

Ivana Radić\*

## KLJUČNE DIGITALNE KOMPETENCIJE POLICIJSKIH SLUŽBENIKA POTREBNE U VRIJEME PANDEMIJE BOLESTI COVID-19

### Sažetak

Cilj je ovoga rada identificirati digitalne kompetencije koje su u vrijeme pandemije bolesti COVID-19 bile potrebne policijskim službenicima koji po naravi posla najviše komuniciraju s građanima, a to su djelatnici temeljne policije, kriminalističke policije koji rade na poslovima općeg kriminaliteta i kontakt-policije. Rad se sastoji od dva dijela: nakon pregleda relevantnih inozemnih primjera pokušaja regulacije digitalnih kompetencija policije slijedi prikaz kvalitativnog istraživanja provedenog u Hrvatskoj. Tijekom prosinca 2022. godine i siječnja 2023. godine održane su četiri fokusne skupine s deset sudionika istraživanja u svakoj skupini, odnosno tri u Policijskoj upravi osječko-baranjskoj i jedna u Policijskoj upravi požeško-slavonskoj. Rezultati polustrukturiranog intervjua pokazuju da su policijskim službenicima potrebne dvije kategorije digitalnih kompetencija koje bi se mogle operacionalizirati kao temeljna digitalna pismenost i osnovna kibernetička sigurnost, a na temelju uvodno prezentiranog i relevantnog primjera dobre prakse razvoja standarda digitalnih kompetencija policije. Glavno je ograničenje ovoga istraživanja da je ono provedeno samo u jednom dijelu Hrvatske. Iz toga proizlaze perspektive budućih istraživanja u smjeru ponavljanja istog istraživanja s policijskim službenicima u drugim policijskim upravama u Hrvatskoj. Tako bi se stekla potpunija slika potreba za digitalnim kompetencijama policijskih službenika u vrijeme pandemije bolesti COVID-19.

**Ključne riječi:** digitalne kompetencije, policija, pandemija COVID-19, Hrvatska

### 1. Uvod

Pandemija bolesti COVID-19 gotovo je preko noći promijenila glavne aspekte života modernog društva, uključujući i rad policije. Samo dva mjeseca nakon što je Svjetska zdravstvena organizacija proglasila pandemiju bolesti COVID-19, otprilike jedna trećina svjetske populacije bila je u nekom obliku karantene da bi se smanjilo

\* dr. sc. Ivana Radić, voditeljica Službe za javni red i sigurnost, PU požeško-slavonska, Hrvatska, iradic@mup.hr

širenje virusa (Warren, Gualco, Davidson i Edginton, 2020). Krajem ožujka 2020. Hrvatska je bila među zemljama s najstrožim restrikcijama u Europi jer je ušla u prvo potpuno zatvaranje (engl. *lockdown*). Tijekom pandemije svakodnevno je više od 2 600 policijskih službenika bilo angažirano u nadzoru i kontroli provedbe donesenih ključnih odluka u svrhu sprječavanja širenja zaraze. Za kontrolu provedbe zabrane napuštanja boravišta uspostavljena su 324 policijska punkta. To znači da je na ovim aktivnostima bila angažirana polovina policijskih operativnih snaga na terenu (Lobnikar, Christián, Balla, Kalmár, Cajner Mraović, Borovec i Sotlar, 2023). To su bile goleme nove obveze za policiju što nije pridonosilo kvalitetnim relacijama između policije i građana kao imperativa svake policijske organizacije u modernom demokratskom društvu. S druge strane, uobičajeno obavljanje policijskih poslova dobilo je nove modalitete u cilju prilagodbe novonastalim okolnostima, pri čemu su nužnost fizičkog distanciranja i komunikacije na daljinu predstavljali poseban izazov u odnosu na spomenuti imperativ i ulogu policije u modernom demokratskom društvu. Različite policijske organizacije prilagođavale su se tim okolnostima ne različite načine, pri čemu je veliku važnost predstavljala pretpandemijska uporaba kanala komunikacije na daljinu. Istraživanje provedeno u devet europskih država (Denef, Kaptein, Bayrel i Ramirez, 2012) pokazalo je da je primjerice integracija društvenih mreža u svakodnevni rad policije svakako neminovna, ali se događa sasvim različitom dinamikom u različitim dijelovima Europe. Prije pandemije bolesti COVID-19 hrvatska policija imala je reguliranu komunikaciju s građanima putem elektroničke pošte, a komunikacija putem društvenih mreža bila je tek u razvoju i ograničena na policijske službenike za odnose s javnošću. Ta okolnost ne znači da hrvatska policija ne prihvaća intenziviranje komunikacije u kibernetičkom prostoru, jer je situacija zapravo sasvim suprotna (Jarolimek, 2019), već ona proizlazi iz ukupnog konteksta razvoja policije u Hrvatskoj.

