Kaznenopravni aspekti krađe identiteta

Bingula, Patricia

Pravni fakultet u Zagrebu

Katedra za kazneno pravo

Patricia Bingula

KAZNENOPRAVNI ASPEKTI KRAĐE IDENTITETA

Diplomski rad

Mentor: izv. prof. dr. sc. Aleksandar Maršavelski

Zagreb, srpanj 2024.

Izjava o izvornosti

Ja, Patricia Bingula, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključiva autorica diplomskog rada/završnog rada te da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristila drugim izvorima do onih navedenih u radu.

Patricia Bingula

SADRŽAJ

SAŽETAK

Cilj ovog rada je sveobuhvatno obraditi fenomen krađe identiteta s naglaskom na njezine kaznenopravne aspekte kroz prizmu relevantnih odredbi Kaznenog zakona. Rad će detaljno analizirati različite metode i pojavne oblike krađe identiteta, uključujući tradicionalne i suvremene oblike putem Interneta i računalnih sustava. Posebno će se istražiti zakonsko uređenje krađe identiteta i srodnih zločine kako u okviru Europske Unije, tako i u kontekstu ključnih međunarodnih propisa. Kroz rad će biti prikazani i statistički podaci vezani uz krađu identiteta, kao i kaznena djela nedozvoljene uporabe osobnih podataka i zlouporabe osobne isprave. Konačno, bit će iznesen primjer iz sudske prakse koji ilustrira praktičnu primjenu kaznenopravnih normi u slučajevima krađe identiteta u Hrvatskoj.

Ključne riječi: krađa identiteta, *skimming*, *phishing*, Kazneni zakon, nedozvoljena uporaba osobnih podataka, zlouporaba osobe isprave, sekundarna kaznena djela

ABSTRACT

The aim of this paper is to comprehensively address the phenomenon of identity theft, with a focus on its criminal law aspects through the lens of relevant provisions of the Criminal Code. The paper will provide a detailed analysis of various methods and manifestations of identity theft, including both traditional and modern forms via the Internet and computer systems. Special attention will be given to the legal regulation of identity theft and related crimes both within the European Union and in the context of key international regulations. The paper will also present statistical data related to identity theft, as well as criminal offenses involving the unauthorized use of personal data and the misuse of personal documents. Finally, an example from case law will be presented to illustrate the practical application of criminal law norms in cases of identity theft in Croatia.

Keywords: identity theft, *skimming*, *phishing*, Criminal Code, unauthorized use of personal data, misuse of personal documents, secondary criminal offenses

1. Uvod

U današnjem digitalnom dobu, krađa identiteta postala je alarmantna stvarnost i jedan je od najznačajnijih i najbrže rastućih oblika kaznenih djela tzv. „bijelih ovratnika“[1] *(*eng. *white-collar crime*), odnosno „umnih radnika“[2], u suvremenom društvu. Počinjenje ovog kaznenog djela posljednjih je godina nanijelo milijunske štete fizičkim i pravnim osobama, dok stručnjaci procjenjuju da neotkriveni slučajevi (tzv. „*tamne brojke*“[3]) na globalnoj razini prelaze vrijednost od nekoliko milijardi dolara. Tijekom 2012. godine, američko gospodarstvo pretrpjelo je gubitak od oko 24,7 milijardi dolara, britansko oko 1,3 milijarde funti godišnje, dok Južna Afrika godišnje pretrpi gubitak od oko 1 milijardu randa.[4]

U svojoj suštini, krađa identiteta podrazumijeva neovlašteno korištenje osobnih podataka pojedinca, bez znanja ili pristanka te osobe, a najčešće s ciljem stjecanja materijalne ili neke druge koristi. Posljedice krađe identiteta nisu samo financijske nego i emocionalne prirode, jer žrtve često prolaze kroz dugotrajan i stresan proces vraćanja svog identiteta i popravljanja štete.

Kada se raspravlja o krađi identiteta, potrebno je razlikovati sociološki i filozofski pojam „identiteta“, koji se koristi za opis skupa karakteristika koje čine identitet osobe, od samog cilja krađe identiteta.[5] Osobni identitet je temeljna vrijednost svake osobe, zasnovana na ideji o jedinstvenosti iste, dok su cilj krađe identiteta identifikacijski, odnosno osobni podaci. S pomoću

---

[1] Hoofnagle, Crhis Jay, Identity Theft: Making the Known Unknown Known, Harvard Journal of Law & Technology, Volume 21, Number 1 Fall 2007: https://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech097.pdf, 4. srpnja 2024., str.98.
[2] Dragičević, Dražen et al., Pravna informatika i pravo informacijskih tehnologija, Narodne novine, Zagreb, listopad 2015., str. 52.
[3] Broj realiziranih kažnjivih ponašanja za koja se ne zna, zato što nisu otkrivena.
[4] Cassim, F., Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?, 2015, vol 28. n.2: https://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812015000200003#top_fn20, 4. srpnja 2024.,
[5] Gercke, Marko, Internet-related Identity Theft, Project on Cybercrime, Council of Europe, November 2007: https://rm.coe.int/16802fa3a0, 4. srpnja 2024., str. 18

osobnih podataka, kao što su ime, datum rođenja, broj osobne iskaznice ili podaci o kreditnoj kartici, obavljaju se svakodnevne aktivnosti poput kupnje roba ili usluga, otvaranja bankovnih računa, sklapanja ugovora s telefonskim kompanijama ili podizanja kredita. Ti podaci se koriste i za pristup različitim računima i sustavima evidencije u financijskim institucijama, zdravstvenim organizacijama, školama, državnim agencijama i drugim subjektima, te su zbog svoje osjetljivosti i mogućnostima kojima pružaju izuzetno traženi na crnom tržištu.

Krađa identiteta može biti počinjena fizičkim putem, bez uporabe tehničkih sredstava, ali i *online*, uporabom interneta.[6] Napredak informacijsko-komunikacijske tehnologije (eng. *Information and Communication Technology*; u daljnjem tekstu: ICT) i široka upotreba interneta značajno su olakšali počinjenje ovog kaznenog djela. Povećana upotreba interneta za poslovne i financijske transakcije, društvene mreže te pohranu osobnih podataka omogućila je lakši pristup osjetljivim informacijama, što je dodatno povećalo ranjivost pojedinaca i institucija. Zbog toga je krađa identiteta svrstana među računalna kaznena djela, budući da može biti izvršena kako tradicionalnim, tako i digitalnim metodama.[7]

Radi boljeg razumijevanja koncepta krađe identiteta, cilj ovog rada je pružiti cjelovit pregled njegovih ključnih karakteristika, istražiti glavne uzroke rasprostranjenosti ovog djela, identificirati najčešće pojavne oblike te postoje li odgovarajući međunarodni i nacionalni zakonodavni okviri za suzbijanje i sankcioniranje ovog kaznenog djela.

1.1. Povijesni razvoj krađe identiteta

[6] Kokot, Ivica, Kaznenopravna zaštita računalnih sustava, programa i podataka, Zagrebačka pravna revija, vol. 3, br. 3, 2014: https://hrcak.srce.hr/141877, 4. srpnja 2024. str. 322.
[7] Ibid.

Uz široku medijsku pokrivenost, rezultate različitih istraživanja koja procjenjuju opseg i štetu uzrokovanu krađom identiteta, te brojne pravne i tehničke analize objavljene posljednjih godina, čini se da je krađa identiteta fenomen 21. stoljeća. Međutim, još 1980-ih godina, novine su izvještavale o zloupotrebi informacija vezanih uz identitet i problemima povezanim s krađom identiteta, poput činjenice da je krivotvorenje dokumenata u nekim zemljama kriminalizirano već više od stoljeća.[8]

Ono što se promijenilo su metode koje počinitelji koriste. Dok su 1980-ih godina klasična krađa pošte ili pak kopanje po tuđem smeću (eng. *dumpster diving*)[9] s ciljem pronalaženja relevantnih osobnih podataka igrali važnu ulogu, sve veća upotreba digitalnih informacija otvorila je nove mogućnosti počiniteljima za relativno lak pristup podacima vezanim uz identitet.[10] Proces transformacije iz industrijaliziranih nacija u informacijska društva imao je veliki utjecaj na razvoj krađe identiteta.

Relevantnost krađe identiteta u 21. stoljeću proizlazi iz sve veće važnosti informacija povezanih s identitetom u gospodarstvu i društvenim interakcijama. Prije su reputacija i dobri osobni odnosi bili ključni za poslovanje i svakodnevne transakcije, često obavljane izravno licem u lice. No, s prelaskom na elektroničku trgovinu, identifikacija licem u lice postala je gotovo nemoguća, čime su informacije vezane uz identitet postale mnogo važnije za sudjelovanje u društvenim i ekonomskim aktivnostima. Ovaj proces može se opisati kao instrumentalizacija, pri čemu se identitet pretvara u mjerljive informacije vezane uz identitetom. [11]

[8] Handbook on Identity-related Crime, op.cit., str. 11.
[9] Techniques of Identity Theft, Canadian Internet Policy and Public Interest Clinic, March, 2007: https://www.social-engineer.org/wiki/archives/IdTheif/IdTheif-Techniques.pdf, 3. srpnja 2024., str.5.
[10] Ibid.
[11] Ibid.

S naglim porastom količine osobnih podataka dostupnih na internetu krajem 1990-ih i početkom 2000-ih, krađa identiteta postala je sve češća briga. No, unatoč velikom broju slučajeva krađe identiteta povezanih s internetom, digitalizacija nije omogućila samu pojavu kaznenog djela, već je stvorila nove ciljeve i olakšala razvoj novih oblika krađe identiteta te alata i softvera za počinjene istih.[12]

1.2. Pojam krađe identiteta

Identitet je obično povezan sa skupom osobnih podatka i pripadajućih dokumenata koji razlikuju pojedince.[13] S pravnog gledišta[14], pojam identiteta prvenstveno se odnosi na informacije koje se koriste za razlikovanje jedne osobe od druge. Pritom je ključno razlikovati identitet osobe, definiran kao skup osobnih karakteristika, od mjerljivih informacija vezanih uz identitet koje omogućuju prepoznavanje te osobe.[15]

Prema tome, osnovne komponente identiteta u pravnom smislu relativno je lako shvatiti. One se općenito temelje na određenim fiksnim i provjerljivim atributima, koje obično službeno dodjeljuju i registriraju javna državna tijela.[1617] Ti atributi uključuju spol, ime i prezime, datum i mjesto rođenja, ime i prezime roditelja, te u nekim zemljama dodijeljeni broj socijalnog osiguranja.[18] Tehnološki napredak je dodatno proširio koncept identiteta na *online* svijet te uveo

---

[12] Ibid.
[13] Study on online identity theft and identity-related crime, Directorate-General for Migration and Home Affairs (European Commission), 2022: https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1, 3. srpnja 2024., str. 11
[14] Koncept identiteta puno je širi i može biti promatran s više gledišta (sociološkog, filozofskog, povijesnog, itd.).
[15] Handbook on Identity-related Crime, United Nations Office on Drugs and Crime, April 2011, https://www.unodc.org/documents/congress/background-information/Corruption/Handbook_on_Identity-related_Crime_ENG.pdf, 3. srpnja 2024., str. 12.
[16] OECD, Online Identity Theft, OECD Publishing, Paris, 2009: https://read.oecd-ilibrary.org/science-and-technology/online-identity-theft_9789264056596-en#page18, 3. srpnja 2024., str. 18.
[17] Ovi atributi najčešće su sadržani u službenim dokumentima poput putovnica, osobnih iskaznica, rodnih i smrtnih listova, vozačkih dozvola i u nekim državama, dodijeljenih brojeva socijalnog osiguranja ili primjerice u Hrvatskoj, putem osobnog identifikacijskog broja (OIB).
[18] Online Identity Theft, op. cit.

