

# Vásárlói bizalom az illegális szerek online piacán

Szerkesztette  
Kiss Tibor



**LUDOVIKA**  
EGYETEMI KIADÓ

Vásárlói bizalom az illegális szerek online piacán

Vákát

# Vásárlói bizalom az illegális szerek online piacán

Szerkesztette

Kiss Tibor



**LUDOVIKA**  
EGYETEMI KIADÓ

Budapest, 2021

A tanulmány a Nemzeti Közszolgálati Egyetem rektora által a bölcsészet- és társadalomtudományi doktori képzésben részt vevő hallgatók és a PhD- vagy CSC-fokozattal rendelkező kutatók számára 2019 októberében közzétett, „Az új információs technológiák hatása az emberre, a társadalmi együttélésre és az állam működésére” elnevezésű témakategória keretein belül közzétett pályázati projektben készült.

Szerzők:  
Kiss Tibor  
Szigeti Ákos  
Dornfeld László

Szakmai lektor:  
Krasznay Csaba

A kézirat lezárva: 2020. december 31.

Kiadja a Nemzeti Közszolgálati Egyetem  
Ludovika Egyetemi Kiadó  
A kiadásért felel: Koltay András rektor

Székhely: 1083 Budapest, Ludovika tér 2.  
Kapcsolat: [kiadvanyok@uni-nke.hu](mailto:kiadvanyok@uni-nke.hu)

Felelős szerkesztő: Inzsöl Kata  
Olvasószerkesztő: Kutas Éva  
Korrektor: Bujdosó Hajnalka  
Tördelőszerkesztő: Fehér Angéla

Nyomdai kivitelezés: Pátria Nyomda Zrt.  
Felelős vezető: Orgován Katalin vezérigazgató

ISBN 978-963-531-622-9 (nyomtatott)  
ISBN 978-963-531-623-6 (ePub) | ISBN 978-963-531-624-3 (pdf)

© A szerkesztő, 2021  
© A szerzők, 2021  
© Ludovika Egyetemi Kiadó, 2021

Minden jog védve.

# Tartalom

<i>Táblázatok jegyzéke</i>	7
<i>Ábrajegyzék</i>	11
<i>A kötet szerzői</i>	13
Bevezetés ( <i>Kiss Tibor</i> )	15
A vásárlói attitűdök feltérképezésének időszerűsége és indokoltsága ( <i>Kiss Tibor</i> )	17
Internetszabályozás ( <i>Dornfeld László</i> )	23
Modellek	23
Büntetőjogi szabályozás	25
Az illegális szerek internetes kereskedelmének színterei ( <i>Kiss Tibor</i> )	29
Az illegális szerek internetes kereskedelmének szereplői ( <i>Kiss Tibor</i> )	33
Az illegális szerek internetes kereskedelmének sajátosságai ( <i>Kiss Tibor</i> )	35
Az internetes kábítószer-kereskedelem mint kiberdeviancia ( <i>Kiss Tibor</i> )	41
Az illegális szerek internetes kereskedelme mögött álló résztvevői motivációk	43
A kábítószer-kereskedelem nemzetközi szabályozása ( <i>Dornfeld László</i> )	45
Az illegális szerek internetes kereskedelmének helye a kiberbűncselekmények körében	53
Az illegális szerek internetes kereskedelmének büntetőjogi alakzatai	55
Az illegális szerek internetes kereskedelmének szintérmódzatai	66
Az illegális szerek internetes kereskedelmét magyarázó társadalomtudományi elméletek ( <i>Kiss Tibor</i> )	71
A munkamegosztás és a társadalmi figuráció elmélete a darknetes kereskedelemben	71
A szociális tanulás és szubkultúraelmélet értelmezhetősége a darkneten	72
Illegális szerek online adásvétele a csereelmélet és a racionális döntés-elmélet tükrében	76
A megosztott bizalom elméletének jelentősége a darknetes interakciókban ( <i>Kiss Tibor</i> )	79
A bizalom internetes kereskedelemben betöltött szerepéről és funkciójáról szóló kutatások	80
Az attitűdkutatásban alkalmazott bizalmi faktorok struktúrája	85
A kutatás bemutatása ( <i>Kiss Tibor – Szigeti Ákos</i> )	91
Az attitűdkutatás célja	91
A háromfázisú kutatás célja	92
Az attitűdkutatás hipotézisei	92
A kutatás célcsoportja, időintervalluma és terepe	94
Az attitűdkutatás módszertani leírása	96
A kutatás eredményei: a hipotézisek vizsgálata ( <i>Kiss Tibor – Szigeti Ákos</i> )	103
A kutatás leíró statisztikái	103
Az első hipotézis vizsgálata	111
A második hipotézis vizsgálata	162
A harmadik hipotézis vizsgálata	177
A negyedik hipotézis vizsgálata	179
Az ötödik hipotézis vizsgálata	181
A hatodik hipotézis vizsgálata	181
A hetedik hipotézis vizsgálata	183
Bizalmi mátrix (bizalmi index)	184
Faktorelemzés a bizalmi indexek bevonásával	186

A kutatás hipotéziseken kívüli eredményei ( <i>Kiss Tibor – Szigeti Ákos</i> )	189
A kábítószer-fogyasztással szembeni zéró tolerancia megítélésének hatása	189
Rejtett bűngézőt használók eredményei	198
A kutatás következtetései ( <i>Kiss Tibor – Szigeti Ákos</i> )	209
A kutatás hasznosíthatósága és kapcsolódása a következő kutatási fázishoz ( <i>Kiss Tibor – Szigeti Ákos</i> )	213
Az átfogó kutatás első fázisából nyert eredmények folytatása a postaszolgálatokkal	213
Az átfogó kutatás első fázisából nyert eredmények folytatása a kriptovalutákkal	213
Az első kutatási fázis eredményeinek felhasználási javaslata a bűnmegelőzésben	214
Javaslat a megelőzés fókuszára	215
Javaslatok a megelőzés színterére és szereplőire	216
A kutatás hiányosságai ( <i>Kiss Tibor – Szigeti Ákos</i> )	217
Összefoglaló ( <i>Kiss Tibor</i> )	221
Melléklet (kérdőív)	223
Irodalomjegyzék	245
Felhasznált irodalom	245
Felhasznált jogszabályok	249
Ajánlott irodalom	250
<i>Abstract</i>	255

