

INTERJÚ

Interjú Elena Martellozzóval, az Edinburghi Egyetem intézetigazgatójával és kriminológia professzorával

**Interview with Elena Martellozzo, Institute Director
and Professor of Criminology at the University of Edinburgh**

Szabó Csaba

Dr., PhD, főszerkesztő-helyettes, egyetemi docens, rendőr alezredes
Belügyminisztérium,
Belügyi Szemle Szerkesztősége
Széchenyi István Egyetem,
Deák Ferenc Állam- és Jogtudományi Kar
csaba.szabo3@bm.gov.hu



A szerző a kéziratot magyar nyelven nyújtotta be. Benyújtás: 2025. 04. 17. Átdolgozás: 2025. 04. 30. Elfogadás: 2025. 05. 08.

Absztrakt

Elena Martellozzo kriminológus professzor, az Edinburgh Egyetem Globális Gyermekbiztonsági Intézet igazgatója két évtizede végez úttörő kutatásokat a kiberbűnözés, az online gyermekvédelem és a digitális rendészet területén. Tudományos munkásságának középpontjában a gyermekek online kizsákmányolása elleni küzdelem, az elkövetői magatartás feltérképezése, valamint a mesterséges intelligencia és a big data etikus alkalmazása áll. Interjúnkban beszél a kiberbűnözés természetének átalakulásáról, a digitális rendvédelem új eszközeiről – különös tekintettel a fedett online nyomozásra –, valamint arról, hogyan lehet a kutatási eredményeket közvetlenül beépíteni a rendészeti gyakorlatba és a szakpolitikai döntéshozatalba. Professzor asszony elkötelezett abban, hogy tudományos tevékenysége ne csupán elméleti szinten hasson, hanem valódi társadalmi változások előmozdítója legyen – különösen a gyermekek online térben történő védelme érdekében..

Kulcsszavak: kiberbűnözés, online gyermekvédelem, fedett nyomozás, mesterséges intelligencia

Abstract

Professor Elena Martellozzo, a criminologist and Director of the Global Child Safety Institute at the University of Edinburgh, has been conducting pioneering research for two decades in the fields of cybercrime, online child protection, and digital policing. Her academic work focuses on combating the online exploitation of children, mapping offender behaviour, and promoting the ethical application of artificial intelligence and big data. In our interview, she discusses the transformation of cybercrime, the new tools of digital law enforcement—particularly undercover online investigations—as well as how research findings can be directly integrated into policing practices and policy-making. Professor Martellozzo is committed to ensuring that her scientific work has an impact beyond theory, serving as a driver of real social change—especially in safeguarding children in the digital environment.

Keywords: cybercrime, online child protection, undercover investigation, artificial intelligence

Professzor asszony, ön évek óta kutatja a kiberbűnözést. Milyen változásokat figyelt meg az online bűnözés jellegében az elmúlt két évtizedben?

Több mint húsz éve dolgozom ezen a területen, és a kutatások, valamint a kulcsfontosságú intézmények által megosztott adatok alapján egyértelműen látható, hogy az online bűnözés jellege drámaian megváltozott – mind léptékében, mind összetettségében. Amikor elkezdtem a kiberbűnözést kutatni, az online fenyegetések többnyire a hekkeléssel, adathalászattal és kezdetleges csalásokkal voltak azonosíthatók. Azóta azonban a közösségi média, az okostelefonok, valamint az újabban megjelenő élményalapú technológiák, mint például a Metaverzum, jelentős változásokat hoztak.

Az egyik legfontosabb változás a kiberfenyegetések sokféleségének növekedése. Ma már a kiberbűnözés nemcsak pénzügyi csalásokat és adatlopásokat foglal magában, hanem kifinomult online visszaéléseket is, mint például a kiberzaklatás, az intim képekkel való visszaélés, vagy az élő közvetítésben elkövetett bántalmazás. A dark web illegális tartalmak piacterévé vált, ahol a névtelenséget kihasználva gyermekekkel szembeni szexuális kizsákmányolást is végeznek.

Ezek a technológiai fejlődések mozgékonyabbá és nehezebben nyomon követhetővé tették az elkövetőket.

Kiemelten foglalkozik a gyermekek és fiatalok online védelmével. Milyen új kihívások jelentek meg ezen a téren a technológia fejlődésével?