Modeli rada policije, koji su tijekom nekoliko prethodnih desetljeća razvijani u modernom demokratskom svijetu, bili su fokusirani na zamjenu rigidnih birokratskih i autoritativnih modela rada policije novim modelima koji jamče veću otvorenost policije građanima i zajednici kojoj služe i koju štite (Lobnikar, Sotlar i Meško, 2013). U tom su se smislu pojavili razvojni trendovi koji su zajednički svim modernim demokratskim policijskim sustavima: profesionalizacija, tehnološka modernizacija, demokratizacija, internacionalizacija i pluralizacija policije (Newburn, 2008). Za hrvatsku policiju, kao i za policije ostalih postsocijalističkih država u ovome dijelu Europe, navedeni su se procesi događali znatno brže, odnosno u znatno kraćem vremenu nego li je to bio slučaj u policijskim organizacijama u državama stabilnih demokracija, s obzirom na to da su ti procesi počeli tek s demokratskim promjenama i tranzicijom tih država početkom devedesetih godina 20. stoljeća. U tim policijskim službama dodatno su još bili prisutni procesi europeizacije, depolitizacije i unutarnje demokratiza-

cije (Meško, Sotlar i Lobnikar, 2014). Dakle, dok se policijske organizacije u državama stabilne demokracije još od početka ovog tisućljeća bave digitalizacijom komunikacije kao jednim od aspekata intenzivne primjene modernih tehnologija u obavljanju svakodnevnih policijskih poslova (Montasari, Carpenter i Masys, 2023; O'Connor i Zaidi, 2021; Walby i Wilkinson, 2022), policije u postsocijalističkim državama uz te nove trendove prolaze i intenzivne reforme u kontekstu ukupne demokratizacije javne uprave, što svakako utječe na dinamiku tih procesa (Koprić, 2016).

Vitez i Balgač (2016) u prikazu razvoja hrvatske policije naglašavaju da je pristupačnost i kompetentnost policije kvalitetna javna usluga koju žele građani, a da razvoj modernih tehnologija otvara niz mogućnosti da bi policija bila brža, efikasnija, uspješnija i racionalnija. Upravo je ta činjenica bila od vitalne važnosti u okolnostima pandemije bolesti COVID-19 kada je u situaciji socijalne distance i ograničavanja kontakata uživo policija trebala održati kvalitetnu komunikaciju s građanima, pa je nužno dio svojih aktivnosti premjestila u kibernetički prostor koristeći mogućnosti digitalnih kanala komunikacije. No, takva komunikacija zahtijeva i posebne kompetencije koje trenutno nisu zastupljene na zadovoljavajućoj razini u temeljnoj obuci policijskih službenika u našoj zemlji. Stoga je cilj ovoga rada dati pregled inozemnih rješenja definiranja digitalnih kompetencija policije i identificirati digitalne kompetencije koje su bile potrebne policiji za komunikaciju s građanima u vrijeme pandemije bolesti COVID-19.

## **2. Inozemni primjeri definiranja digitalnih kompetencija policijskih službenika**

S obzirom na to da je Hrvatska članica Europske unije, prvi predmet interesa bio nam je upravo taj međunarodni kontekst. Agencija Europske unije za osposobljavanje u području izvršavanja zakonodavstva – CEPOL prepoznaje potrebu definiranja i razvoja digitalnih kompetencija policijskih službenika. U strateškom dokumentu (CEPOL, 2021) u kojem ova važna europska organizacija daje procjenu potreba europskih policija za obukom u razdoblju između 2022. i 2025. godine višestruko su istaknute kompetencije korištenja društvenih mreža i komunikacije u virtualnom prostoru. U dokumentu (CEPOL, 2021) se također navode glavni raskoraci između potrebnog i aktualnog stanja na temelju analize dokumenata i konzultacija s ekspertima, pa se prioritet daje upravo digitalnim vještinama i upotrebi novih tehnologija te se, između ostalog, izrijeком navode i društvene mreže kao važno područje digitalnih vještina.