## Táblázatok jegyzéke

1. táblázat: Szexuális, hasznoszerzési és agresszióra épülő motivációk és normasértések	44
2. táblázat: A kábítószerrel kapcsolatos nemzetközi kriminalizáció	47
3. táblázat: Az internetes kábítószer- és gyógyszer-kereskedelem jogsértő alakzatai	55
4. táblázat: A kutatásban alkalmazott bizalmi kategóriák és bizalmi faktorok	89
5. táblázat: A kutatásról visszajelzést küldő és nem küldő felsőoktatási intézmények	95
6. táblázat: A kutatást elutasító felsőoktatási intézmények	95
7. táblázat: Élethelyzetek a 2–6. kérdéscsoportokhoz	98
8. táblázat: Életesemények motivációi mentén történő sorrendiség	101
9. táblázat: A hipotézisek és a kérdéscsoportok kapcsolódása	102
10. táblázat: Hány órát használja Ön az internetet munkavégzésre/tanulásra?	103
11. táblázat: Hány órát használja Ön az internetet munkavégzésen/tanuláson kívüli tevékenységre?	104
12. táblázat: Átlagosan milyen gyakran vásárol Ön online webshopokban?	104
13. táblázat: Online vásárlásához melyik eszközt használja inkább?	105
14. táblázat: Használ-e rendszeresen a privát böngészésen kívül olyan internetes böngészőt, amely nem ellenőrizhető, és nem gyűjt adatokat a felhasználóról, illetve lehetővé teszi a rejtett személyazonossággal történő böngészést (például Tor-böngésző)?	105
15. táblázat: Szokott-e internetes közösségi oldalakat, e-mail-szolgáltatásokat és más internetes szolgáltatásokat álnéven (nicknéven) használni?	106
16. táblázat: Milyen mértékben ért egyet a kábítószer-fogyasztással szembeni zéró toleranciával?	106
17. táblázat: Rendelkezik-e szakértelemmel?	107
18. táblázat: A válaszolók nemi eloszlása	108
19. táblázat: A válaszolók életkori eloszlása	108
20. táblázat: A válaszolók lakóhelye	109
21. táblázat: A válaszolók képzési területei	109
22. táblázat: A válaszolók képzési formái	110
23. táblázat: A válaszolók munkarendje	110
24. táblázat: Átnevezett bizalmi faktorok csoportonként	111
25. táblázat: A bizalmi faktorok szükségességének sorrendje átlagok alapján	117
26. táblázat: A bizalmi faktorok szükségességének sorrendje átlagok alapján az illegális 1. vásárlásban	123
27. táblázat: A bizalmi faktorok szükségességének sorrendje átlagok alapján az illegális 2. vásárlásban	128
28. táblázat: A bizalmi faktorok szükségességének sorrendje átlagok alapján az illegális 3. vásárlásban	133
29. táblázat: A bizalmi faktorok szükségességének sorrendje átlagok alapján az illegális 4. vásárlásban	139
30. táblázat: A bizalmi faktorok szükségességének sorrendje átlagok alapján az illegális 5. vásárlásban	144
31. táblázat: A bizalmi faktorok fontossága a legális és az illegális vásárlásban	145
32. táblázat: Az eladó elérhetősége és segítőkészsége bizalmi faktor összevetése a legális és az illegális vásárlásokban	147
33. táblázat: Az eladó megbízhatósága bizalmi faktor összevetése a legális és az illegális vásárlásokban	148
34. táblázat: A webáruház népszerűsége és pozitív véleményzettsége az interneten bizalmi faktor összevetése a legális és az illegális vásárlásokban	148
35. táblázat: A webáruház ajánlottsága ismerősök vagy barátok által bizalmi faktor összevetése a legális és az illegális vásárlásokban	149
36. táblázat: A webáruház oldalának átláthatósága és könnyű kezelhetősége bizalmi faktor összevetése a legális és az illegális vásárlásokban	150
37. táblázat: A vásárlás közben az internetes kapcsolatok zavartalansága bizalmi faktor összevetése a legális és az illegális vásárlásokban	150
38. táblázat: A személyes és a vásárlásról szóló adatok védelme bizalmi faktor összevetése a legális és az illegális vásárlásokban	151
39. táblázat: A vásárlói és eladói jogokról és köteleességekről való tájékoztatás bizalmi faktor összevetése a legális és az illegális vásárlásokban	151
40. táblázat: A regisztrációs lehetőség szükségessége bizalmi faktor összevetése a legális és az illegális vásárlásokban	152
41. táblázat: Az elérhető, gyors és egyszerű fizetési tranzakció bizalmi faktor összevetése a legális és az illegális vásárlásokban	153
42. táblázat: Az online fizetési lehetőség bizalmi faktor összevetése a legális és az illegális vásárlásokban	153



43. táblázat:	A hagyományos offline fizetési lehetőség bizalmi faktor összevetése a legális és az illegális vásárlásokban	154
44. táblázat:	A kriptovalutával történő fizetési lehetőség bizalmi faktor összevetése a legális és az illegális vásárlásokban	154
45. táblázat:	Az azonnali visszajelzés az online fizetési tranzakcióról bizalmi faktor összevetése a legális és az illegális vásárlásokban	155
46. táblázat:	A termékek és a szolgáltatások széles választéka, jó minősége és jó ár-érték aránya bizalmi faktor összevetése a legális és az illegális vásárlásokban	156
47. táblázat:	Az árukra vagy szolgáltatásokra eladói vagy gyártói garancia bizalmi faktor összevetése a legális és az illegális vásárlásokban	156
48. táblázat:	Megfelelő tájékoztatás a kínált árukról és szolgáltatásokról bizalmi faktor összevetése a legális és az illegális vásárlásokban	157
49. táblázat:	Az áruk épségben történő megbízható kézbesítése bizalmi faktor összevetése a legális és az illegális vásárlásokban	158
50. táblázat:	A rejtett és követhetetlen módon történő vásárlási lehetőség bizalmi faktor összevetése a legális és az illegális vásárlásokban	158
51. táblázat:	A vásárláskor megadott adataim azonnal törlődjenek bizalmi faktor összevetése a legális és az illegális vásárlásokban	159
52. táblázat:	A valós adataim még az eladó előtt se legyenek ismertek bizalmi faktor összevetése a legális és az illegális vásárlásokban	159
53. táblázat:	A legális és az illegális vásárlásban választott bizalmi faktorok szükségességének mértékéről	160
54. táblázat:	A webáruház oldalának átláthatósága és könnyű kezelhetősége bizalmi faktor magasabb meglétére adott válaszok az informatika/számítástechnika/infokommunikáció terület ismeretei mentén	164
55. táblázat:	A vásárlói és eladói jogokról és köteleességekről való tájékoztatás bizalmi faktor magasabb meglétére adott válaszok az informatika/számítástechnika/infokommunikáció terület ismeretei mentén	165
56. táblázat:	A vásárlói és eladói jogokról és köteleességekről való tájékoztatás bizalmi faktor magasabb meglétére adott válaszok az élettani terület ismeretei mentén	165
57. táblázat:	A regisztrációs lehetőség bizalmi faktor magasabb meglétére adott válaszok az informatika/számítástechnika/infokommunikáció terület ismeretei mentén	166
58. táblázat:	A regisztrációs lehetőség bizalmi faktor magasabb meglétére adott válaszok az élettani terület ismeretei mentén	166
59. táblázat:	Az elérhető, gyors és egyszerű fizetési tranzakció bizalmi faktor magasabb meglétére adott válaszok az informatika/számítástechnika/infokommunikáció terület ismeretei mentén	167
60. táblázat:	A hagyományos offline fizetési lehetőség bizalmi faktor magasabb meglétére adott válaszok az informatika/számítástechnika/infokommunikáció terület ismeretei mentén	167
61. táblázat:	A kriptovalutával történő fizetési lehetőség bizalmi faktor magasabb meglétére adott válaszok az informatika/számítástechnika/infokommunikáció terület ismeretei mentén	168
62. táblázat:	Az azonnali visszajelzés az online fizetési tranzakcióról bizalmi faktor magasabb meglétére adott válaszok az élettani terület ismeretei mentén	168
63. táblázat:	A termékek és a szolgáltatások széles választéka, jó minősége és jó ár-érték aránya bizalmi faktor magasabb meglétére adott válaszok az informatika/számítástechnika/infokommunikáció terület ismeretei mentén	169
64. táblázat:	Az árukra vagy szolgáltatásokra eladói vagy gyártói garancia bizalmi faktor magasabb meglétére adott válaszok az informatika/számítástechnika/infokommunikáció terület ismeretei mentén	169
65. táblázat:	A megfelelő tájékoztatás a kínált árukról és szolgáltatásokról bizalmi faktor magasabb meglétére adott válaszok az informatika/számítástechnika/infokommunikáció terület ismeretei mentén	170
66. táblázat:	A rejtett és követhetetlen módon történő vásárlási lehetőség bizalmi faktor magasabb meglétére adott válaszok az informatika/számítástechnika/infokommunikáció terület ismeretei mentén	171
67. táblázat:	A rejtett és követhetetlen módon történő vásárlási lehetőség bizalmi faktor magasabb meglétére adott válaszok az élettani terület ismeretei mentén	171
68. táblázat:	A részletes, tényezőnkénti elemzés eredményei az informatika/számítástechnika/infokommunikáció terület ismeretei mentén	172
69. táblázat:	Bizalmi tényezők fontossága az illegális szituációkban a kitöltők ismeretszintjéhez képest	174
70. táblázat:	A szituációkban alkalmazott bizalmi faktorok száma	175
71. táblázat:	A szituációk motivációinak hatása a 4. hipotézis tesztelésével	180
72. táblázat:	Cronbach-alpha mérőszám segítségével történő belső konzisztenciamérés eredményei	184
73. táblázat:	Bizalmi index	185