Jelentős elmozdulás figyelhető meg az online károkozásokkal kapcsolatos tudatosság terén, különösen a sérülékeny csoportokat, például a gyermekeket illetően. Ahogy a digitális hozzáférés bővült, úgy növekedtek a kockázatok is. Kutatásaim egyre inkább arra összpontosítanak, miként célozzák meg és használják ki a gyermekeket az online térben, valamint hogy mennyire sürgető a hatékony védelmi intézkedések és szakpolitikai beavatkozások bevezetése.

Hogyan hat a digitalizáció a rendészeti módszerekre, különösen a „kiberrendészet” területén? Mely technológiai megoldásokat tartja a legígéretesebbnek?

A digitalizáció gyökeresen átalakította a rendészeti módszereket, különösen a „kiberrendészet” területén. Ahogy a bűnözés egyre inkább az online térbe helyeződik át, a rendvédelmi szervek új stratégiákkal, eszközökkel és készségekkel kénytelenek alkalmazkodni az új típusú, gyakran határokon átnyúló, titkosított és mozgékony bűnözői magatartásokhoz.

Az egyik legfontosabb fejlemény a digitális fedett nyomozás térnyerése. Ahogy a hagyományos büntetőeljárás során beépített rendőrök kerültek be

a bűnszervezetekbe, úgy ma már online tereken – csetszobákban, dark webes piactereken, közösségimédia-felületeken – zajlik az operatív munka. A rendőrök elkövetőnek vagy vásárlónak kiadva magukat olyan bizonyítékokat gyűjtenek, amelyek másképp elérhetetlenek lennének. Ez különösen hatékony gyermekbántalmazás vagy emberkereskedelem esetén. Az ilyen bevételek speciális képzést és a jogszabályok szigorú betartását követelik meg, hogy a bizonyítékok felhasználhatók legyenek a bíróságon, miközben az alapvető jogokat is tiszteletben tartják.

Nemzetközi szervezetekkel és kormányokkal dolgozott együtt a gyermekek online védelmét célzó szakpolitikák kidolgozásában. Milyen tanulságokat vont le ezekből az együttműködések közül?

Nemzetközi szervezetekkel, kormányokkal és rendvédelmi szervekkel – köztük az Internet Watch Foundationnal (IWF), valamint brit és más országok rendőrségeivel – való együttműködésem során világos képet kaptam az online gyermekvédelem összetettségéről. Az egyik legmegdöbbentőbb tapasztalat az online visszaélések globális jellege. A gyermekekkel szembeni szexuális kizsákmányolás és visszaélés (child sexual exploitation and abuse – CSEA) nem ismer határokat, és az illegális tartalmak gyors terjedése a joghatóságok között súlyos kihívást jelent a bűnüldözés és a jogalkotás számára.

Az IWF-fel végzett közös munkám során első kézből láttam, milyen döntő szerepet játszik a technológia a visszaéléseket megjelenítő anyagok azonosításában és eltávolításában. Az alapítvány élvonalbeli eszközöket alkalmaz a gyermekbántalmazást ábrázoló tartalmak felismerésére, kategorizálására és törlésére, ezzel kulcsfontosságú szerepet játszva a kizsákmányoló hálózatok megzavarásában. Együttműködésünk során azt is világosan láthattam, mennyire elengedhetetlen a köz- és magánszféra összefogása: a technológiai cégeknek, civil szervezeteknek és állami hatóságoknak közösen kell fellépniük a káros tartalmak terjedésének hatékony megfékezéséhez.

Rendvédelmi szervekkel végzett kutatásaim rámutattak még a proaktív és fedett digitális nyomozás kiemelt jelentőségére. Első könyvemben – amely a Scotland Yard Magas Technológiai Bűnözés Elleni Egységének empirikus adataira épült – azt vizsgáltam, hogyan készítik elő az elkövetők az áldozattal való szexuális visszaélést. Az online térben folytatott fedett műveletek ma már kulcsfontosságú eszközei a rejtett közösségek feltérképezésének, ahol az elkövetők gyakran anonim módon működnek. Ezek a bevételek elengedhetetlenek a hírszerzéshez és a szervezett hálózatok szétzúzásához, még mielőtt azok további kárt okoznának.