U detaljnom popisu potrebnih edukacija društvene se mreže spominju u području upotrebe novih tehnologija, ali i u prevenciji kriminaliteta. Dokumentom CEPOL-a (2021), a na temelju prethodno utvrđenih nedostataka, definiraju se prioriteti edukacije po područjima, pa su društvene mreže prisutne i u problematici suzbijanja

trgovanja ljudima s obzirom na to da mogu biti dragocjen izvor informacija. Počinitelji kaznenih djela koriste se prednostima digitalnih komunikacija tijekom krijumčarenja ljudi, pa upravo nedostatak adekvatnih vještina među policijskim službenicima za odgovor na upotrebu digitalnih platformi, društvenih medija i mobilnih aplikacija od strane kriminalaca ograničava uspjeh u procesuiranju počinitelja kaznenih djela. Još jedan od prioriteta jesu obuke za borbu protiv kršenja intelektualnog vlasništva i krivotvorenja roba i valuta.

Iako CEPOL (2021) u ovom dokumentu jasno pozicionira potrebe za digitalnim kompetencijama, on ih dalje ne operacionalizira. Kao mogući relevantan primjer dobre prakse vrijedi istaknuti projekt kanadske policije koji je imao za cilj razviti standarde digitalnih kompetencija (Beesley, 2021). Naime, s obzirom na to da se radi o recentnom projektu kojim su identificirane potrebne digitalne kompetencije za policijske službenike koji rade na različitim vrstama poslova, dakle od svih policijskih službenika koji imaju pristup računalu i internetu do onih koji se bave kriminalističkim istragama kibernetičkog kriminaliteta, moguće je iskoristiti rezultate tog istraživanja kao okvir za definiranje potreba digitalnih kompetencija policijskih službenika u Hrvatskoj. Dodatno je potrebno naglasiti da se kanadski projekt koristio Bloomovom taksonomijom pri definiranju razina pojedinih digitalnih kompetencija, što je sukladno metodologiji europskog i hrvatskog kvalifikacijskog okvira. U Tablici 1 možemo naći opis tih razina.

**Tablica 1.** Razine kompetencija

Razina 1	policijski službenik primjenjuje uvodno znanje u rutinskim i predvidljivim situacijama uz pomoć smjernica
Razina 2	policijski službenik primjenjuje osnovno znanje u nizu tipičnih situacija koje predstavljaju manje izazove; policijskom službeniku potrebno je pružiti smjernice, ali je prisutna određena razina individualne autonomije ili odgovornosti
Razina 3	policijski službenik primjenjuje dobro znanje u nizu netipičnih situacija umjerene složenosti uz minimalne smjernice ili samostalno
Razina 4	policijski službenik primjenjuje napredno znanje u širokom rasponu složenih situacija te usmjerava druge stručnjake
Razina 5	policijski službenik primjenjuje napredna znanja u najsloženijim i nepredvidivim situacijama, razvija nove pristupe, metode ili politike u tom području te pruža smjernice na nacionalnoj i međunarodnoj razini

Izvor: Beesley (2021: 21, prema Canadian Police Knowledge Network, 2020).

S obzirom na to da su predmet ovoga rada digitalne kompetencije policijskih službenika koji najviše komuniciraju s građanima, iz rezultata kanadskog projekta (Beesley, 2021) izdvojili smo dvije kategorije digitalnih kompetencija koje su neophodne policijskim službenicima: (1) digitalna pismenost i korištenje interneta i (2) kibernetička higijena i kibernetička sigurnost.

Kompetencija digitalne pismenosti i upotrebe interneta odnosi se na sposobnost pronalaženja, vrednovanja, korištenja, dijeljenja i kreiranja sadržaja s pomoću informacijskih tehnologija i interneta (Beesley, 2021: 23). Detaljan opis navedenih kompetencija po razinama složenosti nalazi se u Tablici 2.