pojam „digitalnog identiteta“.[19] Kada se informacijski sustavi koriste za autentifikaciju, pojam identiteta može obuhvaćati pojedinačno dodijeljena korisnička imena, prijave, osobne identifikacijske brojeva (PIN - eng. *Personal Identification Number*), IP (eng. *Internet Protocol*) adresu koja identificira računala na internetu, e-mail adresu, bankovni račun ili lozinke. Digitalni identitet stoga uključuje „tko je pojedinac“ i „vjerodajnice“ koje čine atribute njegovog identiteta.[20]

Krađa identiteta je problem koji uključuje osobne podatke, stoga za dublje sagledavanje koncepta krađe identiteta, nužno je imati jasno razumijevanje pojma osobnih podataka. Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ[21] (u daljnjem tekstu: Uredba) određuje da su: Osobni podaci su „svi podaci koje se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi (*ispitanik*); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca“.[22] Važno je istaknuti da informacije koje zajedno prikupljene mogu dovesti do utvrđivanja identiteta određene osobe, također čine osobne podatke.[23] Shodno tome, krađa identiteta odnosi se na korištenje tuđih osobnih podataka, bez

[19] Handbook on Identity-related Crime, op.cit.
[20] Study on online identity theft and identity-related crime, op.cit.
[21] Poznata i kao Opća uredba o zaštiti podataka ili po skraćenici GDPR koja dolazi od engleskog naziva uredbe – General Data Protection Regulation.
[22] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ, na snazi od 25.05.2018., čl.4. st.1.
[23] Ibid., uvodna izjava (26).

dopuštenja i znanja osobe čiji su to osobni podaci. To se često radi u svrhu počinjenja prijevare ili nekog drugog kaznenog djela.[24]

Sam pojam „krađa identiteta“ se ne koristi dosljedno. Prije svega se koristi za opisivanje radnje pribavljanja identiteta, odnosno osobnih podataka, druge osobe (krađa). Osim toga, izraz se koristi i u smislu posjedovanja i korištenja tih osobnih podataka. Končano, njime su često uključena i kasnija kaznena djela počinjena korištenjem identiteta druge osobe (najčešće prijevara).[25]

S pravnog aspekta, sam pojam može biti problematičan iz nekoliko razloga. Naime, upotreba riječi „krađa“ ne može doslovno odražavati situaciju jer identitet pojedinca i dalje ostaje u njegovom posjedu nakon krađe identiteta, što se razlikuje od tradicionalnog pojma krađe.[26]

Nadalje, termin „krađa“ obično implicira samo čin nezakonitog prisvajanja. Međutim, u slučaju krađe identiteta, kasniji zločini koji se počine korištenjem ukradenih osobnih podataka često su obuhvaćeni pod pojmom „krađe identiteta“ u cjelini.[27]

Upravo zbog gore navedene problematike, ni na razini Europske Unije ni na međunarodnoj razini ne postoji zajednički pravni okvir, odnosno zajednički koncept o tome što je krađa identiteta.

Osim što ne postoji jedinstveni koncept što je krađa identiteta, čak ni termin koji se koristi za opisivanje ovog fenomena nije dosljedno korišten. U Sjedinjenim Američkim Državama se najčešće koristi termin *identity theft* (krađa identiteta) No, u Ujedinjenom Kraljevstvu prevladava izraz *identity fraud*[28], za koji ne postoji ustaljen prijevod na hrvatski jezik, ali svakako

[24] Dragičević, Dražen et al., Pravna informatika i pravo informacijskih tehnologija, Narodne novine, Zagreb, listopad 2015., str. 189.
[25] Gercke, op cit., str. 19
[26] Study on online identity theft and identity-related crime, op.cit.
[27] Ibid.
[28] Handbook on Identity-related Crime, op.cit., str. 25.

podrazumijeva termin „prijevara“ (eng. *fraud*). Ispravnije bi možda bilo koristiti potonji termin, zbog gore navedenog razloga da termin „krađa“ (eng. *theft*) ne može biti doslovno primijenjen na ovu situaciju, zato što identitet ne može biti prisvojen niti krađa identitet obuhvaća samo radnju protupravnog prisvajanja.

Osim ova dva, često korišteni termin za ovu vrstu kaznenih djela je „kaznena djela vezana uz identitet“ (eng. *identity-related crimes*).[29]

Slijedom navedenog, postoji mnogo različitih termina i definicija koje se mogu pronaći u pravnim izvorima različitih država i provedenim istraživanjima od strane raznih međunarodnih organizacija. Možda u budućnosti dođe do standardizacije termina koji će opisivati ovo kazneno djelo i shodnu definiciju.

1.3. Faze krađe identiteta

Krađa identiteta može se razdvojiti na četiri različite faze, od kojih se prva faza može opisati kao pripremna faza. Upotreba izraza „priprema“ može zavarati jer vrlo često već postoji interakcija sa žrtvom.[30] U smislu hrvatskog kaznenog zakonodavstva, pripremna faza može se izjednačiti s pripremnim radnjama, onim radnjama „kojima se stvaraju pretpostavke za počinjenje kaznenog djela“.[31] Pripremnim radnjama se nastoji olakšati izvršenje kaznenog djela, no samim njihovim poduzimanjem počinitelj još nije započeo s ostvarivanjem obilježja kaznenog djela.[32]

Druga faza uključuje prisvajanje informacija o identitetu, odnosno osobnih podataka, putem fizičke krađe, pretraživanjem internetskih pretraživača, neovlaštenim pristupom računalnim

[29] Ibid.
[30] Handbook on Identity-related Crime, op.cit., str. 32
[31] Horvatić, Željko ; Derenčinović, Davor ; Cvitanović, Leo, Kazneno pravo - opći dio I. Zagreb: Pravni fakultet Sveučilišta u Zagrebu, 2016, str. 137.
[32] Ibid.

sustavima putem zlonamjernih programa ili korištenjem *phishing* i drugih tehnika društvenog inženjeringa.[33]

Treća faza obuhvaća posjedovanje i raspolaganje prikupljenim informacijama, što može uključivati i njihovu prodaju. Uključivanje ove faze odgovor je na činjenicu da informacije o identitetu ne moraju nužno koristiti sami počinitelji koji su ih prvotno pribavili, već ih često prodaju, prenoseći tako informacije o kreditnim karticama, bankovnim računima, lozinkama i slično iz jedne skupine organiziranog kriminala u drugu.[34]

U posljednjoj fazi, počinitelji koriste ukradene informacije o identitetu kako bi počinili daljnja kaznena djela ili pak sakrili vlastiti identitet. Daljnje kriminalne radnje mogu uključivati, na primjer: pranje novca; trgovinu ljudima (često putem velikih, transnacionalnih kriminalnih mreža) i ilegalnu imigraciju; lažne osobne isprave, npr. kojima se omogućava ilegalnim imigrantima da prođu kroz graničnu kontrolu; izbjegavanje kaznenog progona ili novčane kazne; omogućavanje počinitelju da dobije novi identitet ako je počiniteljevo kreditno stanje loše ili da izbjegne plaćanje dugova; pranje novca; terorizam; trgovinu drogom; nanošenje štete žrtvi u obliku štete njegovom ugledu, *Internet bullying* ili uhođenje; omogućiti počinitelju da izbjegne prepoznavanje po svom pravom identitetu, npr. ako je on/ona diskvalificirani vozač koji pokušava dobiti nazad vozačku dozvolu ili osuđivani pedofil koji želi dobiti dozvolu za rad s djecom; narušavanje prava žrtve na privatnost i obiteljski život.[35]

[33] Handbook on Identity-related Crime, op.cit.
[34] Ibid.
[35] Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft, European Commission, Centre for Strategy and Evaluation Services, 2012: https://www.slideshare.net/slideshow/new-legal-framework-on-identity-theft-2012/30168033#7, 4. srpnja 2024., str. 7.

2. Metode i svrha krađe identiteta

Prikupljanje osobnih podataka prvi je korak pri počinjenju krađe identiteta. Cilj je prikupiti dovoljno informacija o žrtvi kako bi se mogle provoditi transakcije u njeno ime.

Osobni podaci mogu se prikupljati iz raznih izvora i na razne načine, neki su relativno jednostavni i niskotehnološki (kao što su čitanje osmrtnica; krađa pošte iz domova, poslovnih prostora i poštanskih sandučića; provale u urede ili vozila radi krađe datoteka; krađa prtljage i torbi za spise te pretraživanje otpada domaćinstava i tvrtki), a drugi sofisticiraniji (kao što su krađa ili hakiranje računala; lažno predstavljanje u ime klijenata prilikom poziva osiguravateljima, tvrtkama za kreditne kartice; korištenje usluga *online* brokera informacija te dupliciranje magnetskih traka na poleđini kartica). [36]

Ove metode mogu se provoditi osobno ili virtualno putem interneta, telefonskih linija ili mobitela i ostalih informacijsko-komunikacijskih tehnologija.[37]

2.1. Metode koje uključuju fizičku krađu

2.1.1. Krađa novčanika, mobitela, računala i drugih izvora osobnih podataka

Krađa novčanika, torbica, mobitela i računala predstavlja ozbiljnu prijetnju sigurnosti osobnih podataka, poput osobnih iskaznica, kreditnih kartica i lozinki. Mobiteli često sadrže osjetljive aplikacije, dok računala i mediji za pohranu mogu sadržavati financijske i poslovne dokumente. Zaštita uključuje upotrebu sigurnosnih mjera poput lozinki i biometrijske zaštite te redovito ažuriranje softvera. Važno je izbjegavati pohranu osjetljivih informacija na lako dostupnim mjestima te koristiti usluge praćenja i brisanja podataka na mobilnim uređajima. Također je bitno

[36] Techniques of Identity Theft, op. cit., 4.srpnja 2024., str. 3.
[37] Ibid.

dobro čuvati fizičke predmete poput osobnih iskaznica i kreditnih kartica, koje se često ostave na bankomatu poslije korištenja i postaju laka meta kradljivcima, kao i računi s karticama koje često ostanu na bankomatima.[38]

2.1.2. *Dumpster diving*[39]

Kradljivci identiteta često sistematski pretražuju kućni otpad u potrazi za dokumentima koji sadrže financijske i druge osobne podatke. Posebno su osjetljive, na ovakve vrste krađe, hoteli i tvrtke za iznajmljivanje automobila, koje koriste kreditne kartice za rezervacije te nakon plaćanja često odbacuju papirnate kopije, umjesto da ih unište. Ovi dokumenti zatim završavaju u često lako dostupnim spremnicima za smeće, gdje se lako pronalaze.[40]

Kako bi se spriječilo da *dumpster diver*-i nauče bilo što vrijedno iz smeća, stručnjaci preporučuju tvrtkama da uspostave politiku zbrinjavanja prema kojoj se sav papir, uključujući ispise, usitnjava u sjeckalici prije recikliranja. Zatim da se brišu svi mediji za pohranu podataka, budući da odbačeni računalni hardver može biti zlatni rudnik za počinitelje, pogotovo ako imaju znanje kako oporaviti prethodno izbrisane podatke. Posljednja preporuka tiče se educiranja osoblja o opasnosti od ostavljanja osjetljivih podataka u smeću.