74. táblázat:	Faktorelemzés bizalmi indexek bevonásával	186
75. táblázat:	Milyen mértékben ért egyet a kábítószer-fogyasztással szembeni zéró toleranciával?	189
76. táblázat:	A zéró toleranciával való egyetértés és az egyén és a közösség bizalmi kategóriába tartozó eladó elérhetősége és segítőkészsége, az eladó megbízhatósága, a webáruház népszerűsége és pozitív véleményezettsége az interneten, valamint a webáruház ajánlottsága ismerősök vagy barátok által faktorok fontosságának összefüggései	190
77. táblázat:	A zéró toleranciával való egyetértés és a technikai tényezők bizalmi kategóriába tartozó webáruház oldalának átláthatósága és könnyű kezelhetősége, valamint a vásárlás közben az internetes kapcsolatok zavartalansága faktorok fontosságának összefüggései	190
78. táblázat:	A zéró toleranciával való egyetértés és az adatvédelmi tényezők bizalmi kategóriába tartozó személyes és a vásárlásról szóló adatok védelme, a vásárlói és eladói jogokról és köteleességekről való tájékoztatás, valamint a regisztrációs lehetőség faktorok fontosságának összefüggései	191
79. táblázat:	A zéró toleranciával való egyetértés és a fizetési tényezők bizalmi kategóriába tartozó elérhető, gyors és egyszerű fizetési tranzakció, az online fizetési lehetőség, a hagyományos offline fizetési lehetőség, a kriptovalutával történő fizetési lehetőség, valamint az azonnali visszajelzés az online fizetési tranzakcióról faktorok fontosságának összefüggései	192
80. táblázat:	A zéró toleranciával való egyetértés és a termékek és szolgáltatások bizalmi kategóriába tartozó termékek és a szolgáltatások széles választéka, jó minősége és jó ár-érték aránya, az árukra vagy szolgáltatásokra eladói vagy gyártói garancia és a megfelelő tájékoztatás a kínált árukról és szolgáltatásokról faktorok fontosságának összefüggései	193
81. táblázat:	A zéró toleranciával való egyetértés és a termékek és szolgáltatások bizalmi kategóriába tartozó áruk épségben történő megbízható kézbesítése faktor fontosságának összefüggései	193
82. táblázat:	A zéró toleranciával való egyetértés és rejtettség és anonimitás bizalmi kategóriába tartozó rejtett és követhetetlen módon történő vásárlási lehetőség, a vásárláskor megadott adataim azonnal törlődjenek, valamint a valós adataim még az eladó előtt se legyenek ismertek faktorok fontosságának összefüggései	194
83. táblázat:	A zéró toleranciával való egyetértés és az ajánlaná-e másnak a weboldalt összefüggései az illegális 1. szituációban	195
84. táblázat:	A zéró toleranciával való egyetértés és a vásárolna-e újból a weboldalról összefüggései az illegális 1. szituációban	195
85. táblázat:	A zéró toleranciával való egyetértés és az online vagy offline tér választásának összefüggései az illegális 1. szituációban	196
86. táblázat:	A zéró toleranciával való egyetértés és a bizalmi faktorok fontosságának összehasonlítása	196
87. táblázat:	Használ-e rendszeresen a privát böngészésen kívül olyan internetes böngészőt, amely nem ellenőrizhető, és nem gyűjt adatokat a felhasználóról, illetve lehetővé teszi a rejtett személyazonossággal történő böngészést (például Tor-böngésző)	198
88. táblázat:	A Tor-böngésző használata és az egyén és a termékek és szolgáltatások bizalmi kategóriába tartozó az eladó elérhetősége és segítőkészsége, az eladó megbízhatósága, a webáruház népszerűsége és pozitív véleményezettsége az interneten, a webáruház ajánlottsága ismerősök vagy barátok által faktorok fontosságának összefüggései	199
89. táblázat:	Tor-böngésző használata és a technikai tényezők bizalmi kategóriába tartozó webáruház-oldalának átláthatósága és könnyű kezelhetősége, valamint a vásárlás közben az internetes kapcsolatok zavartalansága faktorok fontosságának összefüggései	200
90. táblázat:	A Tor-böngésző használata és az adatvédelmi tényezők bizalmi kategóriába tartozó személyes és a vásárlásról szóló adatok védelme, a vásárlói és eladói jogokról és köteleességekről való tájékoztatás, valamint a regisztrációs lehetőség faktorok fontosságának összefüggései	200
91. táblázat:	A Tor-böngésző használata és a fizetési tényezők bizalmi kategóriába tartozó elérhető, gyors és egyszerű fizetési tranzakció, az online fizetési lehetőség, a hagyományos offline fizetési lehetőség, a kriptovalutával történő fizetési lehetőség, valamint az azonnali visszajelzés az online fizetési tranzakcióról faktorok fontosságának összefüggései	201
92. táblázat:	A Tor-böngésző használata és a termékek és szolgáltatások bizalmi kategóriába tartozó termékek és a szolgáltatások széles választéka, jó minősége és jó ár-érték aránya, az árukra vagy szolgáltatásokra eladói vagy gyártói garancia és a megfelelő tájékoztatás a kínált árukról és szolgáltatásokról faktorok fontosságának összefüggései	202
93. táblázat:	A Tor-böngésző használata és a szállítási szolgáltatások bizalmi kategóriába tartozó áruk épségben történő megbízható kézbesítése faktor fontosságának összefüggései	202

94. táblázat:	A Tor-böngésző használata és a rejtettség és anonimitás bizalmi kategóriába tartozó rejtett és követhetetlen módon történő vásárlási lehetőség, a vásárláskor megadott adataim azonnal törlődjenek, valamint a valós adataim még az eladó előtt se legyenek ismertek faktorok fontosságának összefüggései	203
95. táblázat:	A Tor-böngésző használata és az ajánlaná-e másnak a weboldalt illegális 1. szituációban összefüggése	204
96. táblázat:	A Tor-böngésző használata és a vásárolna-e újból a weboldaltól illegális 1. szituációban összefüggése	204
97. táblázat:	A Tor-böngésző használata és az online vagy offline tér választása illegális 1. szituációban összefüggései	205
98. táblázat:	A Tor-böngésző használatával való egyetértés és a bizalmi faktorok fontosságának összehasonlítása	205