**Tablica 2.** Kompetencije digitalne pismenosti i upotrebe interneta

Razina 1	policijski službenik primjenjuje uvodno znanje u rutinskim i predvidljivim situacijama uz pomoć smjernica	<ul style="list-style-type: none"> <li>– posjeduje svijest o često korištenom hardveru i softveru</li> <li>– posjeduje svijest o radu računalnog hardvera</li> <li>– razumije pretraživanje, dohvaćanje i pohranjivanje podataka, informacija i sadržaja u digitalnim okruženjima</li> <li>– posjeduje sposobnost interakcije putem niza digitalnih komunikacijskih sredstava uključujući elektroničku poštu u određenom kontekstu</li> <li>– pridržava se politika i postupaka povezanih s korištenjem računala, digitalnih uređaja i mreža</li> <li>– po potrebi traži savjete stručnjaka za odgovarajuća područja</li> <li>– posjeduje svijest o uobičajenim internetskim protokolima</li> <li>– primjenjuje razne alate za pretraživanje, dohvaćanje i pohranjivanje podataka, informacija i sadržaja u digitalnim okruženjima</li> <li>– koristi se uobičajenim softverom za obradu teksta i proračunske tablice</li> <li>– koristi se različitim softverima za izradu izvještaja i prezentacija</li> <li>– koristi se raznim softverima za pomoć u istragama</li> <li>– razumije digitalne otiske u internetskom okruženju</li> <li>– posjeduje svijest o hardveru i softveru virtualne privatne mreže, vatrozidima te aplikacijama infrastrukture javnih ključeva</li> <li>– pruža smjernice i savjete o hardverskim i softverskim aplikacijama koje se obično koriste u kontekstu provedbe zakona</li> <li>– upoznat je s radom na internetu i intranetu, e-trgovinom, e-poslovanjem i konvergentnim tehnologijama, mrežnim komunikacijskim protokolima, mrežnom arhitekturom i topologijom, virtualnim okruženjem, ručnim tehnologijama, bazama podataka i specijaliziranim softverima za testiranje i praćenje</li> </ul>
Razina 2	policijski službenik primjenjuje osnovno znanje u nizu tipičnih situacija koje predstavljaju manje izazove; policijskom službeniku potrebno je pružiti smjernice, ali je prisutna i određena razina individualne autonomije ili odgovornosti	<ul style="list-style-type: none"> <li>– razumije računalne periferne uređaje i njihov rad</li> <li>– posjeduje svijest o uobičajenim internetskim protokolima</li> <li>– primjenjuje razne alate za pretraživanje, dohvaćanje i pohranjivanje podataka, informacija i sadržaja u digitalnim okruženjima</li> <li>– koristi se uobičajenim softverom za obradu teksta i proračunske tablice</li> <li>– koristi se različitim softverima za izradu izvještaja i prezentacija</li> <li>– koristi se raznim softverima za pomoć u istragama</li> <li>– razumije digitalne otiske u internetskom okruženju</li> </ul>