2.1.3. Promjena adrese i krađa pošte

[38] Techniques of Identity Theft, op. cit., 4.srpnja 2024., str. 5
[39] Izraz eng. *dumpster diving* (hrv. pretraživanje smeća; doslovan prijevod: ronjenje u smeću) koristi se za opisivanje procesa pretraživanja kanti za smeća kako bi se pronašli papiri, dokumenti ili sredstva za pohranu koji sadrže podatke povezane uz identitet osobe, s ciljem krađe identiteta i osobnih podataka.
[40] Techniques of Identity Theft, op. cit.

Lopovi preusmjeravaju poštu iz dva glavna razloga, prvo, pošta je obilan izvor osobnih podataka informacija i drugo, preusmjeravanje pošte daje lopovu više vremena da se uključi u lažne transakcije prije nego što žrtva otkrije bilo kakvu sumnjivu aktivnost.[41]

Krađa pošte posebno je jednostavan način za krađu osobnih podataka. Pošta se može ukrasti iz kućnih i poslovnih poštanskih sandučića te iz kanti za smeće i recikliranje. Osim što se lako krade, ujedno pruža izvrstan izvor osobnih podataka - kao što su bankovni izvodi i izvodi kreditnih kartica, unaprijed odobreni zahtjevi za kreditne kartice, odbačeni računi za režije itd. Oni mogu sadržavati ključne pojedinosti, kao što su naziv banke žrtve, broj računa, potpis (s poništenih čekova, vozačka dozvola), broj vozačke dozvole i brojevi kreditne kartice i ograničenja.[42]

2.1.4. Unutarnje prijetnje

Krađa identiteta se često događa u organizacijama, korporacijama i državnim tijelima koja posjeduju osobne podatke. Pojedinci su ranjivi jer imaju malo ili nimalo kontrole nad obiljem osobnih podataka koje posjeduju velike banke podataka, vlade i korporacije. U značajnoj mjeri sigurnost ovih informacija ovisi o integritetu zaposlenika. Sve češće se događa da nezadovoljni ili financijski ugroženi zaposlenici prodaju osobne informacije kojima imaju pristup.[43]

„Istraživanje provedeno na uzorku od 501 organizacije u SAD-u pokazalo je da 53% ispitanika smatra da su štete od unutarnjih napada veće nego od vanjskih napada“.[44] Glavni izazov ovakvih prijetnji leži u činjenici da počinitelji često imaju ovlasti za pristup informacijama i računalnim sustavima organizacija kao zaposlenici ili vanjski suradnici, što znači da ne moraju zaobilaziti

[41] Techniques of Identity Theft, op. cit., str.6.
[42] Ibid., str. 7.
[43] Ibid., str. 11.
[44] Dragičević, Dražen et al., op. cit., str. 187.

postojeće sigurnosne sustave. Iznenadni podatak je da većina štete uzrokovane unutarnjim faktorima proizlazi iz nenamjernih aktivnosti, kao što su pogreške ili nemarnost zaposlenika.[45]

Još jedan od razloga uspjeha unutarnjih napada je činjenica da je većina sigurnosnih mjera implementirana kako bi spriječila vanjske napade.[46]

2.1.5. *Skimming*

Skimming je „tehnika snimanja magnetskih zapisa s bankovnih kartica pomoću posebnih uređaja (tzv. *skimmera*) namijenjenih isključivo toj svrsi.“[47] *Skimmer* je „uređaj koji optički čita i bilježi podatke s magnetne trake“[48].

Skimming na bankomatima karakterizira brzo postavljanje *skimmera*,“na utor bankomata u koji se stavlja kartica“ obično unutar nekoliko minuta. *Skimmer* ostaje na bankomatu nekoliko sati, ovisno o kapacitetu baterije i memorije uređaja. Kako bi se došlo i do PIN-a ovlaštenog korisnika, *skimmeri* se „često kombiniraju s optičkim špijuniranjem ili snimanjem putem mikrokamera pričvršćenih na sam bankomat“.[49] *Skimmeri* se često postavljaju na prometnim mjestima i na bankomatima bez video nadzora, a napadi se često ponavljaju svaka dva dana. Također, važno je naglasiti da se „transakcije *skimiranih* kartica vrše se uglavnom na bankomatima u inozemstvu“[50].

[45] Ibid., str. 188.
[46] Handbook on Identity-related Crime, op.cit., str. 16.
[47] Dragičević, Dražen et al., op. cit. str. 189.
[48] Jelenski, Milivoj; Šuperina, Marijan; Budiša, Josip, Kriminalitet platnim karticama (krađa identiteta, krivotvorenje i zlouporaba platne kartice)", Policija i sigurnost, vol.22, br. 3/2013: https://policijska-akademija.gov.hr/UserDocsImages/onkd/3-2013/jelenski_superina_budisa.pdf, 4. srpnja 2024. str. 386.
[49] Dragičević, Dražen et al., op. cit.
[50] Ibid.

Premda su najčešće u pitanju bankomati, ova tehnika se može upotrijebiti „na svim mjestima gdje se plaćanje vrši putem kartica“.[51] Također i „korištenje *near field communication*[52] (NFC) tehnologije u bankovnim karticama i mobilnim uređajima za autorizaciju transakcija“[53] nosi značajan rizik.

Skimming je „u Hrvatskoj najzastupljeniji oblik krađe podataka u kojem su na udaru korisnici kartičnog poslovanja.“[54] Krađa identiteta i zločini povezani s identitetom uglavnom se provode radi financijske dobiti, pri čemu su najčešće ciljani podaci o plaćanju kartica. U razdoblju od 2017. do 2019. godine, 32 milijuna građana EU bili su žrtve prijevara s bankovnim karticama ili *online* bankarstvom. Ukupni izravni gubici građana EU zbog ovih zločina procjenjuju se na 882 milijuna eura.[55]

2.1.6. Korištenje javno dostupnih informacija

Javne evidencije i razni registri sadrže niz informacija vezanih uz identitet pojedinca ili pravne osobe. Traženjem informacija vezanih uz identitet, u takvim publikacijama, počinitelj ponekad može generirati dovoljno relevantnih informacija koje kasnije može koristiti u kriminalne svrhe.[56]

Među javno dostupne informacije ubrajaju se i osobni podaci preminulih osoba, kojima se može pristupiti putem novinskih osmrtnica i nadgrobnih spomenika. Osmrtnice sadrže datume rođenja, puna imena i često ključne podatke o obitelji. Nemarna pogrebna poduzeća mogu dati osobne podatke kradljivcima predstavljajući se kao osiguravajuće društvo preminulog. Kradljivac

[51] Dragičević, Dražen et al., op. cit., str. 189.
[52] Hrv. komunikacija bliskog polja.
[53] Ibid.
[54] Ibid.
[55] Study on online identity theft and identity-related crime, op. cit., str. 15.
[56] Handbook on Identity-related Crime, op.cit., str. 16.

identiteta može iskoristiti te podatke, primjerice, za stvaranje računa i podizanje kredita bez da ih vrati.[57]

2.2. Metode koje se baziraju na informacijsko-komunikacijskoj tehnologiji

Krađa identiteta putem informacijsko-komunikacijskih tehnologija može uključivati korištenje različitih programa, kao što su *keyloggeri*. Ovi programi ili kombinacije programa i uređaja tajno prate i snimaju pritisnutih tipki na računalu, a prikupljene podatke šalju na udaljeno računalo.

Tu su i druge vrste *malwarea* (hrv. maliciozni programi), poput trojanskog konja[58] Zeusa, koji se koriste pri financijskim transakcijama. Uz to, postoje i druge metode, poput već spomenutog phishinga.[59]

2.2.1. *Phishing*

Phishing, poznat i kao *carding* ili *brand spoofing*, oblik je krađe identiteta koji je „danas jedan od najčešćih oblika prijevare u kibernetičkom prostoru“.[60] Ova metoda uključuje „slanje prijevarnih poruka elektroničke pošte koje izgledaju kao da ih je poslala ugledna tvrtka ili institucija, poput banke, kartične kuće, osiguravatelja ili pružatelja usluga na internetu“.[61] U tim porukama primatelje se traži da iz određenih razloga odgovore i unesu svoje osobne podatke poput imena, broja bankovne ili kreditne kartice, korisničkog imena i lozinke, PIN brojeva i slično. Također, poruka može sadržavati poveznicu (link) na lažnu web stranicu koja izgledom podsjeća na

[57] Techniques of Identity Theft, op. cit., str.9.
[58] Trojanski konj je program koji izgleda kao običan softver, ali sadrži skrivene funkcije nepoznate korisniku. Njegovi ciljevi mogu uključivati omogućavanje neovlaštenog pristupa, krađu podataka, nadzor korisnikovih aktivnosti, izvođenje DDoS napada, te traženje sigurnosnih propusta u sustavu.; Dragičević, Dražen et al., op. cit. str.176.
[59] Dragičević, Dražen et al., op. cit., str. 189.
[60] Dragičević, Dražen et al., op. cit., str. 181.
[61] Ibid.

originalnu stranicu te tvrtke ili institucije.[62] Često se iskorištavaju slabosti komunikacijskog protokola za slanje elektroničke pošte, *Simple Mail Transfer Protocol* (SMTP), koji ne sadrži mehanizme za autentifikaciju pošiljatelja, što omogućava brojne zloupotrebe poznate kao *e-mail spoofing*.[63] Nakon što primatelji unesu tražene podatke, prevaranti ih koriste za krađu identiteta, što im omogućuje prijenos sredstava, plaćanje roba ili usluga i slično. S obzirom na sve veći broj financijskih transakcija putem internetskog bankarstva i rastući broj tvrtki koje elektronički nude robe ili usluge, ne iznenađuje da ovaj oblik prijevare postaje sve raširenij.[64]

Pojavila se i nova forma *phishinga*, poznata kao *spear-phishing* („ciljani *phishing"*), koja je izazvala zabrinutost unutar internetske zajednice. Kod *spear-phishinga*, prevaranti ciljaju određene osobe unutar manjih grupa, poput zaposlenika tvrtki ili državnih ureda, umjesto da šalju poruke milijunima korisnika e-pošte. Ciljevi su pažljivo birani, a lažne e-poruke su personalizirane i specifično usmjerene prema korisnicima koji već imaju uspostavljen odnos s lažiranim pošiljateljem, čime se napadi čine težima za otkrivanje i neutralizaciju. Ova vrsta *phishinga* predstavlja oblik socijalnog inženjeringa, metode pribavljanja povjerljivih informacija manipulacijom legitimnih korisnika, koja se koristi, među ostalim, za korporativnu špijunažu. Naime, primatelj ovih poruka otkriva informacije i lozinke koje kriminalcima omogućuju pristup sigurnim područjima korporativne mreže. Posljedice mogu uključivati krađu intelektualnog vlasništva, kao i drugih osjetljivih korporativnih, vladinih ili pak vojnih dokumenata i podataka. Ovaj sofisticirani pristup čini *spear-phishing* ozbiljnom prijetnjom za sigurnost podataka unutar

[62] Ibid.
[63] Ibid.
[64] Ibid.

korporacija i vladinih organizacija, te zahtijeva pojačane mjere zaštite i svijest korisnika o opasnostima ovakvih napada.[65]

Krađa identiteta putem zlonamjernog softvera (*pharming*) je poseban oblik *phishinga* u kojem haker pokušava preusmjeriti elektroničku komunikaciju i podatke s legitimne web stranice na potpuno drugačiju internetsku adresu. Ova vrsta zloupotrebe obično se izvodi promjenom datoteka na korisnikovom računalu ili iskorištavanjem nedostataka na poslužitelju kojeg koristi žrtva. Ovo je sofisticiraniji oblik *phishinga*, jer u ovom slučaju korisnik ne mora odgovarati na e-poruku koja bi počinitelju pružila sve privatne i povjerljive podatke korisnika. Samim otvaranjem takve elektroničke poruke, računalni virus - *trojanac*, zlonamjerni softver (eng. *malware*[66]) ili generator ključeva preuzima se na računalo žrtve, kradući sve važne podatke žrtve - lozinke, korisnička imena i brojeve kreditnih kartica korištene na tom računalu. Nakon dobivanja podataka, moguće je stvoriti lažne identitete, krivotvoriti dokumente, čekove ili kreditne kartice.[67]

Prema izvješću Europske komisije, 31% korisnika Interneta u Europskoj Uniji (otprilike 148 milijuna građana) prijavilo je da su bili mete ili žrtve različitih oblika *phishinga* u razdoblju od 2017. do 2019. godine. Procjenjuje se da su ukupni izravni gubici građana EU zbog *phishinga*, u razdoblju do 2022., dostigli oko 27 milijardi eura.[68]

---

[65] OECD, Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures, OECD Digital Economy Papers No. 114: https://www.oecd-ilibrary.org/docserver/231503010627.pdf?expires=1720207258&id=id&accname=guest&checksum=5A9E3E47525EFD40B1C95D38CD8B9157, 5. srpnja 2024., str. 22.