# Ábrajegyzék

1. ábra:	Kábítószerek, gyógyszerek és a kábítószerek előállításához szükséges vegyszerek kínálatának aránya a darkneten	17
2. ábra:	Különböző kábítószerek darknetes eladásából származó árbevétel országoként 2017 és 2018 között	19
3. ábra:	A darkneten kábítószereket vásárlók számának emelkedése 2014–2020 között az Amerikai Egyesült Államokban, Európában és más kontinensen	20
4. ábra:	Az internetes kábítószer- és illegális gyógyszer-kereskedelem motivációi	45
5. ábra:	Az internetes teret érintő kábítószer-kereskedelem katalizáló módozata	68
6. ábra:	Katalizáló módozat internetes fizetés esetén	69
7. ábra:	Az egyéni és közösségi kategóriába tartozó bizalmi faktorok szükségességének eloszlása a legális vásárlásban	113
8. ábra:	A technológia és hálózat kategóriába tartozó bizalmi faktorok szükségességének eloszlása a legális vásárlásban	113
9. ábra:	Az adatvédelem és jogi tájékoztatás kategóriába tartozó bizalmi faktorok szükségességének eloszlása a legális vásárlásban	114
10. ábra:	A fizetési tranzakciók kategóriába tartozó bizalmi faktorok szükségességének eloszlása a legális vásárlásban	115
11. ábra:	A termékek és szolgáltatások kategóriába tartozó bizalmi faktorok szükségességének eloszlásai a legális vásárlásban	115
12. ábra:	A szállítási szolgáltatások kategóriába tartozó bizalmi faktor szükségességének eloszlásai a legális vásárlásban	116
13. ábra:	A rejtettség és anonimitás kategóriába tartozó bizalmi faktor szükségességének eloszlásai a legális vásárlásban	116
14. ábra:	Az egyéni és közösségi kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 1. vásárlásban	118
15. ábra:	A technológia és hálózat kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 1. vásárlásban	119
16. ábra:	Az adatvédelem és jogi tájékoztatás kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 1. vásárlásban	119
17. ábra:	A fizetési tranzakciók kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 1. vásárlásban	120
18. ábra:	A termékek és szolgáltatások kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 1. vásárlásban	121
19. ábra:	A szállítási szolgáltatások kategóriába tartozó bizalmi faktor szükségességének eloszlása az illegális 1. vásárlásban	121
20. ábra:	A rejtettség és anonimitás kategóriába tartozó bizalmi faktor szükségességének eloszlása az illegális 1. vásárlásban	122
21. ábra:	Az egyéni és közösségi kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 2. vásárlásban	124
22. ábra:	A technológia és hálózat kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 2. vásárlásban	124
23. ábra:	Az adatvédelem és jogi tájékoztatás kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 2. vásárlásban	125
24. ábra:	A fizetési tranzakciók kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 2. vásárlásban	126
25. ábra:	A termékek és szolgáltatások kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 2. vásárlásban	126
26. ábra:	A szállítási szolgáltatások kategóriába tartozó bizalmi faktor szükségességének eloszlása az illegális 2. vásárlásban	127
27. ábra:	A rejtettség és anonimitás kategóriába tartozó bizalmi faktor szükségességének eloszlása az illegális 2. vásárlásban	127
28. ábra:	Az egyéni és közösségi kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 3. vásárlásban	129
29. ábra:	A technológia és hálózat kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 3. vásárlásban	130

30. ábra:	Az adatvédelem és jogi tájékoztatás kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 3. vásárlásban	130
31. ábra:	A fizetési tranzakciók kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 3. vásárlásban	131
32. ábra:	A termékek és szolgáltatások kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 3. vásárlásban	132
33. ábra:	A szállítási szolgáltatások kategóriába tartozó bizalmi faktor szükségességének eloszlása az illegális 3. vásárlásban	132
34. ábra:	A rejtettség és anonimitás kategóriába tartozó bizalmi faktor szükségességének eloszlása az illegális 3. vásárlásban	133
35. ábra:	Az egyéni és közösségi kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 4. vásárlásban	134
36. ábra:	A technológia és hálózat kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 4. vásárlásban	135
37. ábra:	Az adatvédelem és jogi tájékoztatás kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 4. vásárlásban	136
38. ábra:	A fizetési tranzakciók kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 4. vásárlásban	136
39. ábra:	A termékek és szolgáltatások kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 4. vásárlásban	137
40. ábra:	A szállítási szolgáltatások kategóriába tartozó bizalmi faktor szükségességének eloszlása az illegális 4. vásárlásban	138
41. ábra:	A rejtettség és anonimitás kategóriába tartozó bizalmi faktor szükségességének eloszlása az illegális 4. vásárlásban	138
42. ábra:	Az egyéni és közösségi kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 5. vásárlásban	140
43. ábra:	A technológia és hálózat kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 5. vásárlásban	140
44. ábra:	Az adatvédelem és jogi tájékoztatás kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 5. vásárlásban	141
45. ábra:	A fizetési tranzakciók kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 5. vásárlásban	142
46. ábra:	A termékek és szolgáltatások kategóriába tartozó bizalmi faktorok szükségességének eloszlása az illegális 5. vásárlásban	142
47. ábra:	A szállítási szolgáltatások kategóriába tartozó bizalmi faktor szükségességének eloszlása az illegális 5. vásárlásban	143
48. ábra:	A rejtettség és anonimitás kategóriába tartozó bizalmi faktor szükségességének eloszlása az illegális 5. vásárlásban	143
49. ábra:	Az online és az offline tér közötti választás az öt illegális szituációban	177
50. ábra:	Az offline teret választók jelölései az öt illegális szituációban	179
51. ábra:	A kitöltők webmarketbe való visszatéréséről adott jelölései	182
52. ábra:	A kitöltők webmarket ajánlására adott jelölései	183

## A kötet szerzői

KISS Tibor kriminológus, a Nemzeti Közszerológati Egyetem Eötvös József Kutatóközpont Kiberbiztonsági Kutatóintézet kutatója és a Nemzeti Közszerológati Egyetem Rendészet-tudományi Kar Kriminológia Tanszék adjunktusa. Kutatási területe a kiberkriminológia és a kiberdevianciák.

SZIGETI Ákos szociológus, a Nemzeti Közszerológati Egyetem Eötvös József Kutatóközpont Kiberbiztonsági Kutatóintézetének kutatója és a Nemzeti Közszerológati Egyetem Rendészet-tudományi Doktori Iskolájának PhD-hallgatója. Kutatási területei: társadalomkutató módszerek, szövegbányászat, kiberbűnözés.

DORNFELD László jogász, a Mádl Ferenc Összehasonlító Jogi Intézet, valamint a Nemzeti Közszerológati Egyetem Eötvös József Kutatóközpont Kiberbiztonsági Kutatóintézet kutatója és a Miskolci Egyetem Állam- és Jogtudományi Kar doktorjelöltje. Kutatási területe a kiberbűnözés, a kiberkriminológia, a kiberszabályozás és a kiber-geopolitika.

Vákát

Kiss Tibor

## Bevezetés

A kiberbűnözés háttérokait kutató kriminológusok szerint azok a legdominánsabb normasértések a kibertérben, amelyek a legtöbb felhasználó sérelmére képesek kárt okozni, vagy épp a legszélesebb tömegek igényeinek kielégítését szolgálják.<sup>1</sup> Ez utóbbiak egyike az internetes kábítószer- és gyógyszer-kereskedelem, amelynek kínálati oldalán a haszonszerzési igények, a keresleti oldalán különböző kényszerek által előidézett szükségletek elégülnek ki kölcsönös érdekeken alapulva. A két pólus között zajló tranzakciók akár a John Thibaut és Harold Kelley (1959) amerikai pszichológusok által felállított *csereelmélet* vagy a Gary S. Becker által 1976-ban kidolgozott, majd Derek B. Cornish és Ronald V. Clarke által (1986) a bűnözésre adaptált *racionális döntés-elmélet* modern formációjaként is leírhatók. Mindkét teória szorosan illeszkedik az illegális szerek internetes kereskedelmének folyamatához, mivel a tiltott tranzakciókban zajló adásvétel a felek érdekeit szolgálja, miközben a kockázatok mértékét a titkos működéssel minimálisra próbálják csökkenteni. A hagyományos kriminológiai elméletek mellett az online kereskedelem működésének magyarázatára már létezik egy pragmatikusabb megközelítés is. Eszerint a kínálati és a keresleti oldal két pólusát a *megosztott bizalom* tengelye köti össze, amelyet az infokommunikációs technológia és a globális hálózat erősített meg a résztvevők között az elmúlt évtizedekben.<sup>2</sup> A Silk Road 2013-as bezárása óta tisztán látható, hogy a horizontális bizalom stabilizálódása a virtuális feketepiacok működésére jelentős hatást gyakorolt, sőt, olyan önszabályozó közösségek szerveződését segítette elő, amelyek képesek külső kontroll nélkül fenntartani az illegális drogmarkeket – még a felszámolásukra hivatott hatósági nyomás ellenére is. A résztvevők közötti bizalomnak köszönhetően az illegális kriptopiacok virágkorukat élik – főként a kábítószer-kereskedelem területén, amely az összes tiltott online tranzakció túlnyomó részét teszi ki –, és számuk évről évre emelkedik.<sup>3</sup> Az online kábítószer-kereskedelem visszaszorításának egyik hatékony eszköze a keresletcsökkentés, vagyis olyan szabályozási eszközök, intézkedések, megelőzési és kezelési módok összessége, amelyekkel a vásárlói döntés befolyásolható. Az internetes kereskedelmet meghatározó kereslet mérséklése viszont nem egyszerű feladat, ugyanis az adásvétel egy szakasza a hagyományos térből az online térbe kerülve még láthatatlanabb, és ezzel együtt nehezebben kontrollálható. A helyzetet tovább bonyolítja, hogy az alacsony lebukási kockázat és a szerekhez való konfliktusmentes hozzájutás lehetősége vásárlásra ösztönözheti azokat a felhasználókat is, akik a vásárlásra kényszerítő élethelyzetek ellenére sem kísérelnék meg ugyanezt

<sup>1</sup> Kiss Tibor – Parti Katalin – Prazsák Gergely: *Cyberdeviancia*. Budapest, Dialóg Campus, 2019. 55–133.

