcsoporthoz képest a magyar mintában.

A férfiaknál azért is lehet nagyobb a kitettség az online csalásoknak és adatlopásnak, mivel átlagosan több időt töltenek különböző tevékenységekkel az interneten.

A nők és férfiak heti online tevékenységekkel töltött idejét összehasonlítva a Mann–Whitney-próbával azt találtuk, hogy a férfiak a nőkhöz képest szignifikánsan több időt töltenek számítógépezéssel munkaidőben (U: 1907470,000;  $p < 0,01$ ), online hír- vagy cikkolvasással (U: 1744723,500;  $p < 0,01$ ), online videójátékokkal (U: 1717885,000;  $p < 0,01$ ), egyéb online tevékenységekkel (U: 1758308,500;  $p < 0,01$ ) és online tevékenységekkel összesen (U: 1847341,000;  $p < 0,01$ ). A nők szignifikánsan többet böngészik a közösségi médiát (U: 1804164,000;  $p < 0,01$ ), az online vásárlásra fordított idő esetében viszont nincs szignifikáns különbség a nemek között. A nagyobb mértékű online aktivitás „alkalmas célponttá” teszi a férfiakat a rutintevékenység-elmélet megközelítésében.

Az online aktivitással töltött idő mellett a csalások és egyéb kibercselekmények megelőzésére szolgáló biztonsági intézkedések alkalmazását is vizsgáltuk (4. számú táblázat), feltételezve, hogy ha a férfiak kevésbé tesznek erre irányuló intézkedéseket, az tovább növeli a kibercselekményeknek való kitettségüket.

#### 4. számú táblázat

*Biztonsági intézkedések használata nemek szerint*

Biztonsági intézkedések	Jelenleg alkalmazza		Korábbi áldozattá válás miatt alkalmazza	
	Férfiak	Nők	Férfiak	Nők
Eltakarja a webkamerát a számítógépén, laptopján	36,58%	37,31%	2,55%	1,78%
Személyazonossága ellopását monitorozó megoldást használ	25,19%	22,24%	2,80%	2,86%
Befagyasztja bankkártyáját, amikor nem tervezi használni	15,04%	14,41%	5,20%	4,18%
Vírusirtó programot vagy tűzfalat használ számítógépén	74,21%	69,92%	3,85%	3,14%

*Forrás:* A szerzők saját szerkesztése.

A személyazonosság ellopását monitorozó megoldást, valamint vírusirtó programot vagy tűzfalat szignifikánsan gyakrabban használnak (jelenleg alkalmazásban) a férfiak a nőkhez képest a khi-négyzet próba alapján ( $\chi^2=4,952$ ;  $p<0,01$ ,  $\chi^2=9,432$ ;  $p<0,01$ ). A webkamera eltakarása és bankkártya befagyasztása esetében nem találunk jelentős különbséget a nemek között. A férfiak így részben elővigyázatosabbak, másrészt ezek az intézkedések csak bizonyos családok, átvérések és egyéb kiberbűncselekmények ellen jelentenek védelmet.

A rutintevékenységek-elmélet feltételezi, hogy az elkövetés további feltétele az alkalmas célpont megléte. Előzetes várakozásaink alapján a kibertérben elkövetett cselekmények esetében az alacsonyabb szintű számítógépes készségek, valamint az önkontroll alacsony szintje növelhetik az áldozattá válás kockázatát.

Munkánk során az egyes áldozattá válási módokra regressziós modelleket állítottunk fel (bináris logisztikus regresszió, Forward LR method). Ennek során a nem (1: férfi, 0: nő) és életkor, az online töltött idő (órában) mellett a számítógépes ismeretek (1–5-ig terjedő ordinális változó) és az önkontroll (öt, egytől háromig terjedő itemből álló index-változó) hatását mértük az egyes cselekmények szerinti áldozattá válásra.

Az eredmények azt mutatták, hogy az összes cselekmény esetében az önkontroll mértéke gyakorolta a legnagyobb hatást az áldozattá válásra. Az alacsonyabb önkontrollal rendelkező személyek nagyobb valószínűséggel esnek áldozatul a különböző e-mailes, webes csalásoknak, adatlopási kísérleteknek, számítógépes vírusoknak. Az online töltött idő hatása több csalás esetében szignifikáns, de alacsony mértékű ( $\beta$ : 0,004–0,006). Az alacsonyabb szintű számítógépes ismeretek valószínűsíthetik az e-mail vagy webes felületen történő áldozattá válást ( $\beta$ : -0,123), valamint a bankszámlán, online fizetési rendszeren tapasztalt ismeretlen tranzakciókat ( $\beta$ : -0,103). Egyes online csalástípusok viszont – távoli elérés, webes adatlopás – viszont a számítógéphez jobban értők körében jellemzőek.