[66] Maliciozni programi su računalni programi ili dijelovi programskog koda čije pokretanja dovodi do neželjenih posljedica po korisnika, odnosno njegov računalni sustav, podatke ili programe. U tu grupu spadaju računalni crvi, trojanski konji, računalni virusi, (…)“.; Dragičević, Dražen et al., op. cit. str. 176.

[67] Vilić, Vida M., Phishing and pharming as forms of identity theft and identity abuse, Balkan Social Science Review, 2019, Vol 13, Issue 13: https://js.ugd.edu.mk/index.php/BSSR/article/view/3033/2743, 5. srpnja 2024., str. 47.

[68] Study on online identity theft and identity-related crime, op. cit., str. 15.

2.2.2. „Nigerijsko pismo“

„Nigerijsko pismo“, kao i *phishing*, također spada u prijevare putem elektroničke pošte i lažnih web-stranica, a njegovim sadržajem se pokušava dovesti u zabludu korisnika.[69]

„Nigerijsko pismo“ (*Nigerian letter*), također poznato kao *Nigerian 419 scam*, primjer je prijevare koja iskorištava ljudsku lakovjernost putem e-maila, nudeći razne poslovne prilike s obećanjem brze i lake zarade. Prvi zabilježeni slučajevi pojavili su se već početkom 1980-ih godina.[70] Iako se ova prijevara ne mora nužno provoditi putem interneta (naziv "nigerijsko pismo" potječe od ranijih prijevara koje su se slale putem pisama i faksova), e-mail je danas glavni medij koji omogućuje masovno slanje poruka, dosežući veliki broj potencijalnih žrtava. Unatoč tome što ova vrsta prijevare može izgledati trivijalno, „*Financial Crimes Division of the U.S. Secret Service* dnevno zaprima više od 100 telefonskih poziva i 300-500 dopisa od potencijalnih ili stvarnih žrtava“.[71] Ove prijevarne ponude najčešće spadaju u kategorije poput nasljedstva, ugovora o dobrima i uslugama, kupovine nekretnina, konverzije stranog novca, prijenosa sredstava ili prodaje sirove nafte ispod tržišne cijene. Žrtvama se obično nudi značajna provizija, a ponekad ih se potiče da posjete Nigeriju ili okolne zemlje kako bi dogovorili posao, što može dovesti ne samo do financijskog gubitka, već i do ozbiljnih, pa i smrtonosnih posljedica.[72]

2.2.3. *Vishing*

Voice over Internet Protocol (*VoIP*) je također nova tehnika koja se koristi za krađu osobnih podataka pojedinaca. Putem ove metode, počinitelj šalje klasičnu krivotvorenu e-poštu prikrivenu

[69] Dragičević, Dražen et al., op. cit., str. 182.
[70] Dragičević, Dražen et al., op. cit., str. 182.
[71] Ibid.
[72] Ibid.

kao da dolazi od legitimnih poslovnih ili institucionalnih subjekata, koja poziva primatelja da nazove određeni telefonski broj. Žrtve se obično osjećaju sigurnije na ovaj način jer nije potrebno posjetiti *web-stranicu* na kojoj bi upisivali svoje osobne informacije. Kada nazovu, žrtve dolaze do automatiziranog govornog sustava koji traži unos osobnih podataka poput broja računa, lozinke ili drugih informacija pod izlikom dodatne sigurnosti u identitet pozivatelja. U nekim slučajevima, počinitelj izravno naziva potrošače tražeći financijske informacije.[73]

2.2.4. *SMiShing*

SMiShing je vrsta *phishing* napada koji koristi lažne tekstualne poruke (SMS) na mobilnim uređajima kako bi prevario metu napada da preuzme zlonamjerne programa, podijeli osjetljive podatke ili pošalje novac počiniteljima napada. Jedan od primjera *smishinga* je kad žrtva primi SMS u kojima tvrtka, najčešće tvrtka koja nudi telekomunikacijske usluge, potvrđuje da se korisnik prijavio za korištenje jednu od njenih usluga, navodeći da će im biti naplaćen određeni iznos dnevno ako ne otkažu narudžbu na web-stranici tvrtke, koja je lažna.[74]

Smishing je sve popularniji oblik cyber kriminala. Prema izvještaju Proofpointa za 2024. godinu, 75% organizacija doživjelo je *smishing* napade tijekom 2023. godine.[75]

Više faktora pridonijelo je porastu *smishinga*. Počinitelji koji provode ove napade, ponekad nazvani *smisheri*, znaju da su žrtve sklonije kliknuti na tekstualne poruke nego na druge poveznice (linkove). Istovremeno, napredak u spam filterima otežao je drugim oblicima

[73] Online Identity Theft, op. cit., str. 25
[74] Ibid.
[75] Ibid.

phishinga, poput e-pošte i telefonskih poziva, da dođu do svojih ciljeva.

Povećanje prakse radnih aranžmana na daljinu također je dovelo do toga da više ljudi koristi svoje poslovne mobilne uređaje tijekom posla, olakšavajući počiniteljima pristup korporativnim mrežama putem takvih mobilnih telefona zaposlenika.[76]

3. Zakonodavni okvir krađe identiteta u Hrvatskoj

Kazneni zakon Republike Hrvatske ne poznaje kazneno djelo krađe identiteta kao posebno kazneno djelo. Ono kao takvo nije precizno uređeno zakonom, već u slučaju počinjenja ovog zločina, isto će najčešće biti kažnjivo, ako su ostvarena bitna obilježja bića kaznenih djela nedozvoljene uporabe osobnih podataka (čl. 146. KZ-a) ili zlouporabe osobne isprave (čl. 280. KZ-a).

3.1. Kazneni zakon Republike Hrvatske

3.1.1. Nedozvoljena uporaba osobnih podataka

Kazneni zakon Republike Hrvatske zabranjuje nedozvoljenu uporabu osobnih podataka. Prema čl. 146. st. 1. KZ-a, svatko tko protivno uvjetima određenim u zakonu prikuplja, obrađuje ili koristi osobne podatke fizičkih osoba, kaznit će se kaznom zatvora do jedne godine. Zaštita se odnosi na osobne podatke, odnosno na nepovredivost tih podataka, koji se bez odobrenja osobe na koju se odnose ne smiju koristiti izvan zakonom određenim svrha.[77]

[76] Ibid.
[77] Dragičević Prtenjača, Marta; Zagorec, Marina, Ponešto o privatnosti, pravu na privatnost i njezinoj zaštiti u Hrvatskoj kroz kazneno djelo Nedozvoljene uporabe osobnih podataka, Godišnjak Akademije pravnih znanosti Hrvatske/ Yearbook Croatian Academy of Legal Sciences, XIV, 2023, 1: https://hrcak.srce.hr/clanak/447566, 6. srpnja 2024., str. 70.

Za ispravnu primjenu ovog kaznenog djela ključno je temeljito razumijevanje njegovog zakonskog opisa i sastavnih elemenata te pravilno definiranje tih pojmova. Važno je istaknuti da se radi o blanketnom kaznenom djelu, čija se suština ne može shvatiti bez upućivanja na druge zakone ili propise, s obzirom na to da su elementi njegovog zakonskog opisa bliskoj vezi s drugim zakonima.[78] Primjerice, odredbe kaznenog djela ovise o sadašnjoj Uredbi i prijašnjem Zakonu o zaštiti osobnih podataka, kao i o drugim zakonima poput Zakona o medijima, Zakona o elektroničkim medijima, Zakona o zaštiti potrošača i Zakona o elektroničkim komunikacijama, koji također često upućuju na primjenu Uredbe.

Zanimljivo je da članak 146. KZ-a koristi izraz „zakon“, iako se uglavnom odnosi na Uredbu. Budući da Uredba ima izravnu primjenu i veću pravnu snagu od zakona, ne bi škodilo u budućnosti jasno regulirati ovu inkriminaciju i preciznije je nomotehnički urediti, uz obrazloženje izmjena kako bi se očuvala pravna sigurnost i pravni kontinuitet. Ako Uredba (ili drugi zakoni) predviđaju posebne razloge za prikupljanje podataka u određenim slučajevima, tada se to ne bi smatralo kaznenim djelom. Za razliku od većine drugih kaznenih djela iz te glave, kazneni postupak za ovo djelo pokreće se po službenoj dužnosti.[79]

Nadalje, stavak 2. članka 146. Kaznenog zakona propisuje da će kaznom zatvora do tri godine biti kažnjen onaj tko suprotno uvjetima određenim u zakonu (Uredbi) iznosi osobne podatke iz Republike Hrvatske radi daljnje obrade, objavi ih ili na drugi način učini dostupnim drugome, ili tko takvom radnjom sebi ili drugome pribavi znatnu imovinsku korist ili prouzroči znatnu štetu.

Stavak 2. članka 146. propisuje teži oblik kaznenog djela nedozvoljene uporabe osobnih podataka, dok stavak 3. dodatno definira još jedan primjer težeg oblika tog kaznenog djela.

[78] Ibid.
[79] Ibid.

Kaznom zatvora do tri godine bit će kažnjen i onaj tko (protivno Uredbi) nedozvoljeno prikupi, obradi ili koristi osobne podatke djeteta ili podatke koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska uvjerenja, sindikalno članstvo, zdravlje, spolni život ili kaznene i prekršajne postupke.[80]

Posebno težak oblik ovog kaznenog djela nastaje kada, navedene oblike, počini službena osoba tijekom obavljanja službene dužnosti ili odgovorna osoba prilikom vršenja javnih ovlasti. U tom slučaju predviđena je stroža kazna, koja može iznositi od šest mjeseci do pet godina zatvora.[81]

Kako bi se u potpunosti razumjele odredbe ovog kaznenog djela, potrebno je definirati koji podatci spadaju u osobne podatke i što podrazumijeva obrada tih podataka.