Az évek során újra és újra visszatérő tanulság, hogy a gyermekek online kizsákmányolásának kezelése csakis áldozatközpontú megközelítéssel lehet

hatékony. A rendőrséggel folytatott közös munkában gyakran hangsúlyt kaptak azok a felismerések, amelyek szerint a gyermekeket minden egyes megtekintés vagy megosztás újra traumatizálja. Ez a tudás még sürgetőbbé teszi a tartalmak gyors eltávolítását és a hosszú távú pszichológiai támogatás biztosítását.

Kutatásaiban hogyan biztosítja, hogy eredményei ne csak az akadémiai közösséget szolgálják, hanem a gyakorlatban is hasznosuljanak? Milyen stratégiákat alkalmaz annak érdekében, hogy szélesebb körben is ismertté váljanak kutatási eredményei?

Pályafutásom során mindig is arra törekedtem, hogy a kutatásaim ne csupán tudományos ismereteket gyarapítsanak, hanem a valóságban is érezhető hatást gyakoroljanak. Ezt egy többrétegű megközelítéssel érem el, amely összeköti az akadémiai világot a gyakorlati alkalmazással.

Az egyik legfontosabb módszerem, hogy közvetlen kapcsolatot építek ki iskolákkal és szülőkkel. Rendszeresen tartok workshopokat és szemináriumokat tanárok, szülők és fiatalok számára az online biztonság, a kiberzaklatás és a digitális ellenállóképesség témájában. Ezek az alkalmak arra szolgálnak, hogy a komplex kutatási eredményeket közérthető, könnyen alkalmazható stratégiákká alakítsuk. Például az online zaklatásról és digitális kockázatokról szóló munkáimat gyakorlati útmutatóvá formálom, amelyet a szülők felhasználhatnak gyermekeik védelmében, a pedagógusok pedig beépíthetnek a digitális írástudás fejlesztésére irányuló programokba.

A rendvédelmi szervekkel való együttműködésem – mind az Egyesült Királyságban, mind nemzetközi szinten – biztosítja, hogy kutatásaim közvetlenül hozzájáruljanak a kiberrendészet és a gyermekvédelem fejlesztéséhez. Szoros együttműködésben dolgoztam ki képzési programokat, amelyek segítik az online fenyegetések felismerését, az elkövetői viselkedés megértését és a fedett digitális műveletek támogatását. Ez a gyakorlatorientált megközelítés lehetővé teszi, hogy a rendőrök valós idejű nyomozások során közvetlenül alkalmazzák a kutatási eredményeket, így biztonságosabbá téve a digitális környezetet a sérülékeny felhasználók számára.

Lehetőségem volt kormányokat és nemzetközi szervezeteket is tanácsokkal ellátni – többek között a brit Belügyminisztériumot, az Európai Nemek Közötti Egyenlőségi Intézetet (EIGE), a finn és a bahreini kormányt, valamint gyermekvédelmi szervezeteket Olaszországban – az online biztonságot szolgáló hatékony szakpolitikai intézkedések kidolgozásában. E szakpolitikai tevékenységem során az aktuális kutatási eredmények szolgálnak alapul a jogalkotás számára, így biztosítva, hogy a törvényi keretek tükrözzék a legújabb tudományos

ismereteket. Tapasztalataim alapján a kutatás és a szakpolitika közötti szoros kapcsolat eredményesebb szabályozást eredményez, amely jobban védi a gyermekeket és a sérülékeny csoportokat az online térben.

Miközben a tudományos publikálás továbbra is fontos, ugyanilyen elkötelezett vagyok a nyilvánosság tájékoztatása és a közösségi szerepvállalás iránt. Rendszeresen részt veszek szakértői panelbeszélgetéseken, nemzetközi konferenciákon és közéleti vitákon, ahol a jobb online védelmi intézkedések mellett érvelek. Ezek a nyilvános fellépések segítenek szélesebb körű társadalmi tudatosságot teremteni a digitális kockázatokkal kapcsolatban.

Végül digitális platformokat is aktívan használok a kutatási eredmények szélesebb körű terjesztésére. Online webinariumok, oktató videók és a közösségi média révén globális közönséget tudok megszólítani gyorsan és hatékonyan.