		<ul style="list-style-type: none"> <li>– posjeduje svijest o hardveru i softveru virtualne privatne mreže, vatrozidima te aplikacijama infrastrukture javnih ključeva</li> </ul>
Razina 3	<p>policijski službenik primjenjuje dobro znanje u nizu netipičnih situacija umjerene složenosti uz minimalne smjernice ili samostalno</p>	<ul style="list-style-type: none"> <li>– upoznat je s novim tehnologijama i tehnologijama u nastajanju</li> <li>– pruža smjernice i savjete o hardverskim i softverskim aplikacijama koje se obično koriste u kontekstu provedbe zakona</li> <li>– upoznat je s radom na internetu i intranetu, e-trgovinom, e-poslovanjem i konvergentnim tehnologijama, mrežnim komunikacijskim protokolima, mrežnom arhitekturom i topologijom, virtualnim okruženjem, ručnim tehnologijama, bazama podataka i specijaliziranim softverima za testiranje i praćenje</li> <li>– razumije i pristupa internetskim tržištima uključujući kriminalna tržišta ili ona koja se odnose na kriminal kao uslugu</li> <li>– razumije Dark Web, TOR kriminalna tržišta i trendove</li> </ul>
Razina 4	<p>policijski službenik primjenjuje napredno znanje u širokom rasponu složenih situacija te usmjerava druge stručnjake</p>	<ul style="list-style-type: none"> <li>– trenira i obučava policijske službenike u područjima digitalne pismenosti</li> <li>– daje smjernice o složenim pitanjima</li> <li>– daje savjete o pitanjima vezanim za digitalnu pismenost u kontekstu provedbe zakona</li> <li>– ocjenjuje operativno okruženje i daje strateške smjernice vodstvu</li> <li>– povezuje se s vanjskim agencijama i drugim dionicima</li> <li>– identificira potrebu za istraživanjem i razvojem novih tehnika i tehnologija</li> <li>– razumije protokole prijenosa podataka</li> </ul>
Razina 5	<p>policijski službenik primjenjuje napredna znanja u najsloženijim i nepredvidivim situacijama, razvija nove pristupe, metode ili politike u tom području te pruža smjernice na nacionalnoj i međunarodnoj razini</p>	<ul style="list-style-type: none"> <li>– stvara alate, metode i tehnike za digitalnu forenzičku analizu</li> <li>– daje stručne savjete o pitanjima digitalne pismenosti u kontekstu provedbe zakona na nacionalnoj i međunarodnoj razini</li> <li>– djeluje kao predmetni stručnjak u razvoju i pružanju specijalizirane obuke</li> <li>– djeluje kao predmetni stručnjak u razvoju zakonodavstva, propisa ili politika povezanih s korištenjem tehnologija</li> <li>– član je strukovnih udruga</li> <li>– objavljuje istraživanja i bijele knjige</li> <li>– izlaže na domaćim i međunarodnim konferencijama</li> </ul>

Izvor: Beesley (2021: 24-25)

Sljedeća se kategorija digitalnih kompetencija (Beesley, 2021) odnosi na kibernetičku higijenu i kibernetičku sigurnost, odnosno na prakse koje primjenjuju korisnici računala i ostalih informacijskih tehnologija da bi održali sustav zdravim i unaprijedili mrežnu sigurnost. Opis ove kategorije kompetencija po pripadajućim razinama nalazi se u Tablici 3.

**Tablica 3. Kompetencije kibernetičke higijene i kibernetičke sigurnosti**

Razina 1	policijski službenik primjenjuje uvodno znanje u rutinskim i predvidljivim situacijama uz smjernice	<ul style="list-style-type: none"> <li>– posjeduje svijest o kibernetičkoj higijeni i najboljim praksama kibernetičke sigurnosti</li> <li>– posjeduje svijest o društvenom inženjeringu i krađi identiteta kao potencijalnoj opasnosti</li> <li>– posjeduje svijest o tehnikama zaštite uređaja i digitalnog sadržaja</li> <li>– posjeduje svijest o rizicima i prijetnjama u digitalnim okruženjima</li> <li>– posjeduje svijest o korporativnim praksama i politikama kibernetičke sigurnosti uključujući ovlaštenu upotrebu hardvera i softvera</li> <li>– razumije koncept digitalnog otiska u kontekstu provedbe zakona</li> <li>– razumije politike lozinki i integritet lozinki</li> <li>– po potrebi traži savjete stručnjaka za odgovarajuća područja</li> </ul>
Razina 2	policijski službenik primjenjuje osnovno znanje u nizu tipičnih situacija koje predstavljaju ograničene izazove; policijskom službeniku potrebno je pružiti smjernice, ali je prisutna određena individualna autonomija i odgovornost	<ul style="list-style-type: none"> <li>– razumije internetsku sigurnost i privatnost</li> <li>– posjeduje svijest o potrebi zaštite identiteta na internetu</li> <li>– primjenjuje pravila i protokole za zaštitu osobnih i korporativnih podataka i kibernetičke sigurnosti</li> <li>– razumije i primjenjuje tehnike za postupanje i ograničavanje osobnih podataka proizvedenih putem digitalnih alata i okruženja</li> <li>– razumije korištenje društvenog inženjeringa i često korištene tehnike krađe identiteta</li> </ul>
Razina 3	policijski službenik primjenjuje dobro znanje u nizu netipičnih situacija umjerenе složenosti uz minimalne smjernice ili samostalno	<ul style="list-style-type: none"> <li>– upoznat je s novom kibernetičkom sigurnošću i novim kibernetičkim prijetnjama</li> <li>– daje smjernice članovima službe o kibernetičkoj higijeni i kibernetičkoj sigurnosti uključujući smanjenje digitalnog otiska</li> <li>– razumije tehnologije i komponente mrežne infrastrukture</li> <li>– primjenjuje načela kibernetičke sigurnosti korištenjem tehnologija nadzora mreže</li> <li>– primjenjuje tehnike za izradu analize atribucije nakon eksploatacije</li> </ul>
Razina 4	policijski službenik primjenjuje napredno znanje u širokom rasponu složenih situacija, usmjerava druge stručnjake	<ul style="list-style-type: none"> <li>– razumije složeno sigurnosno okruženje uključujući arhitekturu, infrastrukturu, fizičko upravljanje, upravljanje identitetom i pristupom, kao i tehnologije koje se razvijaju uz uključivanje višestrukih dionika</li> <li>– primjenjuje tehnike dizajna, integracije tehnologije i analize sustava uključujući metode ispitivanja i istraživanja te detaljne prakse izviđanja</li> <li>– ocjenjuje i preporučuje promjene korporativnih praksi i politika kibernetičke sigurnosti</li> <li>– služi kao predmetni stručnjak u razvoju i pružanju specijalizirane obuke</li> <li>– koristi se uobičajenim alatima i tehnikama testiranja prodora u svrhu testiranja kibernetičke sigurnosti</li> </ul>