Osim definicije osobnih podataka koja je ponuđena u Uredbi i gore navedena, postoji još nekoliko pokušaja definiranja osobnih podataka. Pa se tako Direktivom (EU) 2016/680[82] osobnim podatkom smatraju svi podatci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, odnosno kao osobu koja se može identificirati izravno ili neizravno, posebno uz pomoć identifikatora poput imena, identifikacijskog broja, podataka o lokaciji, mrežnog identifikatora ili s pomoću jednog ili više čimbenika karakterističnih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

Europski sud za ljudska prava (u daljnjem tekstu: ESLJP) također je definirao osobne podatke kao svaku informaciju koja se odnosi na identificiranu osobu ili osobu koja se može identificirati. Takvi podaci uključuju ne samo informacije koje izravno identificiraju pojedinca, poput imena i

[80] čl. 146. st. 3. KZ-a
[81] Čl. 146. st. 4. KZ-a
[82] Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podatakate o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP

prezimena, već i elemente koji neizravno identificiraju osobu, poput dinamičke IP adrese. Osobni podaci mogu poprimiti različite oblike, primjerice, uzorci stanica i DNK profili, otisci prstiju, podaci o rođenju i smrti pojedinca, informacije o internetskim pretplatnicima i specifične IP adrese, glasovni uzorci, bankovni dokumenti, podaci o korištenju interneta i poruka zaposlenika na radnom mjestu dobivenih nadzorom, kopije elektroničkih podataka zaplijenjenih u odvjetničkom uredu[83], podaci prikupljeni neprikrivenim videonadzorom na sveučilištu, te podaci o oporezivom dohotku i imovini mnogih pojedinaca.[84]

Važno je spomenuti i pojam obrade podataka, koji obuhvaća različite radnje, a Uredba je definira kao bilo koju operaciju ili skup operacija koje se izvode na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim sredstvima ili ne. Te radnje uključuju prikupljanje, snimanje, organizaciju, strukturiranje, pohranu, prilagodbu ili izmjenu, dohvaćanje, konzultacije, uporabu, otkrivanje prijenosom, širenjem ili drugim načinom stavljanja na raspolaganje, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.[85]

Ovo kazneno djelo u praksi se može pojaviti kao produljeno kazneno djelo.[86] Počinitelj produženog kaznenog djela, poznat i kao serijski počinitelj, je osoba koja u kraćem ili duljem vremenskom periodu ponavlja istu radnju kaznenog djela.[87] Isto tako javlja se u stjecaju s drugim kaznenim djelima, a to je situacija u kojoj dolazi do *pluraliteta kaznenih djela*[88], zato što počinitelj jednom ili više radnji ostvari obilježja više kaznenih djela. U načelu, stjecaj označava

[83] Premda nisu dešifrirani, prepisani ili pao službeno pripisani njihovim vlasnicima.
[84] Dragičević Prtenjača et al., op. cit., str. 72.
[85] Čl. 4. Uredbe.
[86] Uz uvjet da su ostvarene nužne pretpostavke tog pojma: 1. da je riječ o više istih ili istovrsnih k.d.; 2. da se ne radi o napadu na strogo osobna dobra; 3. da između pojedinih radnji postoji kontinuitet u smislu prostorne i vremenska povezanosti te 4. da postoji tzv. produljena namjera počinitelja. – Horvatić et al., op cit. str. 188.
[87] Horvatić et al., op. cit., str. 187.
[88] Ibid., str. 179.

situaciju u kojoj se počinitelju, u istom kaznenom postupku, istodobno sudi za više kaznenih djela, a na kraju mu se izriče jedinstvena kazna.[89]

Zanimljiv slučaj iz prakse obuhvatio je oba prethodno navedena aspekta kaznenog prava.

Zaposlenik jedne telefonske kompanije u Hrvatskoj je prikupljao osobne podatke korisnika usluga, koje je potom koristio za sklapanje novih ugovora o mobilnoj pretplati na rok od 24 mjeseca i za nabavku mobitela kao što su Samsung Galaxy 5 i slični uređaji. Sud je optuženika proglasio krivim za stjecaj tri teška kaznena djela: nezakonito korištenje osobnih podataka (članak 146., stavak 1. Kaznenog zakona), zlouporabu položaja i ovlasti (članak 291., stavak 1. Kaznenog zakona) te krivotvorenje službene ili poslovne isprave (članak 279., stavak 1. Kaznenog zakona). Za sva tri kaznena djela osuđen je u formi produljenog kaznenog djela. Osuđen je na jedinstvenu kaznu od 11 mjeseci zatvora, koja je kasnije zamijenjena radom za opće dobro.[90]

Tijekom razdoblja od 2013. do 2023. godine, Republika Hrvatska svjedočila je značajnom skoku u broju prijavljenih slučajeva nedozvoljene uporabe osobnih podataka, s 46 prijava u 2013. na 413 prijava u 2014. godini. Ovaj nagli porast može ukazivati na povećanu osviještenost o ovom obliku kriminaliteta ili na poboljšane kapacitete nadzora i prijavljivanja. Nakon 2014., broj prijavljenih slučajeva ostao je relativno visok, s vrhuncem od 601 prijave u 2015. godini, što sugerira kontinuirani trend problema u zaštiti osobnih podataka. Unatoč visokom broju prijava, razina rješavanja slučajeva varirala je tijekom godina, s manjim brojem riješenih slučajeva u nekim godinama u usporedbi s prijavljenim. Na primjer, u 2014. godini riješeno je 366 od 413

[89] Ibid.
[90] Dragičević Prtenjača et al., op. cit.

prijava, dok je u 2019. riješeno 269 od 289 prijava. To može ukazivati na izazove u istrazi i procesuiranju ovih kaznenih djela, kao i na varijacije kapacitetima pravosudnog sustava.[91]

Nadalje, broj osuđenih za nedozvoljenu uporabu osobnih podataka pokazuje trend oscilacije, s vrhuncem 2017. godine, nakon čega slijedi pad do 2020. kada je zabilježeno 24 osude. Nakon te godine, broj osuđenih opet je u opadanju, s 22 osude u 2021. godini. U odnosu na ukupan broj osuđenih za sve kaznene djela, nedozvoljena uporaba osobnih podataka u 2020. je činila 0,2% svih kaznenih djela protiv privatnosti, dok je za ta djela osuđeno 0,18% počinitelja u 2021. godini.[92]

3.1.2. Zlouporaba osobne isprave

Zlouporaba osobne isprave predstavlja relativno novo kazneno djelo uvedeno Kaznenim zakonom donesenim 21. listopada 2011., a koji je stupio na snagu 1. siječnja 2013. Ovim kaznenim djelom obuhvaćeno je „prijevarno korištenje osobne isprave izdane na ime druge osobe.“[93] Kazneno djelo zlouporabe osobne isprave dio je glave dvadeset šeste Kaznenog zakona, koja objedinjuje kaznena djela krivotvorenja. Ono što je zajedničko svim kaznenim djelima sadržanim u ovoj glavi je radnja krivotvorenja, kojom se zlonamjerno preinačuje istina na štetu drugoga.[94]

[91] Ministarstvo unutarnjih poslova Republike Hrvatske, Overview of basic indicators for public safety in the Republic of Croatia for 2014 – 2023., Zagreb, 2023: https://mup.gov.hr/UserDocsImages/statistika/2024/3/Overview%20of%20the%20basic%20indicators%20for%20public%20safety_2014_2023_web.pdf, 6. srpnja 2024., str. 2.
[92] Dragičević Prtenjača et al., op cit., str. 77.-78.
[93] Cvitanović, Leo; Derenčinović, Davor; Dragičević Prtenjača, Marta; Maršavelski, Aleksandar; Munivrana Vajda, Maja; Roksandić Vidlička, Sunčana, Kazneno pravo – posebni dio, Pravni fakultet Sveučilišta u Zagrebu, 2017, str. 392.
[94] Ibid.

Valja napomenuti da Kazneni zakon (NN 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11, 143/12) iz 1997. godine (u daljnjem tekstu: KZ/97) nije poznavao zlouporabu osobne isprave kao zasebno kazneno djelo.

Razlog za propisivanje zasebnog kaznenog djela zlouporabe osobne isprave proizlazi iz činjenice da je sudska praksa povremeno tretirala korištenje nepreinačene tuđe osobne isprave kao kazneno djelo krivotvorenja isprave, što predstavlja nedopuštenu analogiju[95] Naime, zlouporaba osobne isprave nije bila obuhvaćena kaznenim djelom krivotvorenja isprave iz članka 311.[96] KZ/97, smještenim u glavi dvadesetoj i trećoj – kaznena djela protiv vjerodostojnosti isprava. S obzirom na činjenicu da počinitelj ne vrši nikakve izmjene na takvoj ispravi, odnosno niti izrađuje niti preinačuje osobnu ispravu, ne može se govoriti o krivotvorenju isprave. Stoga je bilo nužno zasebno inkriminirati takve radnje.[97]

Sadržaj članka kaznenog djela zloupotrebe osobne isprave glasi: „Tko osobnu ispravu, izdanu na ime druge osobe, prijevarno koristi u pravnom prometu ili radi prijevare u pravnom prometu prepušta drugoj osobi osobnu ispravu koja na ime te osobe nije izdana, kaznit će se kaznom zatvora do jedne godine.“[98]

[95] Novoselec, Petar; Garačić, Ana, Primjena blažeg zakona nakon stupanja na snagu novog Kaznenog zakona, Hrvatski ljetopis za kazneno pravu i praksu, vol.19., br. 2., 2012: https://hrcak.srce.hr/file/163374, 6. srpnja 2024., str. 545.

[96] *Krivotvorenje isprave* - članak 311.:
(1) Tko izradi lažnu ispravu ili preinači pravu s ciljem da se takva isprava uporabi kao prava, ili tko lažnu ili preinačenu ispravu uporabi kao pravu ili je nabavi radi uporabe,
kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.
(2) Tko kazneno djelo iz stavka 1. ovoga članka počini glede javne isprave, domovnice, oporuke, mjenice, čeka, javne ili službene knjige koja se mora voditi na temelju zakona,
kaznit će se kaznom zatvora od tri mjeseca do pet godina.
(3) Za pokušaj kaznenog djela iz stavka 1. ovoga članka počinitelj će se kazniti.

[97] Cvitanović et al., Kazneno pravo – posebni dio, op. cit.

[98] čl. 280.Kazneni zakon (NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23, 36/24)

Postoje dva modaliteta radnje počinjenja ovog kaznenog djela: prvo, prijevarno korištenje tuđe osobne isprave u pravnom prometu, kao što je neovlašteno pribavljanje tuđe osobne iskaznice putem krađe; drugo, prepuštanje osobne isprave drugoj osobi radi prijevarnog korištenja u pravnom prometu, kao što je sklapanje pravnih poslova. Predmet zaštite su osobne isprave.[99]

Zabilježen je slučaj u sudskoj praksi Općinskog suda u Slavonskom Brodu u kojem je optuženik počinio ozbiljno kazneno djelo zlouporabe osobne isprave tako da je ukrao osobnu iskaznicu svog brata, koja se nalazila u njihovoj zajedničkoj sobi. Korištenjem ukradene isprave, pretvarao se da je njegov brat prilikom zaključivanja ugovora o pretplatničkom odnosu s trgovačkim društvom H... d.d. Time je namjerno stvorio lažni identitet, dovodeći brata u nezakoniti položaj. Sud je ispravno prepoznao ovaj čin kao oblik zlouporabe osobne isprave prema čl. 280. KZ-a.