<sup>2</sup> Rachel Botsman: *Kiben bízunk*. Budapest, Cser, 2017. 11–257.

<sup>3</sup> United Nations Office on Drugs and Crime (UNODC): *World Drug Report. Cross-Cutting Issues. Evolving Trends and New Challenges*. United Nations Publication, Sales, No. E.20.XI.6. 2020.

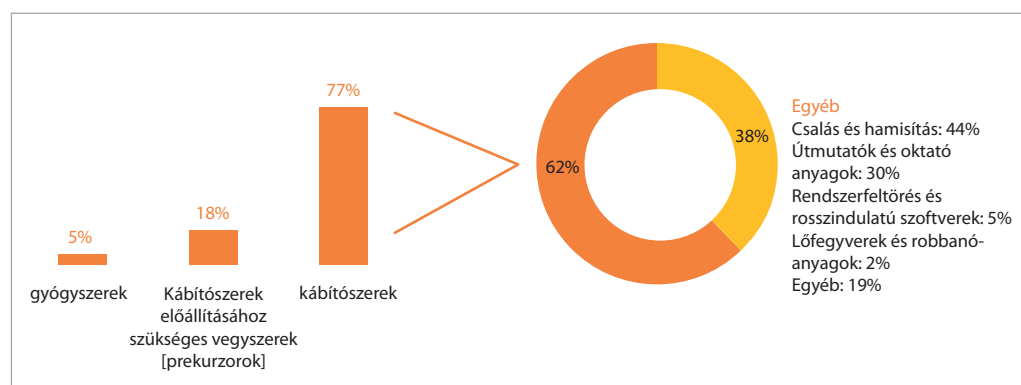


a magasabb kockázatú hagyományos környezetben.<sup>4</sup> Az internetes drogvásárlók egyre bővülő táborát vagy a még materiálisan nem érintett, de potenciális vásárlóként számításba vehetők csoportját elsősorban a különböző szinteken és színtereken is megvalósulni képes bűnmegelőzési módszerekkel lehet kíméletesen elérni és eltéríteni őket vásárlási szándékuktól.

<sup>4</sup> Atte Oksanen – Lee Miller Bryan – Iina Savolainen – Anu Sirola – Jakob Demant – Markus Kaakinen – Izabela Zych: Illicit Drug Purchases via Social Media Among American Young People. In Gerhard Goos – Juris Hartmanis (szerk.): *Social Computing an Social Media*. 12th International Conference, SCSM 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Koppenhága, 2020. július 19–24. 278–289.

## A vásárlói attitűdök feltérképezésének időszerűsége és indokoltsága

A globális internetes kereskedelem vásárlói körének bővülését az Amerikai Egyesült Államokban és Európában zajló online kábítószer-vásárlás számszerű emelkedése példázza a legjobban. A United Nation Office and Drug Crime (UNODC) 2020-as jelentésében közölt kutatások eredményei szerint a darkneten működő fekete piac 62%-át a kábítószer- vagy illegális gyógyszer-kereskedelem, 38%-át más tárgyak vagy szolgáltatások (például fegyverek, hamisított okmányok, gyermekekről készült pornográf felvételek vagy épp információs rendszerek feltörésére alkalmazható szoftverek) kínálata teszi ki.<sup>1</sup> A jelentésben közölt arányokból egyenesen következik, hogy az internetes feketekereskedelemben a kábítószerpiacnak van a legnagyobb és legheterogénebb összetételű vásárlói csoportokból álló látogatója világszerte. A globális kábítószer-kereskedelem hagyományos szintéhez kötöttségét magyarázzák azok a kutatási eredmények is, amelyek szerint 2015–2020 között a darkneten működő drogpiacon az amerikai és az európai hagyományos kábítószer-kereskedelem csupán 0,2%-át teszik ki. Az illegális szerek kereskedelmét bonyolító internetes feketepiacon inkább a kábítószer adásvétele dominál, azonban megtalálhatók az illegálisan árusított hamis vagy hamisított gyógyszerek, valamint a kábítószerek előállításához szükséges vegyszerek is (prekursorok) – bár sokkal kisebb arányban (1. ábra).



1. ábra: Kábítószerek, gyógyszerek és a kábítószerek előállításához szükséges vegyszerek kínálatának aránya a darkneten

Forrás: European Monitoring Centre for Drugs and Drug Addiction and Europol (EMCDDA): *Perspectives for enforcement, research and policy*. Europol Joint Publications. Luxembourg, Publications Office of the European Union, 2017. 15.

<sup>1</sup> UNODC (2020): i. m. 72.

Az elmúlt öt év tendenciája azt mutatja, hogy átlagosan minden második évben fel-tűnik egy olyan darknetes kábítószermarket, amely nagyobb vásárlói tömeget vonz maga köré, majd hónapokig óriási profitot termel. Az elmúlt időszakban több efféle market is megjelent, egyebek mellett az Alpha Bay, a Dream Market, a TradeRout, a Valhalla, a Berlusconi Market, amelyek köztudottan az internetes feketepiac óriá-saiként látták el az amerikai és az európai vásárlók tömegét.<sup>2</sup> A Kábítószer és Kábító-szerfüggőség Európai Megfigyelőközpontja (*European Monitoring Centre for Drugs and Drug* – EMCDDA) 2019-es Európai Kábítószerjelentése (*Addiction Drug Markets Report*, 2019) szerint a nagyobb kábítószermarketek folyamatosan fluktuálnak, vagyis miközben nyomtalanul eltűnnek (például a hatósági felszámolás vagy az exit scam eredményeként), újabbak jelennek meg. 2015 és 2019 között több mint száz market tűnt el az internetről különböző okok miatt, de ugyanebben az időpontban jó néhány folytatta a kábítószer-értékesítő tranzakcióit.<sup>3</sup> A piacok némelyikének bezárása vagy felszámolása mindig hatást gyakorol az internetes marketekre, de valójában nem ingatja meg számottevően a vásárlás dinamikáját, ugyanis a hoppon maradt vásárlók a megmaradó vagy az új marketek keresleti köreihez csapódva az internetes piacon maradnak.<sup>4</sup> A vizsgált darknet marketekben a legtöbb kábítószer-rendelés az Amerikai Egyesült Államokból, Ausztráliából és Kanadából érkezett, míg Európában Angliából, Németországból, Hollandiából, Franciaországból és végül Spanyolországból. Európában az internetes piacon működő drogmarketek némelyike ugyanezekhez az államokhoz köthető.<sup>5</sup> Az elmúlt öt évben működő nagyobb darknetes piacok forgalmának elemzése stabil trendeket mutat. Például 2016-ban a globális kábítószer-kereskedelemből bejövő illegális jövedelem a nemzetközi jelentések szerint 625 milliárd dollár, a darknetes vásárlásokból bejövő összeg 20 millió dollár volt.<sup>6</sup> Európán belül 2017 és 2018 között az Egyesült Királyságban a darkneten 2825 kg kábítószerrel adtak el 28,2 millió euró értékben, Németországban ez idő alatt 3153 kg kábítószerrel értékesítettek 18,8 mil-lió euróért, míg Hollandiában 1174 kg kábítószer kelt el 10,3 millió euró értékben.<sup>7</sup> Az európai országok marketjei közül a legtöbbet a német piacon, viszont a jobb minő-ségű és drágább szereket Angliában értékesítették (*2. ábra*).