Célom az, hogy a kutatás ne rekedjen meg az akadémiai folyóiratok hasábjain, hanem élő, gyakorlati erőforrássá váljon, amely megerősíti a közösségeket, formálja a szakpolitikát, és hatékonyabb védelmi intézkedéseket tesz lehetővé a digitális térben.

Milyen szerepet játszik a mesterséges intelligencia és a big data az online bűnözés megelőzésében és feltárásában? Lát-e etikai aggályokat e technológiákkal kapcsolatban?

A mesterséges intelligencia (MI) és a big data napjainkra kulcsszereplővé váltak az online bűnözés megelőzésében és feltárásában, alapvetően átalakítva a digitális rendszert és a gyermekvédelem területét. Rendvédelmi szervekkel és nemzetközi partnerekkel végzett munkám során első kézből tapasztaltam meg, hogy ezek a technológiák jelentősen növelik a képességeinket az újonnan felbukkanó kiberfenyegetések észlelésére, elemzésére és kezelésére.

Az MI-alapú eszközök mára központi szerepet töltenek be a bűnözői magatartásminták azonosításában olyan adatmennyiségekben, amelyeket emberi nyomozók nem tudnának manuálisan feldolgozni. Például a gépi tanuláson alapuló algoritmusok képesek gyorsan elemezni több millió online interakciót, hogy azonosítsák az online csábítás, az emberkereskedelem vagy a gyermekek sérelmére elkövetett szexuális visszaélések (child sexual abuse material – CSAM) terjesztésének jeleit. Az olyan szervezetek, mint az IWF, MI-t alkalmaznak a visszaélést tartalmazó képek gyors átvizsgálására és besorolására, így csökkentve az áldozatok kitettségét, és elősegítve a tartalmak mielőbbi eltávolítását.

A big data elemzések lehetővé teszik a prediktív rendszert alkalmazását is: a korábbi bűnesetek adatainak elemzésével előre jelezhetők azok az online felületek, ahol megnő a bűncselekmények kockázata. Ez lehetőséget ad a hatóságoknak

arra, hogy proaktívan figyeljék a web azon rejtett részeit is, mint a dark web, ahol gyakran titokban szerveződnek illegális tevékenységek.

Az MI emellett tovább erősíti a digitális fedett nyomozást is, amelyet kiemelten kutattam. Fejlett algoritmusok segítik a nyomozókat a titkosított kommunikációs csatornák és rejtett fórumok feltérképezésében, ahol kiberbűncselekményeket és kizsákmányolást szerveznek. Ez növeli az akciók hatókörét és hatékonyságát, különösen a szervezett bűnözői hálózatokkal szemben.

Ugyanakkor számos etikai aggály is felmerül. A legfontosabb a magánszféra és a megfigyelés kérdésköre. A bűnmegelőzési célú adatelemzések könnyen elmoshatják a határt a biztonság és a magánélet védelme között. Fennáll a túlzott megfigyelés veszélye, különösen akkor, ha az adatgyűjtés nem célzott vagy nem átlátható. Emellett figyelmet kell fordítanunk az emberi ellenőrzés szerepére is: bár az MI kivételes gyorsasággal dolgozza fel az adatokat, az értelmezéséhez emberi belátás és etikai mérlegelés szükséges. A technológia jelezheti a kockázatot, de a döntéseket felelősségteljes emberi megítélésre kell alapozni.

Meggyőződésem, hogy a kulcs egy kiegyensúlyozott megközelítésben rejlik: az MI és a big data képességeit csakis szilárd etikai irányelvekkel, szigorú ellenőrzési mechanizmusokkal és világos jogi keretekkel együtt szabad alkalmazni. Az IWF-hez hasonló szervezetekkel, a rendvédelmi szervekkel és a nemzetközi szakpolitikai döntéshozókkal való együttműködés elengedhetetlen ezen normák kialakításához, hogy biztosítsuk a polgári szabadságjogok tiszteletben tartását, miközben hatékonyan védjük a digitális tér biztonságát.

Mely jövőbeli kutatási területeket tartja kulcsfontosságúnak az online károkozás és a digitális bűnözés visszaszorítása szempontjából? Hol látja a legnagyobb fejlődési potenciált?