U ovom slučaju kazneno djelo počinjeno je samo jednom. No, kada bi ista osobna isprava bila korištena u svrhu počinjena više različitih prijevara u pravnom prometu[100] (npr. sklapanja ugovora s više različitih trgovačkih društava), tada bi bila riječ o zlouporabi osobne isprave kao produljenom (nastavljenom) kaznenom djelu.

Osim kao produljeno kazneno djelo, u praksi se ovo zlouporaba osobne isprave često može pojaviti u stjecaju s drugim kaznenim djelima, na primjer, s krivotvorenjem isprave (čl.278. KZ-a), krivotvorenjem službene ili poslovne isprave (čl. 279. KZ-a) ili pak s iznimno teškim kaznenim djelima poput trgovanja ljudima (čl.106. KZ-a).

Zlouporaba osobne isprave ne poznaje godine i uzrast. Djeca i adolescenti također mogu počiniti ovo kazneno djelo, na primjer, uzimanjem osobne iskaznice roditelja ili bliske osobe kako bi

[99] Osobna iskaznica je javna isprava kojom državljanin Republike Hrvatske dokazuje identitet, hrvatsko državljanstvo, spol, datum rođenja, prebivalište i adresu stanovanja. – čl. 1. Zakona o osobnoj iskaznici (NN 62/15, 42/20, 144/20, 114/22, 18/24)

[100] Ili više različitih osobnih isprava u više prijevara u pravnom prometu.

neovlašteno kupili alkohol ili duhanske proizvode, koji su inače zabranjeni osobama mlađima od 18 godina. Iako se ova vrsta krađe identiteta često smatra neozbiljnom i dijelom tinejdžerskog eksperimentiranja, ponekad ima i slučajeva prijavljenih kaznenih djela zlouporabe osobne isprave od strane maloljetnika. Prema izvješću[101] Ministarstva unutarnjih poslova za 2023. godinu, zabilježena su četiri slučaja zlouporabe osobne isprave od strane maloljetnika u dobi od 14 do 18 godina.

U razdoblju od 2014. do 2023. godine, Hrvatska je zabilježila promjenjive trendove u broju prijavljenih i riješenih slučajeva zloupotrebe osobne isprave, što reflektira dinamičnost i izazove u suzbijanju ovog specifičnog oblika kaznenog djela.

Godine 2014. zabilježeno je 67 prijava, od kojih je 62 slučaja riješeno, dok je 2023. godine bilo 90 prijava s rješenjem u 89 slučajeva. Tijekom ovog desetogodišnjeg razdoblja, najveći broj prijava zabilježen je 2015. godine sa 116 slučajeva, dok je najmanje prijava evidentirano 2017. godine s 56 slučajeva. Unatoč fluktuacijama u broju prijava, pravosudni sustav je uglavnom uspješno rješavao slučajeve zloupotrebe osobnih isprava, s postotkom rješavanja koji je često bio blizu ili iznad 90% tijekom većeg dijela analiziranog razdoblja.[102]

3.2. Međunarodni pristup zakonskoj regulaciji krađe identiteta i srodnih zločina

[101] Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2023. godini, Ministarstvo unutarnjih poslova: služba za strateško planiranje, statistiku i unaprjeđenje rada, Zagreb, 2024: https://mup.gov.hr/UserDocsImages/statistika/2024/3/Statisticki_pregled_2023_.pdf, 6. srpnja 2024., str. 78.
[102] Ministarstvo unutarnjih poslova Republike Hrvatske, Overview of basic indicators for public safety in the Republic of Croatia for 2014 – 2023., Zagreb, 2023: https://mup.gov.hr/UserDocsImages/statistika/2024/3/Overview%20of%20the%20basic%20indicators%20for%20public%20safety_2014_2023_web.pdf, 6. srpnja 2024., str. 6.

Nema sveobuhvatnog zakonodavnog instrumenta na razini Europske Unije (u daljnjem tekstu: EU) ili međunarodnoj razini koji se fokusira isključivo na krađu identiteta. Ipak, nekoliko relevantnih pravnih alata su na raspolaganju.

3.2.1. Propisi i direktive Europske Unije

Na razini EU-a, zakonodavni instrumenti mogu se podijeliti u dvije glavne kategorije: prva ima za cilj usklađivanje različitih kaznenih djela povezanih s krađom identiteta (npr. Direktiva (EU) 2019/713[103], Direktiva 2013/40/EU[104]), dok druga obuhvaća mjere koje povećavaju sposobnost država članica da spriječe, suzbiju i smanje rizike od krađe identiteta, uključujući inicijative za zaštitu osobnih podataka, poboljšanje kibernetičke sigurnosti i uspostavu sustava elektroničke identifikacije (Uredba (EU) 2016/679, Direktiva (EU) 2015/2366[105], Uredba (EU) 910/2014[106]).[107]

Prva kategorija obuhvaća pravne instrumente EU-a koji nastoje osigurati nacionalnim kaznenim zakonodavstvima država članica adekvatne alate za suzbijanje krađe identiteta i povezanih kaznenih djela. Nedavno usvojena Direktiva o borbi protiv prijevara i krivotvorenja u vezi s bezgotovinskim sredstvima plaćanja[108] kriminalizira krađu i zloupotrebu podataka za plaćanje te njihovu daljnju prodaju i distribuciju, standardizirajući mjere država članica za prevenciju, otkrivanje i gonjenje prekršaja povezanih s prijevarama i krivotvorenjem sredstava za

[103] Direktiva (EU) 2019/713 Europskog parlamenta i Vijeća od 17. travnja 2019. o borbi protiv prijevara i krivotvorenja u vezi s bezgotovinskim sredstvima plaćanja i zamjeni Okvirne odluke Vijeća 2001/413/PUP
[104] Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP
[105] Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ
[106] Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ
[107] Study on online identity theft and identity-related crime, op. cit., str. 49.-50.
[108] Direktiva (EU) 2019/713.

elektroničko plaćanje. Članak 2. pruža prvu definiciju sredstva za elektroničko plaćanje kao „nematerijalnog ili materijalnog zaštićenog uređaja, predmeta ili zapisa, ili njihove kombinacije, osim zakonskog sredstva plaćanja, koji, sam ili u kombinaciji s postupkom ili skupom postupaka, omogućuje nositelju ili korisniku prijenos novca ili novčane vrijednosti, uključujući putem digitalnih sredstava razmjene“. Članak 3. određuje kaznena djela koja se smatraju: „prijevarna upotreba ukradenog ili na drugi način nezakonito pribavljenog sredstva za elektroničko plaćanje“ i „prijevarna upotreba krivotvorenog ili falsificiranog sredstva za elektroničko plaćanje“. Preambula (31) napominje da su takva djela često povezana s krađom identiteta, stoga „države članice trebaju usvojiti mjere pomoći i podrške“ žrtvama krađe identiteta i odgovoriti direktnije na njihove specifične potrebe.

Jedan od primarnih ciljeva Direktive 2013/40/EU o napadima na informacijske sustave je usklađivanje nacionalnih kaznenih zakonodavstava u vezi s napadima na informacijske sustave, uspostavljajući minimalne standarde u definiciji kaznenih djela i kazni te poboljšavajući suradnju između nadležnih tijela. Iako ta pravila izričito ne ciljaju krađu identiteta, države članice ih ponekad koriste za progon povezanih djela, poput ilegalnog pristupa informacijskim sustavima ili ilegalnog presretanja.[109] Preambula (14) iste Direktive ističe važnost „uspostave učinkovitih mjera protiv krađe identiteta i drugih identitetom povezanih kaznenih djela“, dok članak 9. omogućuje državama članicama da definiraju krađu identiteta kao otežavajuću okolnost kada im nedostaje specifičan zakon.

Druga kategorija obuhvaća pravne instrumente EU-a koji propisuju niz obveza usmjerenih na prevenciju krađe identiteta i povezanih kaznenih djela. Članak 4., točka 12. Uredbe o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnim kretanjem takvih podataka definira

[109] Study on online identity theft and identity-related crime, op. cit., str. 49.-50.

povredu osobnih podataka kao „povredu sigurnosti koja dovodi do slučajnog ili nezakonitog uništavanja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji se prenose, pohranjuju ili na drugi način obrađuju“. Preambule 75. i 85. ističu da je krađa identiteta jedna od mnogih posljedica povreda osobnih podataka. Osim obveze kontrolora podataka da štite osobne podatke, GDPR zajedno s drugim regulativama o sigurnosti podataka doprinosi sprječavanju online krađe identiteta.

Revidirana Direktiva (EU) 2015/2366 (Direktiva o platnim uslugama) ažurirala je i unaprijedila pravila EU-a koja je postavila prva Direktiva o platnim uslugama iz 2007. Druga direktiva je stupila na snagu u siječnju 2016. i članice su je implementirale do kraja siječnja 2018 Ova direktiva je uvela napredne sigurnosne mjere za sve pružatelje platnih usluga, uključujući banke, koje zahtijevaju snažnu autentifikaciju korisnika (*Strong Customer Authentication* - SCA) za elektroničke platne transakcije kako bi se spriječile neovlaštene aktivnosti poput krađe identiteta.[110]

U lipnju 2021. Komisija je usvojila prijedlog za izmjenu Uredbe o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu (skr. eIDAS[111]). Uvedena 2014. godine, Uredba eIDAS uspostavila je prvi EU sustav za sigurne elektroničke interakcije reguliranjem elektroničkih potpisa, novčanih transfera i drugih vrsta elektroničkih transakcija na jedinstvenom europskom tržištu. Time je omogućila stvaranje jedinstvenih standarda za elektroničke potpise, digitalne certifikate, vremenske pečate i druge oblike elektroničke autentifikacije, omogućujući zamjenu papirnatih dokumenata digitalnim ekvivalentima s istom pravnom vrijednošću i službenim priznanjem u svim zemljama EU-a. Međutim, procjena

[110] Ibid.
[111] Electronic IDentification, Authentication and trust Services Regulation.

učinkovitosti Uredbe eIDAS iz 2014. pokazala je da nije u potpunosti zadovoljila tržišne zahtjeve. Stoga je 3. lipnja 2021. godine usvojen prijedlog koji uključuje novi europski digitalni identitet „Wallet App“, putem kojeg će građani moći dokazati svoj identitet i dijeliti elektroničke dokumente, ne samo za javne e-upravne usluge, već i za sve vrste privatnih (npr. e-trgovina) usluga. Osiguravanjem zaštite osobnog identiteta pri obavljanju svakodnevnih transakcija, izmijenjena Uredba eIDAS trebala bi postati uspješan instrument prevencije krađe identiteta.[112]

3.2.2. Zakonodavna rješenja u ostalim članicama Europske Unije

Borba protiv krađe identiteta i identifikacijskih kaznenih djela unutar Europske unije oslanja se na različite pravne mehanizme i strategije koje provode države članice. Unutar EU-a postoje tri glavne vrste mjera koje se primjenjuju kako bi se suzbila krađa identiteta i srodna kaznena djela. Prva kategorija obuhvaća opće prekršaje koji nisu specifično usmjereni protiv krađe identiteta, već kažnjavaju slučajeve u kojima se osobni podaci kradu i/ili zloupotrebljavaju. Druga kategorija uključuje specifične olakšavajuće okolnosti koje povećavaju kazne za druge prekršaje kada je identitet žrtve uključen. Treća kategorija obuhvaća specifična kaznena djela koja se odnose isključivo na krađu identiteta i srodne zločine.[113]

Države članice EU-a prilagođavaju svoje pravne sustave jednoj od ovih kategorija, te se dijele u četiri osnovne skupine prema vrsti mjera koje primjenjuju. Švedska je primjer države koja ima specifične olakšavajuće okolnosti, specifično kazneno djelo, kao i opće prekršaje. Estonska, Finska, Francuska, Nizozemska, Poljska i Slovenija primjeri su zemalja koje imaju opće prekršaje i specifično kazneno djelo. Austrija, Cipar, Španjolska, Irska, Italija, Malta i Portugal imaju opće prekršaje i specifične olakšavajuće okolnosti. Belgija, Bugarska, Češka, Njemačka,

[112] Study on online identity theft and identity-related crime, op. cit., str. 49.-50.
[113] Ibid., str. 48.