Razina 5	policijski službenik primjenjuje napredna znanja u najsloženijim i nepredvidivim situacijama, razvija nove pristupe, metode ili politike u tom području te pruža smjernice na nacionalnoj i međunarodnoj razini	<ul style="list-style-type: none"><li>– stvara nove alate, metode i tehnike za digitalnu forenzičku analizu nakon napada</li><li>– daje stručne savjete o pitanjima vezanim za kibernetičku higijenu i kibernetičku sigurnost u kontekstu provedbe zakona na nacionalnoj i međunarodnoj razini</li><li>– djeluje kao predmetni stručnjak u razvoju propisa ili politika povezanih s kibernetičkom i informacijskom sigurnošću</li><li>– član je strukovnih udruga</li><li>– objavljuje istraživanja i bijele knjige</li><li>– izlaže na domaćim i međunarodnim skupovima</li></ul>
----------	---	--

Izvor: Beesley (2021: 26-27)

Navedene kompetencije mogle bi se sažeti u obliku preporuka Europske unije za razvoj digitalnih kompetencija putem cjeloživotnog obrazovanja.

Naime, ECDL/ICDL<sup>1</sup> program, koji je osmišljen da bi pojedincima omogućio stjecanje temeljnih znanja i vještina u radu s računalima i softverskim aplikacijama, doživio je transformaciju 2014. godine prelaskom u program cjeloživotnog učenja s ciljem održavanja ECDL ID-a<sup>2</sup> i omogućavanja prekvalifikacije i nadogradnje vještina. Treba istaknuti da ECDL/ICDL sve intenzivnije stavlja fokus ne samo na vještine digitalne pismenosti, već i na rješavanje problema, kao što je slučaj u npr. računalnom modulu. Iako rješenja leže u kodiranju, ovaj program nije namijenjen stručnjacima programerima, već skupini ljudi koja će u sklopu navedenog modula steći dovoljno znanja za rješavanje zadanog problema. „Nastavni plan i program modula obuhvaća sljedeće teme:

- opći računalni pojmovi
- metode računalnog razmišljanja kao što su rješavanje problema i algoritmi
- osnove kodiranja (varijable, vrste podataka...)
- pisanje i korištenje koda (logika, iteracija...)
- testiranje i ispravljanje pogrešaka” (Bieber, 2022: 454).

Prema Bieberu (2022) austrijska je policijska škola od 2018. godine uključila ECDL program u svoje kurikule, što omogućuje budućim policajcima stjecanje ECDL certifikata tijekom osposobljavanja, a cilj je policijske škole da cjelokupni policijski sastav prođe navedenu obuku. To pokazuje da je važnost ECDL programa za poboljšanje digitalnih vještina među policijskim snagama u pravo vrijeme prepoznalo Ministarstvo unutarnjih poslova koje je odgovorno za obrazovanje policijskih službenika u Austriji. Tako je postavljen visoki standard digitalnih vještina u policijskim školama na

<sup>1</sup> European Computer Driving Licence (ECDL) europski je priznat program certificiranja računalne pismenosti koji se 2019. godine transformirao u International Computer Driving License (ICDL), međunarodno priznat program certificiranja računalne pismenosti.