Az online ártalmak és a digitális bűnözés visszaszorítása összetett feladat, amelyhez innovatív, jövőorientált kutatásokra van szükség. A kiberbűnözés, az online gyermekvédelem, valamint a nemzetközi rendvédelmi és szakpolitikai együttműködések területén szerzett tapasztalataim alapján úgy vélem, hogy több kulcsfontosságú kutatási irányt kell előtérbe helyezni, ha hatékonyan akarunk fellépni a digitális térben jelentkező új típusú fenyegetésekkel szemben.

Ahogy egyre inkább elmozdulunk az élményalapú digitális terek – például a Metaverzum, a kiterjesztett valóság (AR) és a virtuális valóság (VR) – irányába, úgy változik az online bántalmazás természete is. Jelenlegi kutatásom például a gyermekvédelem kérdését vizsgálja a Metaverzum kontextusában. Ezek a környezetek új típusú sebezhetőségeket hoznak magukkal, például valós

idejű online zaklatást, ellenőrizetlen élő interakciókat és virtuális visszaélés lehetőségét. A jövőbeli kutatásoknak ki kell dolgozniuk a megfelelő szakpolitikai kereteket, technológiai védelmi megoldásokat és etikai irányelveket annak érdekében, hogy a felhasználók – különösen a gyermekek – védelmet kapjanak ezekben a bővülő digitális terekben.

Ugyanilyen fontos a digitális írástudás és az ellenállóképesség fejlesztése. Bár a technológiai iparágak és a szakmai szervezetek sokat tehetnek, legalább ennyire fontos a felhasználók – különösen a gyermekek, szülők és pedagógusok – felkészítése arra, hogy biztonságosan tudjanak eligazodni az online térben. A digitális ellenállóképességre vonatkozó oktatási kutatások hozzájárulhatnak olyan képzési programok kidolgozásához, amelyek kritikai gondolkodásra, adatvédelemre és biztonságos online viselkedésre tanítanak. Ha ezek a tananyagok beépülnek az iskolai oktatásba és a közösségi programokba, hatékony eszközei lehetnek az online áldozattá válás megelőzésének.

Véleményem szerint a legnagyobb fejlődési potenciál abban rejlik, ha a mesterséges intelligenciát és a big datát felelősségteljes módon alkalmazzuk, és ezt nemzetközi együttműködéssel és robusztus digitális oktatási programokkal egészítjük ki. Ha sikerül egyensúlyt teremtenünk a technológiai fejlődés és az etikai elkötelezettség között, meggyőződésem, hogy jelentősen csökkenthetjük az online ártalmakat, és biztonságosabbá tehetjük a digitális világot, különösen a legsebezhetőbb felhasználók számára.

Interview with Elena Martellozzo, Professor of Criminology at Middlesex University

Professor, you have been researching cybercrime for many years. What changes have you observed in the nature of online crime over the past two decades?

I have been working in this arena for over two decades and it is clear, from research and data shared by key institutions that the nature of online crime has evolved dramatically, both in scale and complexity. When I first began researching cybercrime, online threats were mostly limited to hacking, phishing, and rudimentary forms of online fraud. However, the landscape has shifted with the rise of social media, smartphones, and more recently, immersive technologies like the Metaverse.

One of the most important changes I have observed is the diversification of cyber threats. Today, cybercrime includes not only financial scams and data breaches but also sophisticated forms of online exploitation, such as cyberstalking,

intimate image abuse, and live-streamed abuse. The dark web has become a marketplace for illicit activities, where anonymity is exploited to traffic illegal content, including child exploitation material.

These technological advancements have made cybercriminals more agile and harder to trace.

You focus extensively on the online protection of children and young people. What new challenges have emerged in this field with the advancement of technology?

A significant shift is the growing awareness of online harms against vulnerable populations, particularly children. As digital access has expanded, so too have the risks. My research has increasingly focused on how children are targeted and exploited online, and the critical need for robust safety measures and policy interventions to protect them.

How does digitalisation impact law enforcement methods, particularly in 'cyber policing'? Which technological solutions do you consider the most promising?

Digitalisation has transformed law enforcement methods, particularly in the realm of 'cyber policing'. As I explained, as crime increasingly migrates online, law enforcement agencies have had to adapt their strategies, tools, and skill sets to address a new breed of criminal behaviour that is often borderless, encrypted, and highly agile.