Danska, Grčka, Mađarska, Litva, Luksemburg, Latvija, Rumunjska i Slovačka primjeri su država koje imaju samo opće prekršaje.[114]

Specifična kaznena djela krađe identiteta i/ili kaznenih djela povezanih s identitetom uvedena su u sedam od 27 država članica. Estonija je uvela kazneno djelo nezakonite uporabe tuđeg identiteta u članak 157. stavak 2. Kaznenog zakona. Finska je dodala kazneno djelo krađe identiteta u Poglavlje 38 Kaznenog zakona, članak 9.a, koji se odnosi na kaznena djela protiv podataka i komunikacija. Francuska je regulirala kazneno djelo krađe identiteta u članku 226-4-1 Kaznenog zakona. Nizozemska je uključila članak 231.-b u Kazneni zakon, dok je Poljska dodala stavak 2. članku 190.-a Kaznenog zakona, nazvan "kazneno djelo krađe identiteta" u nacionalnoj doktrini i sudskoj praksi. Švedska je regulirala kazneno djelo krađe identiteta u članku 6.-b Poglavlja 4 Kaznenog zakona, koji se odnosi na kaznena djela protiv slobode i mira. Slovenija je u članku 143. Kaznenog zakona, stavak 4., uvela kazneno djelo zlouporabe osobnih podataka.

U usporedbi s prethodnom pravnom procjenom iz 2011., broj država članica sa specifičnim kaznenim djelom se više nego udvostručio, s tri u 2011. na sedam u 2021. Države članice koje su uvele ovu odredbu u posljednjih deset godina su Finska (2015.), Poljska (2011.), Nizozemska (2014.) i Švedska (2016.).[115]

Italija predstavlja neobičan slučaj jer domaći pravni sustav nema kazneno djelo specifično usmjereno na krađu identiteta i/ili kaznena djela povezana s identitetom. Članak 494. talijanskog Kaznenog zakona sadrži generičko kazneno djelo "zamjene osobe" (*substitution of a person*).[116] Međutim, ova odredba je prilično stara (1930.) i, iako je njezin opseg proširen na *online* slučajeve putem sudske interpretacije talijanskog Kasacijskog suda, njezin tekst nije izvorno osmišljen za

[114] Ibid.
[115] Ibid., str. 52.
[116] Ibid., str.53.

pokrivanje incidenata u digitalnom svijetu. To otvara mogućnost da pravna usporedba s novijim, prilagođenim odredbama može dovesti do interpretativnih iskrivljenja. Stoga članak 494. talijanskog Kaznenog zakona ne može biti uključen u razmatranje kao specifično kazneno djelo koje se bavi *online* krađom identiteta i/ili kaznenim djelima povezanih s identitetom.[117]

Specifična kaznena djela unutar EU-a nisu jedinstvena i razlikuju se po fazi zločina koju obuhvaćaju, obveznim elementima koje počinitelji moraju ispuniti da bi djelo bilo nezakonito, ciljevima koje počinitelji ostvaruju zloupotrebom identiteta druge osobe te vrsti i strogoći sankcija. Države članice koje nemaju specifična kaznena djela vjeruju da su njihovi postojeći pravni instrumenti i sankcije dovoljni za suzbijanje kaznenih djela identiteta te stoga ne smatraju nužnim uvođenje nacionalnih zakonskih odredbi posvećenih isključivo krađi identiteta.[118]

Međutim, postojeće poteškoće koje ometaju učinkovitu borbu protiv krađe identiteta i srodnih kaznenih djela nisu povezane samo s nedostatkom specifičnih zakonskih odredbi, već i s operativnim i praktičnim izazovima koji su česti u istraživanju i progonu zločina u *online* okruženju. To uključuje poteškoće u međunarodnoj suradnji s zemljama izvan EU-a, izazove u dobivanju i obradi podataka od tvrtki koje nisu u EU te teškoće u provođenju istraga i prikupljanju dokaza u digitalnim okruženjima.[119]

3.2.3. Međunarodni ugovori i konvencije

Jedna od važnijih međunarodnih konvencija koja se dodiruje ove tematike je Konvencija Vijeća Europe o kibernetičkom kriminalu iz 2001. godine, koja kriminalizira ponašanja povezana s krađom identiteta, poput ilegalnog pristupa računalima (članak 2.), zloupotrebe uređaja (članak

[117] Ibid.
[118] Ibid.
[119] Ibid.

6.), računalnog krivotvorenja (članak 7.) i računalne prijevare (članak 8.). Iako se Konvencija ne bavi direktno krađom identiteta, sadrži značajne odredbe o međunarodnoj policijskoj i pravosudnoj suradnji te prilagodbi tehnološkim inovacijama koje koriste kriminalci.[120]

Godine 2004., Ekonomsko i socijalno vijeće Ujedinjenih naroda (ECOSOC[121]) usvojilo je Rezoluciju 2004/26, koja potiče države članice UN-a na suradnju u prevenciji, istrazi, progonu i kažnjavanju prijevara, zloupotrebe i falsifikacije identiteta. Rezolucija poziva države članice da surađuju kroz Konvenciju Ujedinjenih naroda protiv transnacionalnog organiziranog kriminala i druge međunarodne instrumente te da preispitaju svoje domaće zakone kako bi olakšale tu suradnju.[122]

Na 11. Kongresu UN-a o prevenciji kriminala i kaznenom pravosuđu 2005. godine, usvojena je Bangkoška deklaracija, koja naglašava važnost borbe protiv prijevara s dokumentima i identitetom za suzbijanje organiziranog kriminala i terorizma. Deklaracija potiče međunarodnu suradnju i usvajanje odgovarajućeg nacionalnog zakonodavstva. Konačno, Konvencija UN-a protiv transnacionalnog organiziranog kriminala (UNTOC[123]) promiče međunarodnu suradnju u borbi protiv transnacionalnog organiziranog kriminala, uključujući i krađu identiteta u *offline* kontekstu.[124]

3.3. Problem sintetičke krađe identiteta

Sintetička krađa identiteta uključuje stvaranje novog, fabriciranog identiteta koristeći kombinaciju stvarnih i izmišljenih podataka. Kradljivci zatim mogu otvoriti lažne račune i

[120] Ibid., str. 51.
[121] Economic and Social Council.
[122] Ibid.
[123] UN Convention against Transnational Organized Crime and the Protocols Thereto, UN
[124] Ibid.

provoditi nezakonite aktivnosti koristeći tako stvoren lažni identitet, koji je teže otkriti jer se nezakonite aktivnosti ne prikazuju na kreditnom stanju žrtve.

Shodno tome, potrebno je odlučiti treba li inkriminirati samo djela povezana sa stvarnim identitetom ili treba inkriminirati čak i uporabu lažnih podataka povezanih s identitetom. Inkriminacija uporabe lažnih identiteta na prvi pogled ne čini se relevantnom, jer u tim slučajevima nema utjecaja na legitimnog korisnika identiteta. Ipak, odsutnost prirodne osobe koja je pogođena kaznenim djelom ne znači da takva djela ne uzrokuju štetu. Korištenjem sintetičkih identiteta počinitelji mogu zavarati istražitelje i time otežati svoju identifikaciju. Veliki dio slučajeva povezanih s prijevarama ne temelji se na identitetima s pravim imenom, već na sintetičkim identitetima. Prema rezultatima istraživanja ID Analytics[125], manje od 15 posto svih slučajeva uključivalo je identitete s pravim imenom, dakle preko 85 posto slučajeva krađe identiteta uključuje sintetički identitet.

Sintetički identiteti mogu biti temeljeni isključivo na generiranim podacima ili kombinirati generirane i stvarne podatke povezane s identitetom. Stoga, u procesu izrade zakona stoga je potrebno odlučiti je li miješanje s postojećim identitetom nužan uvjet za inkriminaciju.[126]

4. Analiza predmeta iz sudske prakse Općinskog kaznenog suda u Zagrebu

Za potrebe boljeg shvaćanja kako se krađa identiteta može manifestirati u hrvatskoj sudskoj praksi, u nastavku će biti analiziran jedan pravomoćan predmet iz prakse Općinskog kaznenog suda u Zagrebu (u daljnjem tekstu: OKSZg).

[125] Handbook on Identity-related Crime, op. cit., str. 44.-45.
[126] Ibid.

Prema optužnici[127], osumnjičenik I.F.R. je 6. srpnja 2018. u Zagrebu, u nakani da se nepripadno materijalno okoristi te u nakani da radi prijevare u pravnom prometu koristi tuđu osobnu iskaznicu, najprije nabavio osobnu iskaznicu A.L.-a, nakon čega je putem *webshop* narudžbe neistinito naveo da je on A.L. i da želi sklopiti pretplatnički ugovor u tarifi TELE2 „Raspali“ za određeni broj mobitela. Djelatnici trgovačkog društva „Tele 2“ nisu smatrali da imaju razlog za sumnju u navedeno te su odobrili sklapanje pretplatničkog ugovora u spomenutoj tarifi, uz koju je okrivljenik dobio i mobitel marke „Huawei Mate 10“, u vlasništvu trgovačkog društva „Tele 2“, po povoljnijoj cijeni. Prilikom preuzimanja mobitela, I.F.R. je na dostavnici potpisao A.L-a i time ostvario nepripadnu materijalnu korist u iznosu od 4.265,00 kuna, te je u tom iznosu oštetio navedeno trgovačko društvo (u daljnjem tekstu: t.d.).

Dakle, I.F.R. je s ciljem da sebi pribavi protupravnu imovinsku korist lažnim prikazivanjem činjenica doveo A.L.-a u zabludu i time ga naveo da na štetu tuđe imovine nešto učini. Osim toga, optužen je da je osobnu ispravu izdanu na tuđe ime prijevarno koristio u pravnom prometu.

I.F. R. je ponovno počinio kazneno djelo s gotovo identičnim načinom postupanja (*modus operandi*) kada je 9. srpnja 2018. u Zagrebu, najprije nabavio osobnu iskaznicu na ime A.L.-a, a zatim i ostvario nepripadnu materijalnu korist u iznosu od 7.296,00 kuna. Korist je ostvario tako da je putem *webshopa* „T-Hrvatskog telekoma“ djelatnicima navedenog t.d.-a naveo da je on A.L. i da želi sklopiti pretplatnički ugovor u tarifi „Najbolja L“, što su mu djelatnici t.d.-a i odobrili. Uz sklapanje pretplatničkog ugovora, I.F.R. je dobio i mobitel marke „Huawei P20“.

[127] Općinsko državno odvjetništvo u Zagrebu, broj: K-DO-818/2019.

S obzirom na počinjene radnje, osumnjičenog se tereti za stjecaj[128] dva kaznena djela protiv imovine, prijevarom (opisano i kažnjivo po čl. 236. st. 1. KZ-a), i dva djela krivotvorenja, zlouporabom osobne isprave iz čl. 280. KZ-a.