<sup>2</sup> UNODC (2020): i. m. 76.

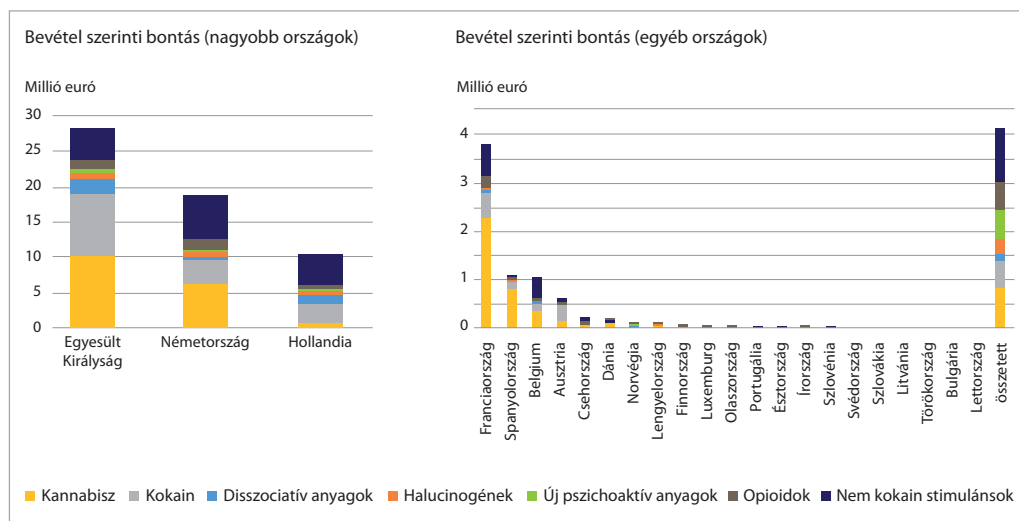
<sup>3</sup> Ilyen volt a Tchka, az OW Market, a The Majestic Garden, a Berlusconi Market, a Cannazon, a Rapture Market, az Empire Market, az Apollon, a Serpent Market és a Nightmare Market (European Monitoring Centre for Drugs and Drug Addiction and Europol [EMCDDA]: *EU Drug Markets Report*. Luxembourg, Publications Office of the European Union, 2019).

<sup>4</sup> Judith Aldridge – David Décary-Hétu: [Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets](#). *International Journal of Drug Policy*, 35. (2016). 7–15.

<sup>5</sup> UNODC (2020): i. m. 75; EMCDDA (2019): i. m. 5–283.

<sup>6</sup> Lucia Bird et al.: *Transformative technologies*. Global Initiative Against Transnational Organized Crime. 2020. 4–38.

<sup>7</sup> EMCDDA (2019): i. m. 71.

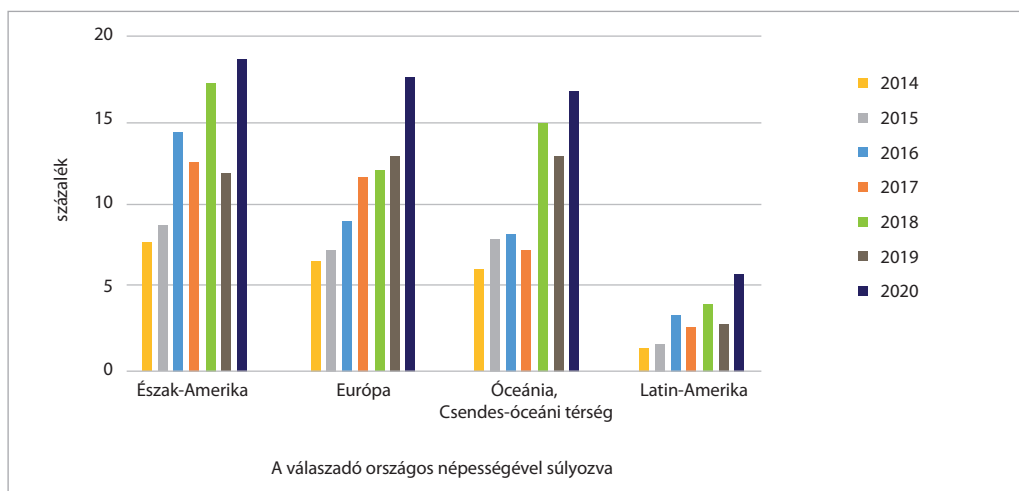


2. ábra: Különböző kábítószeres darknetes eladásából származó árbevétel országoként 2017 és 2018 között  
 Forrás: EMCDDA (2019): i. m. 71.

A megrendelések sok esetben azokból az országokból érkeznek, amelyekhez a market leginkább kötődik, valamint ahonnan a szereket a fogyasztóknak kiszállítják. Gyakori jelenség, amikor a market weboldalán a kereskedő megjelöli, hogy kizárólag mely országokba szállít, és melyekbe nem. Ez nem csoda, hisz a szállítás és a kézbesítés kockázatai csökkenthetők, ha nem kell határellenőrzéseken átjuttatni a küldeményt. A vásárlók körében már évek óta a kannabisz, az amfetaminszármazékok, az új pszichoaktív szerek és a kokain vezetnek a népszerűségi listán, miközben a heroin folyamatosan lemaradt a rangsorban. A heroin alacsony keresletének az egyik magyarázata, hogy a beszerzés hosszú és szövevényes útja miatt még a darkneten is drágább. Nem beszélve arról, hogy a heroin a leghatásosabb drogok közé tartozik, ezért sok helyütt alkalmasszerűen fogyasztják és rendelik meg. A másik magyarázat a heroinfogyasztók elképesztően rossz anyagi helyzetében, illetve az alacsony digitális képességeikben keresendő, ami a tisztító szer által kiváltott rossz fizikális és mentális állapotukhoz köthető. Ebből adódóan még alkalmasszerűen sem képesek a darkneten keresztül jobb minőségű anyagokat vásárolni. Számukra marad a rossz minőségű és drágább szerek utcai értékesítése. A kábítószeres internetes rendeléséből az ázsiai országok sem maradnak ki, bár ezek az államok a kábítószeres előállító országoként is működnek. Kétségtelenül igaz, hogy Kínában az internet szabályozottsága miatt a darknetes kereskedelem nemzetközi formája visszafogottabb. Ez a legfőbb oka annak, hogy a globális darknetes drogkereskedelemnek csak a 9%-a kötődik kínai webmarketekhez vagy rendelésekhez.<sup>8</sup> Ha mégis van internetes forgalom, akkor Kínából és más ázsiai országokból jellemzően nagyobb mennyiségben érkeznek rendelések, ami viszonteladói aktivitásra is utal. A darknet marketek száma globálisan

<sup>8</sup> UNODC (2020): i. m. 77.

nehezen meghatározható a jól lokalizálható nagyobb piacokon kívül. Ennek háttérében részben a Silk Road 2013-as bezárását követő fragmentálódás (*hydra effect*) áll, ami annyit jelent, hogy egy felszámolt vagy más okból bezárt nagyobb piac helyébe több kisebb market lépett.<sup>9</sup> Ilyenek voltak a titkosított csatornákkal működő és orosz nyelvű marketek vagy a singli piacok is, amelyeknek az egyik jellegzetessége, hogy nem minden esetben kötődnek a bünszervezetekhez.<sup>10</sup> A marketek számszerű emelkedése az online vásárlások lehetőségét is felélénkítette. A Global Drug Survey 2020-as eredményei szerint a darknetes kábítószer-vásárlás kedvezőbb körülményeinek köszönhetően az elmúlt hat évben az Amerikai Egyesült Államokban és Európában a vásárlók száma megháromszorozódott (3. ábra).