A sértő tartalom megjelenése, valamint a nem kívánt szexuális hozzászólások kapcsán elmondható, hogy ezek az online cselekmények elsősorban a fiatalabb, alacsony önkontrollal rendelkező nőket érintik, akik több időt töltenek online felületeken. Ezzel szemben az online társskereső oldalon keresztül végrehajtott csalás áldozatai alacsonyabb önkontrollal rendelkező fiatalabb férfiak.

A regressziós modellekben használt változókkal kapcsolatban érdemes megjegyezni, hogy a nem és életkor, az online töltött idő, a számítógépes ismeretek és az önkontroll mértéke összességében kevés magyarázóerővel bírnak az elkövetést illetően ( $R^2$ : 0,05–0,25). További kutatások tárgyát képezheti, hogy milyen demográfiai, internetezési szokásokkal kapcsolatos, vagy egyes személyiségdimenziókat mérő változókkal ragadható meg az online térben történő áldozattá válás.

## *Elkövetések*

A kutatás során használt kérdőívben, az áldozattá válás mellett, tízféle online cselekmény elkövetéséről kérdeztük a résztvevőket, a kérdést megelőző 12 hónapra vonatkozóan. Az online cselekmények áldozataihoz hasonlóan az elkövetők esetében is azt találjuk, hogy az Egyesült Államokban vannak a legnagyobb arányban a megkérdezettek közül. Az összefüggés szignifikáns a khi-négyzet próba alapján, két cselekmény – a szerzői joggal védett fájlok vagy programok illegális letöltése, illetve valaki kizárása egy online közösségből – kivételével. Ezek mindhárom országban közel hasonló arányban fordulnak elő.

Az összes elkövetői típusból összevont elkövetés-indexen az amerikaiak 0,97-es, a finnek 0,47-es, végül a magyarok 0,39-es átlagot értek el.

Hasonlóan az online áldozattá váláshoz, a férfiak a nőkhöz képest nagyobb arányban válnak elkövetővé: a nőknél 18,7% (385 fő), a férfiaknál 25,7% (497 fő) az elkövetők aránya. Az összefüggés szignifikáns a khi-négyzet próba alapján ( $\chi^2=28,458$ ;  $p<0,01$ ).

## *Elkövetések a magyar mintában*

A kutatás magyar résztvevői (N=1421) közül 321 (22,59%) fő követett el legalább egyet az általunk vizsgált online cselekmények közül. A leggyakoribb cselekmény valaki online közösségből való kizárása volt (15,3%), amelyet az illegális letöltés (8,0%) és a sértő információ megosztása (5,5%) követett. Az 5. számú táblázat a magyar elkövetők nem és korcsoportok szerinti gyakoriságát, illetve az önkontroll-skálán elért átlagát mutatja, azokhoz viszonyítva, akik egy cselekményt sem követtek el. Kutatásunk során feltételeztük, hogy az alacsony önkontroll egyaránt kapcsolatban áll az áldozattá válással, illetve az online térben elkövetett egyes cselekményekkel is. Az önkontroll szintje minden cselekmény esetében alacsonyabb volt az elkövetők csoportjában, a Mann–Whitney-próba alapján ( $p<0,01$ ).