One major impact is the shift towards undercover digital policing. A particularly critical development has been the rise of undercover digital policing. In the same way that law enforcement has traditionally used undercover officers to infiltrate criminal networks, digital undercover operations now take place within chat rooms, dark web marketplaces, and social media platforms where criminal activities are coordinated. Officers, posing as buyers or fellow criminals, gather intelligence and evidence that would otherwise be inaccessible. This method has proven particularly effective in cases involving child exploitation, human trafficking. It requires highly specialised training and strict adherence to legal guidelines to ensure evidence is admissible in court and civil liberties are respected.

You have collaborated as an advisor with various international organisations and governments in developing online child protection policies. What insights have you gained from these collaborations?

My collaborations with international organisations, governments, and law enforcement agencies, including the Internet Watch Foundation (IWF) and

police forces in the UK and abroad, have provided me with a clear understanding of the complexities of online child protection. One of the most striking observations is the global nature of online abuse. Child sexual exploitation and abuse (CSEA) is not confined by borders, and the rapid dissemination of illegal content across jurisdictions poses many challenges for law enforcement and policymakers.

Working closely with the IWF, I have witnessed firsthand the crucial role that technology plays in identifying and removing abusive material. The IWF's use of cutting-edge tools to detect, categorise, and remove child sexual abuse imagery has been instrumental in disrupting networks of exploitation. Through this partnership, I have also seen how critical public-private collaboration is: technology companies, non-profits, and government agencies must work together to effectively combat the spread of harmful content.

My research with law enforcement has further highlighted the importance of proactive and undercover digital policing. My very first book, which collected empirical data from the High Technological Crime Unit at Scotland Yard, explored how offenders groom children to prepare for sexual abuse. Undercover operations online have become a powerful strategy to infiltrate hidden online communities, where offenders often operate anonymously. These covert investigations are vital for intelligence gathering and disrupting organised networks before further harm is inflicted.

Throughout these years what keep emerging is how important is to utilise a *victim-centered approach*. Much of my work with police forces has emphasised that children who are exploited online are often re-victimised each time content is shared or viewed. This understanding has reinforced the urgency of swift content removal and long-term psychological support for victims.

In your research, how do you ensure that your findings benefit not only the academic community but are also applied in practice? What strategies do you use to communicate your research results more widely?

Throughout my career, I have been committed to ensuring that my research not only contributes to academic knowledge but also has a tangible impact on real-world practices. Achieving this involves a multi-layered approach that bridges the gap between academia and frontline practice.

One of the primary ways I extend my research beyond academic circles is through direct engagement with schools and parents. I regularly conduct workshops and seminars aimed at educating teachers, parents, and young people about online safety, cyberbullying, and digital resilience. These sessions are designed

to translate complex research findings into practical strategies that can be easily understood and implemented. For example, my work on online grooming and digital risks is distilled into clear guidance that parents can use to protect their children and that teachers can integrate into digital literacy programs.

My collaboration with law enforcement agencies, both in the UK and internationally, ensures that my research is practically applied to enhance cyber policing and child protection strategies. I have worked closely with police forces to develop training programs that focus on identifying online threats, understanding offender behaviour, and supporting undercover digital operations. This hands-on approach allows officers to leverage research insights in real-time investigations, making the digital world safer for vulnerable users.

I have had the privilege of advising governments and international organisations, including the Home Office, the European Institute of Gender Equality (EIGE); the Finnish Government, The Government of Bahrain, and other child protection agencies in Italy, on creating robust online safety policies. This policy work is rooted in evidence-based research, ensuring that legislative frameworks are informed by the latest findings in cybercrime and online safety. My experience has shown that bridging the gap between research and policy leads to more effective regulations that protect children and vulnerable groups online.

While academic dissemination remains important, I am equally committed to engaging in public forums, media discussions, and community events. I frequently contribute to expert panels, international conferences, and public debates to advocate for better online protection measures. This public engagement helps to raise awareness and influence broader societal understanding of digital risks.

Finally, I leverage digital platforms to disseminate findings more broadly. Online webinars, educational videos, and social media engagements allow me to reach a global audience quickly and effectively.