3. ábra: A darkneten kábítószereket vásárlók számának emelkedése 2014–2020 között az Amerikai Egyesült Államokban, Európában és más kontinensen

Forrás: UNODC (2020): i. m. 77.

Feltételezhetően ugyanebből az okból azok, akik korábban már vásároltak kábítószereket az interneten, a szerek fajtájából kezdtek többfélét kipróbálni. Fellendült azoknak a látogatóknak a részvétele is, akik korábban egyáltalán nem vásároltak kábítószereket sem online, sem offline. Ez utóbbiak az elmúlt két évben kezdték a tranzakciókat, és inkább csak alkalmoszerűen.<sup>11</sup> A kábítószerek és az illegális gyógyszerek internetes vásárlását erőteljesen meghatározza a surface weben történő kereskedés is. Az elérhető internetes hálózatokon a közösségi oldalak a mai napig jelentős szerepet töltenek be a szerek népszerűsítésében és vásárlásuk megszervezésében. A nagymértékű emelkedést az okostelefonokra letölthető alkalmazások általi könnyű elérhetőség támogatta,

<sup>9</sup> EMCDDA (2019): i. m. 70.

<sup>10</sup> Monica J. Barratt – Jason A. Ferris – Adam R. Winstock: *Safer Scoring? Cryptomarkets, Social Supply and Drug Market Violence*. *International Journal of Drug Policy*, 35. (2016). 24.

<sup>11</sup> UNODC (2020): i. m. 78.

bár a titkos kommunikáció garanciái ebben az esetben nem mindig érvényesülnek. A közösségi oldalak közül a népszerű Facebookot, Instagramot és a Twittert használják erre a célra (például a közösségi platformok nagyon népszerűek Dániában, Izlandon és Svédországban). Nyilvánvaló, hogy a heterogénebb összetételű és számszerűségében is bővülő vásárlói kör az internetes kábítószer-kereskedelem működését stabilizálja, viszont emellett szofisztikáltabb működést és megbízhatóbb biztonsági garanciákat követel a feketekereskedelmet lebonyolító platformok adminisztrátoraitól és kereskedőitől (például további fizetési, kézbesítési, árminőségi, eladói garanciákat biztosító faktorok meglétét vásárlási alapfeltételként). Az internetes drogvásárlás egyik alappillére a vásárlói kereslet, ezért az illegális adásvétel csökkentésére jó megoldás lehet a *bizalmi kapcsolatok befolyásolása*. Ennek első lépése a vásárlók attitűdjeinek megismerése, pontosabban a vevők által prioritásként kezelt bizalmi garanciák rendszerének, valamint az offline-online terek közti választásuk okainak feltérképezése. Ebben az esetben először arról a társadalmi csoportról lehet szó, akik az offline környezetben kevésbé, de az internetes környezetben nyújtott lehetőség által nagyobb eséllyel szánják rá magukat a kábítószeres és az illegális gyógyszerek vásárlására, viszont a vásárlási szándékuk még visszafordítható. Az attitűdök felméréséből származó eredményekre épülő megelőzés jellegű intézkedéseket már nemcsak egy körülhatárolható korosztály tekintetében lehet és célszerű alkalmazni, hanem olyan társadalmi közösségek körében is, amelynek tagjai még nem tartoznak ebbe a korosztályba.

A bizalomra épülő vásárlói attitűdök feltárásának első lépéseként a Nemzeti Közszolgálati Egyetem Eötvös József Kutatóközpont Kiberbiztonsági Kutatóintézetében 2020 januárjában egy 12 hónapos kvantitatív kutatást indítottunk, és tárgyának középpontjába a mindennapi életszituációkban rejlő *individuális* vagy *társadalmi* pressziókból felépülő vásárlói bizalmat helyeztük. Jelen tanulmányunk első részében az internetszabályozást, az online teret érintő kábítószer-kereskedelem színtereit, szereplőit és sajátosságait, a kiberdevianciák körében betöltött szerepét, motivációit és színtérmódosításait, valamint a kriptovaluták funkcióit mutatjuk be. Szintén a tanulmány első részében kitérünk a kábítószer-kereskedelem nemzetközi szabályozására, a kábítószer-kereskedelem interneten megjelenő büntetőjogi alakzataira, a darknet szabályozási dilemmáira, valamint az adásvételben megjelenő megosztott bizalom tényezőire. A tanulmány második felében az attitűdkutatás (első kutatási szakasz) részleteit és eredményeit taglaljuk, végül az eredmények hasznosíthatóságát és a további két kutatáshoz való kapcsolódását részletezzük.

Vákát

## Internetszabályozás

### Modellek

Az elmúlt évtizedek ugrásszerű technológiai fejlődése és új vívmányai nemcsak újabb és újabb kihívások elé állítják a társadalmakat és az országokat, de egyúttal új lehetőségeket is teremtenek az államok közötti versengésben. Az új technológiák átvétele, szabályozásának megalkotása előnyhöz juttattja azokat, akik az elsők között teszik ezt meg: az innováció, a tehetség és a rugalmasság kiemelkedően fontossá váltak a 21. század elején.<sup>1</sup> Az államok egyik legfontosabb feladata, hogy az új technológiák alkalmazásának lehetővé tétele mellett azok biztonságosságáról is gondoskodjanak.<sup>2</sup> A kibertér, a digitális technológiák szabályozása az államok közötti versengés egyik színterévé vált, ahol két eltérő modell alakult ki: a minden érdekelt fél bevonását hirdető irányzat a nyugati államokban, valamint a nemzeti szuverenitás alapján álló irányzat más országokban, elsősorban Oroszországban és Kínában.<sup>3</sup> Ezek között a fő különbség az, hogy míg az előbbi rendszerben a nem állami szereplők (például az internetszolgáltatók) szerepe jelentős a szabályozás alakításában mind nemzeti, mind nemzetközi szinten, addig utóbbi megoldás kizárólagosan az államok által hozott szabályozás betartásában juttat szerepet nekik.

Az eltéréseknek számos különböző oka lehet a gazdasági érdekektől kezdve az eltérő politikai kultúrán át a történelmi-ideológiai hagyományokig. Az európai államok által favorizált modell mögött például felfedezhető az az európai történelmi gyökerekhez visszahúzó törekvés, hogy egyfajta „erényes polgári térnek” őrizze meg az internetet, amelyet az erényes viselkedés, az udvariasság és az óvatosság jellemez. Az Amerikai Egyesült Államok politikai kultúrája ettől teljesen eltérő, nagy fokú szabadságon alapul, ahol kevés dolog korlátozza az innovációt, amíg az nem okoz bizonyíthatóan károkat, és csak ezután lép fel ellene.<sup>4</sup> Míg sokáig az Egyesült Államok volt a minden érdekelt fél részvételével működő modell globális zászlóvivője, napjainkra az Európai Unió szabályozása is egyre inkább az univerzalizmus felé mutat. Ennek egyik ékes példája a 2016/679 általános adatvédelmi rendelet (GDPR), amely az Európán kívül működő vállalkozások esetén is elvárja az európai szabályozáshoz való konformitást. Ebben

<sup>1</sup> Peter Engelke: *Three Ways the Fourth Industrial Revolution is Shaping Geopolitics*. *World Economic Forum*, 2018. augusztus 24.

<sup>2</sup> Frederick Douzet: Geopolitika a kibertér megértéséhez. In Pintér István (szerk.): *Műhelymunkák: A virtuális tér geopolitikája*. Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016. 29–30.

<sup>3</sup> Dornfeld László: A kibertér főbb nemzetközi és nemzeti szabályozásai. In Pintér István (szerk.): *Műhelymunkák: A virtuális tér geopolitikája*. Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016. 78.