## 5. számú táblázat

Magyar elkövetők nem, életkor és az önkontroll mértéke szerint

Cselekmény az online térben	Nem			Kor				Alacsony önkontroll		
	Nő	Férfi	p.	18–25 éves	26–59 éves	60+ éves	p.	Elkövető		p.
	%	%		%	%	%		Igen	Nem	
Sértő információ megosztása valakiről az interneten (N=77)	3,3	7,8	<0,01	4,9	4,9	6,9	N.S.	10,02	6,58	<0,01
Megfenyegetett vagy inzultált valakit e-mailben vagy üzentküldő alkalmazásban (N=20)	1,0	1,8	N.S.	1,4	1,9	0,5	N.S.	10,69	6,68	<0,01
Kizárt valakit egy online közösségből (N=213)	14,6	16,1	N.S.	10,6	16,0	15,7	N.S.	8,14	6,66	<0,01
Betört az internet egy olyan részére, amelyhez nincs engedélyezett hozzáférése (N=18)	0,4	2,1	<0,01	2,8	1,5	0,3	<0,1	10,92	6,71	<0,01
Rosszindulatú szoftvert terjesztett (N=16)	0,9	1,5	N.S.	1,4	1,4	0,3	N.S.	11,22	6,67	<0,01
Illegálisan töltött le szerzői joggal védett fájlokat vagy programokat (N=111)	4,3	11,8	<0,01	13,3	9,1	4,0	<0,01	8,99	6,67	<0,01
Illegálisan töltött fel szerzői joggal védett fájlokat vagy programokat (N=37)	2,0	3,3	N.S.	3,5	3,2	1,1	<0,1	10,08	6,69	<0,01
Felhasználta valaki más személyes adatait az interneten az illető engedélye nélkül (N=21)	0,7	2,2	<0,05	3,5	1,8	0,3	<0,05	10,84	6,69	<0,01
Illegális kábítószerket vagy vényköteles gyógyszereket vásárolt az interneten recept nélkül (N=13)	0,9	1,0	N.S.	0,7	1,2	0,3	N.S.	10,83	6,70	<0,01
Meztelen fotókat osztott meg valaki másról az illető engedélye nélkül (N=18)	0,6	1,9	<0,05	3,5	1,4	0,3	<0,05	10,87	6,70	<0,01
Statisztikai próba	Fisher-próba			Khi-négyszet próba				Mann-Whitney-próba		

Forrás: A szerzők saját szerkesztése.

A Fisher-próba alapján szignifikánsan gyakoribb volt a férfiakra a nőkhöz képest a sértő tartalom megosztása online, a betörés az internet egy olyan részére, amelyhez nincs engedélyezett hozzáférése, az illegális letöltés, mások személyes adatainak engedély nélküli felhasználása, valamint a másokról készült meztelen fotók engedély nélküli megosztása.

Az elkövetők korcsoportok szerinti megoszlása kapcsán elmondható, hogy az illegális le- és feltöltés, mások adatainak engedély nélküli felhasználása és

a meztelen fotók engedély nélküli megosztása a fiatal felnőtt korcsoport tagjai esetében gyakoribb cselekmény, míg más elkövetési formáknál – például sértő információk megosztása, vagy online közösségből való kizárás – nincs eltérés az egyes korcsoportok között.

## Diszkusszió és kitekintés

Kérdőíves kutatásunk során az online és offline áldozattá válást, a kiberbűncselekmények és azok elkövetésének egyes kriminológiai elméletekkel való kapcsolatát vizsgáltuk. Azt találtuk, hogy a vizsgált országok mindegyikében a férfiak nagyobb arányban váltak áldozattá és több kiberbűncselekményt is követtek el az online térben. Az offline területen ez megerősíti a korábbi kutatások adatait, valamint a hivatalos statisztikai adatokkal is megegyezik (van Dijk, van Kersteren & Smit, 2007). A férfiak gyakoribb online áldozattá válását összefüggésbe hoztuk a nőkhöz képest szignifikánsan nagyobb mértékű online aktivitással, ami csak bizonyos biztonsági megelőző intézkedések gyakoribb használatával járt együtt (például személyazonosság ellopását monitorozó megoldások, vírusirtó használata), más intézkedések esetében nem találtunk szignifikáns különbséget.

Kutatásunk során bebizonyosodott, hogy az önkontroll alacsony szintje az áldozattá válás és az online elkövetés valószínűségét egyaránt növeli.

Az alacsonyabb önkontrollal rendelkező személyek nagyobb valószínűséggel estek áldozatul a különböző e-mailes, webes csalásoknak, adatlopási kísérleteknek, számítógépes vírusoknak. Az így elkövetett bűncselekmények esetében szintén több tényező van, amelyek gyengítik az önkontroll és környezeti kontroll hatását (Varga, 2021): az online tér távolító hatása, az alacsony felde-rítettség, vagy az anonimitásba vetett hit egyes elemei.

A másik ilyen, online térben is igaznak bizonyuló elmélet a rutintevékeny-ség-teória, amelynek a Dearden–Parti szerzőpáros szerint az oka az, hogy a kibertér megkönnyíti az elkövető és áldozat konvergenciáját, és a technológiai eszközök terjedése hatással van a bűncselekmények elkövetésére (Dearden & Parti, 2021; Parti & Szigeti, 2021).

Ezek az eredmények összecsengenek a korábban az Egyesült Államokban, valamint Finnországban végzett más vizsgálatok eredményeivel is, amelyek azt mutatták, hogy az önkontroll szintje, a rutinszerű online tevékenységekben való részvételre fordított idő és a demográfiai jellemzők mind az áldozattá válás, mind a bűncselekmények elkövetésének szignifikáns előrejelzői voltak (Näsi et al., 2023).