My goal is to ensure that research is not confined to academic journals but becomes a living, practical resource that empowers communities, informs policy, and strengthens protective measures in the digital world.

What role do artificial intelligence and big data play in preventing and uncovering online crime? Do you see any ethical concerns associated with these tools?

Artificial intelligence and big data have become key in both preventing and uncovering online crime, fundamentally transforming the landscape of digital policing and child protection. In my work with law enforcement agencies and international partners, I have witnessed firsthand how these technologies enhance our ability to detect, analyse, and respond to emerging cyber threats.

AI-driven tools are now central to identifying patterns of criminal behavior in vast datasets that would be impossible for human investigators to process manually. For example, machine learning algorithms can swiftly analyse millions of online interactions to detect indicators of grooming, trafficking, or the distribution of child sexual abuse material (CSAM). Platforms like the Internet Watch Foundation (IWF), with whom I have collaborated, leverage AI to scan and classify abusive content rapidly, reducing exposure and facilitating quicker takedowns.

Big data analytics also enable predictive policing, where historical crime data is analysed to anticipate potential hotspots for online offenses. This allows law enforcement to proactively monitor high-risk areas of the web, including hidden spaces on the dark web where illicit activities are often concealed.

Furthermore, AI enhances undercover digital policing, a field I have researched extensively. Advanced algorithms can help undercover officers navigate encrypted communication channels and identify hidden forums where exploitation and cybercrime are orchestrated. This increases the scope and efficiency of operations targeting organised cybercriminal networks.

I seen a number of ethical concerns. While AI and big data offer powerful tools for combatting online crime, they also present ethical challenges that must not be overlooked. The most important is Privacy and Surveillance. The widespread use of data analytics for crime prevention can blur the lines between security and privacy. There is always a risk of overreach, where constant monitoring infringes on individual rights, particularly if data collection is indiscriminate or lacks transparency. There is also the risk of **human oversight**. We know that AI can process data at extraordinary speeds, the interpretation of its findings must always involve human oversight. Technology can flag risks, but contextual understanding and ethical judgment are crucial in determining the next steps.

In my view, the key lies in a balanced approach, embracing the capabilities of AI and big data while embedding strong ethical guidelines, rigorous oversight, and clear legal frameworks. Collaborations with organisations like the IWF, law enforcement, and international policymakers are crucial to setting standards that protect civil liberties while ensuring robust digital safety measures.

What future research areas do you consider crucial for reducing online harm and digital crime? Where do you see the greatest potential for advancement?

Reducing online harm and digital crime is a multifaceted challenge that requires innovative, forward-thinking research. Based on my work in cybercrime, online

child protection, and collaborations with international law enforcement and policy-makers, I believe several critical research areas must be prioritised to effectively tackle emerging threats in the digital landscape. For example, as we move towards more immersive digital experiences like the **Metaverse**, augmented reality (AR), and virtual reality (VR), the nature of online harm is evolving. My current work on child safeguarding in the Metaverse highlights that these environments introduce new vulnerabilities, such as real-time grooming, unmonitored live interactions, and the potential for virtual abuse. Future research must explore policy frameworks, technological safeguards, and ethical guidelines to protect users, particularly children, in these expansive digital spaces.

Digital Literacy and Resilience Building is also important. There much organisations and the tech industry can do, but empowering users with the knowledge and skills to navigate online spaces safely is equally fundamental, particularly children, parents, and educators. Research into digital resilience education can inform the development of effective training programs that teach critical thinking, privacy protection, and safe online behaviors. Integrating these lessons into school curricula and community outreach initiatives can serve as a preventive measure against online victimization.

Ultimately, In my view, the greatest potential for advancement lies in harnessing AI and big data responsibly, coupled with international cooperation and robust digital literacy programs. If we can achieve a balance between technological innovation and ethical integrity, I believe we can reduce online harm and make digital spaces safer for everyone, especially vulnerable populations.

A cikk APA szabály szerinti hivatkozása

Szabó Cs. (2025). Interjú Elena Martellozzóval, az Edinburghi Egyetem intézetigazgatójával és kriminológia professzorával. *Belügyi Szemle*, 73(7), 1555–1567. <https://doi.org/10.38146/BSZ-AJIA.2025.v73.i7.pp1555-1567>