I.F.R. je na temelju presude[129] OKSZg-a proglašen krivim za počinjena kaznena djela, uz obrazloženje da je okrivljeni koristio osobnu iskaznicu za koju je znao i bio svjestan da nije njegova osobna iskaznica te da je izdana na ime druge osobe, a da je to poduzeo u nakani da se nepripadno materijalno okoristi, pri čemu je bio svjestan svih okolnosti djela i htio je njihovo počinjenje. Djela su počinjena u realnom stjecaju, uz primjenu čl. 51. KZ-a, budući da je okrivljenik s više odvojenih radnji, koja svaka za sebe predstavljaju zasebnu i dovršenu cjelinu, ostvario obilježja više kaznenih djela koja su međusobno povezana osobom okrivljenika. Stoga je I.F.R. svojim ponašanjem ostvario sva bitna obilježja kaznenog djela prijevare (čl. 236. st. 1. KZ-a) i zlouporabe osobne iskaznice (čl. 280. KZ-a). Što se tiče krivnje[130], sud je ustvrdio da je počinitelj postupao s izravnom namjerom. Izravna namjera uključuje da je počinitelj prilikom postupanja bio svjestan djela, tj. njegovih zakonskih obilježja.[131]

I.F.R. je osuđen na jedinstvenu kaznu zatvora u trajanju od jedne godine, koja neće biti izvršena pod uvjetom da okrivljenik u roku od četiri godine po pravomoćnosti presude ne počini novo kazneno djelo. Presudom je također presuđeno da okrivljeni mora vratiti ostvarenu imovinsku koristi, u iznosu od 11.561,00 kn, a koji predstavlja imovinu Republike Hrvatske.

Važno je istaknuti da je okrivljenik osuđen na dva kaznena djela u stjecaju, što ukazuje na to da su radnje kojima se počini krađa identiteta često u stjecaju s drugim kaznenim djelima.

[128] Kažnjiv u svezi s čl. 51. KZ-a.
[129] Općinski kazneni sud u Zagrebu, broj: K-506/19-2, od 1. srpnja 2019.
[130] Subjektivnog odnosa počinitelja prema djelu.
[131] Horvatić et al., op. cit., str. 97.

Osim toga, zanimljivo je da je uvidom u tri od četiri spisa, stavljenim na raspolaganje od strane OKSZg-a, primijećeno da je okrivljenik tuđim osobnim ispravama sklapao prijevarne pretplatničke ugovore s nekim od trgovačkih društva koja u Hrvatskoj nude usluge pružanja telekomunikacijskih usluga. Čime se dolazi do zaključka da je takav način postupanja jedan od zastupljenijih u Hrvatskoj kada se govori o krađi identiteta i pokušajima iste. Također je bitno naglasiti da je u tim predmetima, također, bio slučaj kažnjivosti prema čl. 51. KZ-a, a najčešće se radilo o stjecaju kaznenog djela zlouporabe osobne isprave i kaznenog djela prijevare (čl. 236. KZ-a) te kaznenog djela krivotvorenja isprave (čl. 278. KZ-a).

5. Zaključak

Krađa identiteta u stalnom je porastu od 1980-ih godina, a posljednjih desetljeća sve se češće događa putem Interneta, umjesto tradicionalnih metoda fizičke krađe identiteta. Neki od modernih načina krađe identiteta, uključuju *phishing*, gdje počinitelji koriste lažne e-poruke ili web stranice kako bi ukrali osobne podatke i *skimming*, gdje se uređaji koriste za neovlašteno čitanje podataka s bankovnih kartica.

Borba protiv počinitelja koji pokušavaju pribaviti i koristiti podatke vezane uz identitet donosi brojne izazove za policiju i kazneno pravosuđe. Analiza različitih definicija koje se koriste za opisivanje pojma krađe identiteta, kao i metoda dobivanja podataka vezanih uz identitet, vrste podataka koje počinitelji ciljaju i motivacije počinitelja, pokazuje da djela povezana s krađom identiteta imaju vrlo malo zajedničkog osim činjenice da općenito sadrže tri različite faze: prvo, pribavljanje informacija vezanih uz identitet; drugo, interakcija s tim informacijama (posjedovanje, prijenos); i konačno, njihovo korištenje za počinjenje kaznenog djela.

Što se tiče pravne reguliranosti krađe identitetea na razini EU-a, prijedlog Komisije je „da bi suradnja u provedbi zakona EU bila bolje ostvarena kada bi krađa identiteta bila kriminalizirana u svim državama članicama“.[132] No, i dalje ne postoji suglasnost treba li kriminalizirati krađu identiteta kao zasebno kazneno djelo ili ne, nego samo progoniti kroz naknadna kaznena djela, npr. prijevara, računalna prijevara. U Hrvatskoj se zakonodavni okvir temelji na specifičnoj odredbi (čl. 146. KZ-a) koja se fokusira na osobne podatke vezane uz identitet kao predmet pravne zaštite. Prednost tog pristupa je u tome što pokriva bilo koji oblik krađe identiteta, ne samo ako je počinjena putem interneta.

Bez obzira na rezultate rasprava o kriminalizaciji krađe identiteta na europskoj razini, važno je naglasiti da uspjeh u borbi protiv krađe identiteta nije prvenstveno pitanje dodatnih materijalnopravnih odredbi. Ostali aspekti, poput poboljšanja međunarodne suradnje među policijskim agencijama - za što okvir pruža Konvencija o kibernetičkom kriminalu - jednako su relevantni. Konačno, treba istaknuti da je rješavanje problema krađe identiteta kaznenopravnim odredbama samo jedan od mnogih pristupa; druge strategije, osobito preventivne mjere, edukacija korisnika interneta, razvoj sigurnijih postupaka identifikacije ili poboljšanje zakona o zaštiti podataka, jednako su, ako ne i važnije.

Za kraj, važno je ponovno naglasiti visoku *tamnu brojku* počinjenja ovog kaznenog djela, budući da osoba kojoj je ukraden identitet često postane svjesna krađe tek kad nastupe posljedice. Posljedično, žrtve se suočavaju s brojnim izazovima, uključujući financijske gubitke, emocionalni stres te narušen osjećaj sigurnosti. Stoga se preporučuje svima da budu izuzetno oprezni pri raspolaganju i korištenju svojih osobnih isprava i podataka.

[132] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime {SEC(2007) 641} {SEC(2007) 642}: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52007DC0267, 8. srpnja 2024.

Literatura

Knjige:

1. Dragičević, Dražen et al., Pravna informatika i pravo informacijskih tehnologija, Narodne novine, Zagreb, listopad 2015.
2. Horvatić, Željko ; Derenčinović, Davor ; Cvitanović, Leo, Kazneno pravo - opći dio I. Zagreb: Pravni fakultet Sveučilišta u Zagrebu, 2016
3. Cvitanović, Leo; Derenčinović, Davor; Dragičević Prtenjača, Marta; Maršavelski, Aleksandar; Munivrana Vajda, Maja; Roksandić Vidlička, Sunčana, Kazneno pravo – posebni dio, Pravni fakultet Sveučilišta u Zagrebu, 2017

Pravni izvori:

4. Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ, na snazi od 25.05.2018 (Opća uredba o zaštiti podataka)
5. Kazneni zakon (pročišćeni tekst, Narodne novine, 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23, 36/24)
6. Kazneni zakon (pročišćeni tekst, Narodne novine, 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11, 143/12)

Internetski članci i publikacije:

7. Kokot, Ivica, Kaznenopravna zaštita računalnih sustava, programa i podataka, Zagrebačka pravna revija, vol. 3, br. 3, 2014: https://hrcak.srce.hr/141877, 4. srpnja 2024.

8. Handbook on Identity-related Crime, United Nations Office on Drugs and Crime, April 2011, https://www.unodc.org/documents/congress/background-information/Corruption/Handbook_on_Identity-related_Crime_ENG.pdf, 3. srpnja 2024.
9. OECD (2009), Online Identity Theft, OECD Publishing, Paris, https://read.oecd-ilibrary.org/science-and-technology/online-identity-theft_9789264056596-en#page18, 3. srpnja 2024.
10. Study on online identity theft and identity-related crime, European Commission, Directorate-General for Migration and Home Affairs, 2022: https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1, 3. srpnja 2024.
11. Techniques of Identity Theft, Canadian Internet Policy and Public Interest Clinic, March, 2007: https://www.social-engineer.org/wiki/archives/IdTheif/IdTheif-Techniques.pdf, 3. srpnja 2024
12. Gercke, Marko, Internet-related Identity Theft, Project on Cybercrime, Council of Europe, November 2007: https://rm.coe.int/16802fa3a0, 4. srpnja 2024.
13. Hoofnagle, Crhis Jay, Identity Theft: Making the Known Unknown Known, Harvard Journal of Law & Technology, Volume 21, Number 1 Fall 2007: https://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech097.pdf, 4. srpnja 2024.
14. Jelenski, Milivoj; Šuperina, Marijan; Budiša, Josip, Kriminalitet platnim karticama (krađa identiteta, krivotvorenje i zlouporaba platne kartice)", Policija i sigurnost, vol.22, br. 3/2013: https://policijska-akademija.gov.hr/UserDocsImages/onkd/3-2013/jelenski_superina_budisa.pdf, 4. srpnja 2024.
15. Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft, European Commission, Centre for Strategy and Evaluation Services, 2012:

https://www.slideshare.net/slideshow/new-legal-framework-on-identity-theft-2012/30168033#7, 4. srpnja 2024.

16. OECD, Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures, OECD Digital Economy Papers No. 114: https://www.oecd-ilibrary.org/docserver/231503010627.pdf?expires=1720207258&id=id&accname=guest&checksum=5A9E3E47525EFD40B1C95D38CD8B9157, 5. srpnja 2024.
17. Vilić, Vida M., Phishing and pharming as forms of identity theft and identity abuse, Balkan Social Science Review, 2019, Vol 13, Issue 13: https://js.ugd.edu.mk/index.php/BSSR/article/view/3033/2743, 5. srpnja 2024.
18. Dragičević Prtenjača, Marta; Zagorec, Marina, Ponešto o privatnosti, pravu na privatnost i njezinoj zaštiti u Hrvatskoj kroz kazneno djelo Nedozvoljene uporabe osobnih podataka, Godišnjak Akademije pravnih znanosti Hrvatske, XIV, 2023, 1: https://hrcak.srce.hr/clanak/447566, 6. srpnja 2024.
19. Novoselec, Petar; Garačić, Ana, Primjena blažeg zakona nakon stupanja na snagu novog Kaznenog zakona, Hrvatski ljetopis za kazneno pravu i praksu, vol.19., br. 2., 2012: https://hrcak.srce.hr/file/163374, 6. srpnja 2024.
20. Ministarstvo unutarnjih poslova Republike Hrvatske, Overview of basic indicators for public safety in the Republic of Croatia for 2014 – 2023., Zagreb, 2023: https://mup.gov.hr/UserDocsImages/statistika/2024/3/Overview%20of%20the%20basic%20indicators%20for%20public%20safety_2014_2023_web.pdf, 6. srpnja 2024.
21. Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2023. godini, Ministarstvo unutarnjih poslova: služba za strateško planiranje, statistiku i unaprjeđenje rada, Zagreb, 2024:

https://mup.gov.hr/UserDocsImages/statistika/2024/3/Statisticki_pregled_2023_.pdf, 6. srpnja 2024