Az elmélet helytállóságát támasztja alá az, hogy ezeket a cselekményeket a mindinkább bővülő internethasználat, az online térben zajló társadalmi élet, a közösségi média, a kereskedelmi és vásárlói platformok széles körű, egyre egyszerűbb és mindenki által elérhető felületei elősegítik. Az emberek egyre több időt töltenek az online világban, virtuális kapcsolatok épülnek fel, időnként valós háttér nélkül. Az internet mindenki számára elérhető a nap minden szakaszában, és a telefonon történő böngészés gyakorlatilag ezt mindinkább fokozza azzal, hogy minél gyorsabb reakciókra késztet – alkalmasint átgondolatlanul – az esetlegesen elérhető társadalmi és/vagy gazdasági előny, nyereség érdekében.

A férfiak nagyobb kitettsége összefügghet nemcsak az online térben eltöltött több idővel, hanem a nagyobb kockázatvállalási készséggel, ami az offline világban is nagyobb mértékű sértetté válást eredményez körükben (Barabás, 2015).

Az áldozattá válásban jelentős szerepet játszik a megfelelő védelem, valamint a biztonsági ismeretek hiánya, ami mind a technikai, mind pedig tudás szinten megmutatkozik, különösen a nők esetében (Barabás, 2014).

Mindez rámutat arra, hogy további kutatásokra van szükség, mert a magyarázatok azonosítása lehetővé teszi a megelőzés célcsoportokra, illetve konkrét felhasználói típusokra, illetve magatartásformákra történő kidolgozását.

## Melléklet

### *Az online és offline áldozattá válás kérdésblokk itemei*

Az elmúlt 12 hónapban...	
Online áldozattá válás	Ön pénzt veszített egy e-mailben, weboldalon megjelenő vagy más számítógépes csalás következtében
	az Ön személyes adatait felhasználva valaki más bankszámlát, hitelkártyát létesített vagy kölcsönt vett fel
	Ön ismeretlen tranzakciókat észlelt a bankszámláján, bankkártyáján vagy más online fizetési rendszerén
	Ön értesítést kapott egy cégtől vagy szervezettől, hogy személyes adatait (nevét, bankkártya adatait, jelszavát stb.) ellopták vagy publikusan megosztották
	sértő hozzászólás, kép vagy videó jelent meg Önről az interneten
	Ön nem kívánt szexuális jellegű hozzászólásokat vagy utalásokat kapott online
Offline áldozattá válás	egy számítógépes vírus vagy rosszindulatú program jelent meg az Ön számítógépén, amely befolyásolta annak működését
	Ön pénzt veszített egy offline vagy telefonos csalás következtében
	az Ön személyigazolványát vagy forgalmi engedélyét fizikailag ellopták
	az Ön bankkártyáját vagy készpénzét ellopták
	Ön sértő hozzászólásokat kapott személyesen
	Ön nem kívánt szexuális jellegű hozzászólásokat vagy utalásokat kapott offline, személyesen
	az Ön személyes tulajdonát megrongálták

## Önkontroll kérdésblokk:

*Ön mennyire ért egyet a következő állításokkal?...*

- Gyakran válok dühössé, és veszítem el a türelmem (1)
- Veszélyes dolgokat csinállok szórakozásból (2)
- Izgalmas dolgokat csinállok, akkor is, ha veszélyesek (3)
- Kockázatvállaló vagyok (4)
- Gyakran azután gondolkodom, hogy cselekedtem (5)

## Rutintevékenység-elmélet kérdésblokkok

*Jelenleg alkalmazásban / Korábbi áldozattá válás miatt alkalmazom...*

- Eltakarja a webkamerát a számítógépén, laptopján (1)
- Személyazonossága ellopását monitorozó megoldást használ (2)
- Befagyasztja bankkártyáját, amikor nem tervezi használni (3)
- Vírusirtó programot vagy tűzfalat használ számítógépén (4)