<sup>4</sup> Kleron O'Hara – Dame W. Hall: *Four Internets. The Geopolitics of Digital Governance*. *CIGI Papers*, (2018), 206. 6–7.



fontos tényező az, hogy az EU együttesen túlságosan is nagy piacot jelent ahhoz, hogy az óriás amerikai számítástechnikai cégek figyelmen kívül hagyják az új szabályozást.<sup>5</sup>

Ugyanakkor az EU más területeken nem tudott hasonló sikereket elérni, például a 2017-ben benyújtott online magánéletet védő rendeletervezetet mind a mai napig nem sikerült elfogadni az EU-szervek és a tagállamok eltérő álláspontjai, belső vitái miatt.<sup>6</sup> Mint az iratokból kiderült, jelentős technológiai vállalatok – így például az Amazon is – aktív lobbitevékenységet folytattak a javaslat ellen.<sup>7</sup> Chris Painter, egykori vezető amerikai kiberdiplomata szerint úgy tűnik, hogy saját belső problémái és a nagy technológiai vállalatok hatalmas befolyása miatt az Egyesült Államok még jó ideig nem lesz képes visszanyerni sokáig élvezett globális vezető szerepét.<sup>8</sup>

Ezzel szemben áll Oroszország és Kína modellje, amely kizárólag a nemzeti szuverenitáson alapul. Ebben sokszor a legmagasabb szinteken érdekeltek: az ITU 2012-es világkonferenciáját megelőzően, 2011 júniusában Vlagyimir Putyin orosz elnök például kijelentette, hogy országának célja az, hogy a szervezeten keresztül nemzetközi irányítás alá vonja az internetet.<sup>9</sup> Kína esetében a változtatás iránti igény abból ered, hogy az ország globális normakövető helyett inkább globális normaalkotó kíván lenni. A kínai érdek az, hogy a kibertér felől az ország jelenlegi politikai berendezkedését és a nemzetbiztonságot érő fenyegetéseket ellenőrizni tudják.<sup>10</sup> Ez a politikai alapú szembenállás a jelenleg uralkodó nyugati modellel szemben számos dokumentumban testet öltött, amelyeket Oroszország és Kína közösen készített el, és tárt a nemzetközi közösség elé, ám ezek inkább politikai deklarációnak tekinthetők, semmint valós szakmai dokumentumoknak.<sup>11</sup> A szembenállás politikai céljait hangsúlyozza, hogy Donald Trump amerikai elnök konfrontatív Kína-politikájának – amely a kereskedelmi háborúban öltött testet – szerves részét képezte a kínai technológiai cégek és befolyás elleni fellépés a kiberkémkedés vádjával. Ennek egyik fő célpontja a Huawei cég volt, amely az okostelefon-piac mellett nyugati országok 5G hálózati rendszereinek kiépítésében is szerepet vállalt. Amerikai nyomásra az Egyesült Királyság végül megszakította az együttműködést a céggel.<sup>12</sup> Ahogy az EU–USA viszonyban, a Kína–Oroszország együttműködésben is vannak

<sup>5</sup> O'Hara–Hall (2018): i. m. 7.

<sup>6</sup> Az Európai Parlament és a Tanács rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet) 2017/0003 (COD).

<sup>7</sup> Vincent Manancourt: [Amazon Sought to Water down Eu Privacy Rules, Document Shows](#). *Politico*, 2020. december 20.

<sup>8</sup> Eric Geller: [China, EU Seize Control of the World's Cyber Agenda](#). *Politico*, 2018. július 22.

<sup>9</sup> André Barrinha: [Virtual Neighbors: Russia and the EU in Cyberspace](#). *Insight Turkey*, 20. (2018), 3. 37.

<sup>10</sup> Greg Austin: International Legal Norms in Cyberspace. Evolution of China's National Security Motivations. In Anna-Maria Osula – Henry Røigas (szerk.): *International Cyber Norms. Legal, Policy & Industry Perspectives*. Tallinn, CCDOE, 2018. 172.

<sup>11</sup> Dornfeld László: A kibertér szabályozási modelljei Európában. In Antalík Imre (szerk.): *Térrerő – Erőtér: Tanulmányok a Kárpát-medencei geopolitikai konferencia előadásaiból*. Komárno, Selye János Egyetem, 2019b. 44–48.

<sup>12</sup> A 2020. november végén elfogadott telekommunikáció-biztonsági törvény effektíve megtiltotta a Huawei részvételét az 5G hálózat kiépítésében és működtetésében, és 2027-ig előírta minden Huawei eszköz kiiktatását az egész kiépített rendszerből.

ellentétek. Míg a pekingi vezetés politikájának legfőbb célja az internet uralása, addig az orosz motivációkat illetően akad olyan vélemény, amely szerint csupán eszköznek tekintik azt a Nyugattal szemben. Az érvelés szerint az oroszok nem azért támadják a fennálló szabályozási status quót, mert új rendszert szeretnének, hanem hogy a kialakuló káoszt és szabályozatlanságot saját dezinformációs tevékenységükre használhassák fel.<sup>13</sup>

### Büntetőjogi szabályozás

Az internetszabályozás számos fontos biztonsági kérdése közül kiemelkedik a büntetőjogi szabályozás harmonizációjának problémája. Az eltérő kulturális és történelmi gyökerek miatt szinte minden állam büntetőjogi rendszere különbözik a többitől. A harmonizáció kérdése az Európai Unió szintjén is igen nagy ellenérzéseket szült, mivel a büntetőjogot a tagállamok szuverenitásuk utolsó védőbástyájaként hajlamosak kezelni. Ezért csak nagyon lassan halad a szabályozás, annak ellenére is, hogy a kiberbűnözés jelentette globális probléma egységes fellépést kíván a résztvevőktől. A rossz szabályozás nemcsak bizonyos cselekmények büntethetőségét érinti, de sok esetben a megindult eljárások során sem lehet beszerezni a külföldön található bizonyítékokat.

Az elmúlt évtizedekben több nagy jelentőségű dokumentum született, ám szinte mind csak regionális szinten. Ezek közül kiemelkedik és alapidokumentumnak tekinthető az Európa Tanács 2001-ben elfogadott számítástechnikai bűnözés elleni egyezménye (a budapesti egyezmény),<sup>14</sup> amelyet mintegy harminc ország írt alá, köztük olyan Európán kívüli országok is, mint az Amerikai Egyesült Államok, Japán, Kanada és a Dél-afrikai Köztársaság. Az egyezmény közös minimumot határoz meg a kiberbűnözés elleni fellépésben, és egyaránt tartalmaz anyagi jogi és eljárásjogi szabályokat is. Az EU már számos alkalommal elismerte az egyezmény jelentőségét, arra buzdítva a még nem részes tagállamait, hogy mihamarabb csatlakozzanak hozzá.<sup>15</sup> Napjainkra ez a szám tovább nőtt: 68 ország írta alá az egyezményt, és ebből 65 ratifikálta is azt. Közöttük olyan államok is, amelyek nem tagjai az egyezményt létrehozó Európa Tanácsnak, mint a Fülöp-szigetek, Izrael, Paraguay és Ausztrália.<sup>16</sup> Számos előnye mellett azonban a hibáit is meg kell említeni: sok esetben kerülték a megalkotók az egységes fogalmak használatát, a benne található büntető-eljárásjogi eszközök pedig igen korlátozottak. Mindezek ellenére kijelenthetjük, hogy a nyugati világban az egyezmény a szabályozás alapjává vált.

<sup>13</sup> O'Hara–Hall (2018): i. m. 11.

<sup>14</sup> Az Európa Tanács Budapest, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye (ETS No. 185). Kihirdette az Európa Tanács Budapest, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről szóló 2004. évi LXXIX. törvény.

<sup>15</sup> Laviero Buono: *Gearing Up the Fight Against Cybercrime in the European Union. A New Set of Rules and Establishment of the European Cybercrime Centre (EC3)*. *New Journal of European Criminal Law*, 3. (2012), 3–4. 336.

<sup>16</sup> *Council of Europe Chart of signatures and ratifications of Treaty 185*. Council of Europe.