## Felhasznált irodalom

---

- Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, 30(1), 47–88. <http://dx.doi.org/10.1111/j.1745-9125.1992.tb01093.x>
- Akers, R. L. (1998). *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Northeastern University Press.
- Barabás, A. T. (2004). General Victimology, Latency. In Irk, F. (Ed.), *Victims and opinions, Vol. I.* (pp. 161–201). National Institute of Criminology. [https://www.okri.hu/images/stories/joomla/Victims%20and%20Opinion\\_vol.%20I.pdf](https://www.okri.hu/images/stories/joomla/Victims%20and%20Opinion_vol.%20I.pdf)
- Barabás A. T. (Szerk.) (2014). *TOLVAJ-KULCS. A betöréses lopások vizsgálata az elkövetők szemszögéből*. Országos Kriminológiai Intézet. [https://www.okri.hu/images/stories/konyvajanlo/tolvajkulcs\\_2014/tolvajkulcs\\_sec.pdf](https://www.okri.hu/images/stories/konyvajanlo/tolvajkulcs_2014/tolvajkulcs_sec.pdf)
- Barabás A. T. (2015). *Áldozatok és igazságszolgáltatás*. Országos Kriminológiai Intézet.
- Barabás, A. T. (Ed.) (2018). *The Dimensions of Insecurity in Urban Areas. Research on the Roots of Unsafety and Fear of Crime in European Cities*. National Institute of Criminology. [https://en.okri.hu/images/stories/OKRIKOTETEK\\_2016/BT\\_Margin\\_2018/dimensions\\_sec.pdf](https://en.okri.hu/images/stories/OKRIKOTETEK_2016/BT_Margin_2018/dimensions_sec.pdf)
- Bossler, A. M. & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, 38(3), 227–236. <https://doi.org/10.1016/j.jcrimjus.2010.03.001>
- Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–560. <https://doi.org/10.2307/2094589>
- Dearden, T. E. & Parti, K. (2021). Cybercrime, differential association, and self-control: knowledge transmission through online social learning. *American Journal of Criminal Justice*, 46(6), 935–955. <https://doi.org/10.1007/s12103-021-09655-4>

- van Dijk, J. J. M., van Kesteren, J. N. & Smit, P. (2007). *Criminal Victimization in International Perspective, Key Findings from the 2004-2005 ICVS and EU ICS*. Ministry of Justice, WODC. [http://www.unicri.eu/services/library\\_documentation/publications/icvs/publications/ICVS2004\\_05report.pdf](http://www.unicri.eu/services/library_documentation/publications/icvs/publications/ICVS2004_05report.pdf)
- Gottfredson, M. & Hirschi, T. (1990). *A General Theory of Crime*. Stanford University Press.
- Holt, T. J. & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1–25. <https://doi.org/10.1080/01639620701876577>
- Kerezsi K. (2005). A bűnmegelőzés és biztonságérzet területi összetevői. In Irk F. (Szerk.), *Kriminológiai Tanulmányok 42.* (pp. 11–40). Országos Kriminológiai Intézet. [https://www.okri.hu/images/stories/KT/kt42\\_2005\\_sec.pdf](https://www.okri.hu/images/stories/KT/kt42_2005_sec.pdf)
- Messner, S. F. & Rosenfeld, R. (2013). *Crime and the American Dream*. Wadsworth.
- Näsi, M., Danielsson, P. & Kaakinen, M. (2023). Cybercrime Victimization and Politicization in Finland – Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*, 29(2), 283–301. <https://doi.org/10.1007/s10610-021-09497-0>
- Parti, K. & Szigeti, Á. (2021). The Future of Interdisciplinary Research in the Digital Era: Obstacles and Perspectives of Collaboration in Social and Data Sciences – An Empirical Study. *Cogent Social Sciences*, 7(1). <https://doi.org/10.1080/23311886.2021.1970880>
- Reyns, B. W. & Fisher, B. S. (2018). The relationship between offline and online stalking victimization: A gender-specific analysis. *Violence and Victims*, 33(4), 769–786. <https://doi.org/10.1891/0886-6708.VV-D-17-00121>
- Sutherland, E. H. (1937). *The Professional Thief: By a Professional Chief*. University of Chicago Press.
- Sutherland, E. H. (1947). *Principles of Criminology*. University of Chicago Press.
- Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, 8(2), 115–127. <https://doi.org/10.1177/1477370810393156>
- Varga Á. (2021). Kriminológiai elméletek és informatikai bűnözés. *In Medias Res*, 10(1), 155–196. <https://inmediasresfolyoirat.hu/imr/article/view/228>
- Virág Gy. (Szerk.) (2005). *Családi iszonyok*. KJK – KERSZÖV Jogi és Üzleti Kiadó.
- Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, 26(1), 277–292. <https://doi.org/10.1108/JFC-10-2017-0095>

## A cikkben található online hivatkozás

---

URL1: *Internet Crime Report 2021*. [https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC-3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC-3Report.pdf)



## A cikk APA szabály szerinti hivatkozása

---

Barabás A. T. & Koplányi G. (2023). Viktimizáció az online térben. Egy nemzetközi kutatás eredményei hazai szemszögből. *Belügyi Szemle*, 71(10), 1697–1713. <https://doi.org/10.38146/BSZ.2023.10.1>