<sup>2</sup> European Computer Driving Licence ID jedinstveni je identifikacijski broj koji se dodjeljuje polaznicima koji uspješno polože ECDL/ICDL ispite i ostvare certifikat o posjedovanju ECDL/ICDL diplome.



području Austrije u kojoj se planira godišnje povećati broj studenata sa sadašnjih 2 000 na gotovo 4 000 u sljedećih nekoliko godina. Teme poput informacijsko-tehnološkijske sigurnosti, zaštite podataka i metoda računalnog razmišljanja ključne su vještine u današnjem svijetu, pa će se jednako na njih staviti naglasak i u obrazovanju policajaca.

### **3. Metode**

#### **3.1. Uzorak**

Ovaj je rad dio autoričine doktorske disertacije „Komunikacijski kanali policije tijekom pandemije COVID-19 i njihov odjek na instituciju i zajednicu” obranjen na Sveučilištu Sjever.

Ciljanu populaciju kvantitativnog istraživanja u ovome radu čine djelatnici temeljne policije, kriminalističke policije koji rade na poslovima općeg kriminaliteta i kontakt-policije u Policijskoj upravi osječko-baranjskoj i Policijskoj upravi požeško-slavonskoj. Kvalitativno istraživanje predstavljeno u ovom radu uslijedilo je nakon kvantitativnog istraživanja da bi se detaljnije objasnili rezultati dobiveni kvantitativnim istraživanjem. Prvo je formiran uzorak kvantitativnoga dijela istraživanja. Radilo se o prigodnom uzorku policijskih službenika navedenih kategorija koji su se zatekli u smjeni u vrijeme dolaska anketara. Od ukupno 1 325 policijskih službenika temeljne policije i kriminalističke policije koji rade na poslovima općeg kriminaliteta te kontakt-policajaca iz ove dvije policijske uprave formiran je prigodni uzorak od 367 službenika: 267 iz Policijske uprave osječko-baranjske i 100 iz Policijske uprave požeško-slavonske. Nesrazmjer između veličine ta dva dijela uzorka proizlazi iz razlike u broju policijskih službenika u navedenim policijskim upravama. Prilikom formiranja uzorka kvantitativnoga dijela istraživanja vodilo se računa da pojedine kategorije policijskih službenika budu zastupljene s najmanje 10 % ukupnog broja.

Na temelju uzorka kvantitativnoga dijela istraživanja formiran je uzorak kvalitativnoga dijela istraživanja po kriteriju da čini 10 % uzroka kvantitativnoga dijela istraživanja i da vjerno odražava promatrane kategorije policijskih službenika. Tako su formirane tri fokusne skupine po deset sudionika u Policijskoj upravi osječko-baranjskoj i jedna s deset sudionika u Policijskoj upravi požeško-slavonskoj.

#### **3.2. Instrument**

Prethodno spomenuta studija kanadske policije (Beesley, 2021) kojom su definirani standardi digitalnih kompetencija uključuje komponentu kvalitativnog istraživanja, pa smo se odlučili za isti metodološki pristup te smo pri izradi pitanja imali u vidu pitanja koja su tamo postavljena u fokusne skupine. Tako je formulirano sljedećih osam pitanja koja čine strukturirani dio polustrukturiranog intervjua:

1. Kojim ste se kanalima digitalne komunikacije s građanima koristili u vrijeme pandemije bolesti COVID-19?
2. Ako se niste koristili kanalima digitalne komunikacije u vrijeme pandemije bolesti COVID-19, koji su bili razlozi za to? (*nedostatak potrebe, znanja, opreme, uputa, regulative...*)
3. Kojim se kanalima digitalne komunikacije trenutno koristite prilikom obavljanja policijskih poslova i primjene policijskih ovlasti? (*elektronička pošta, mobilne aplikacije za e-dojave, Viber, WhatsApp, Twitter, Facebook, društvene grupe i sl.*)
4. Koje digitalne kompetencije imate? (*tekstna poruka (SMS), videopoziv, elektronička pošta, internetska stranica, chat (video), chatbot, interaktivni portal („Nacionalne evidencije nestalih osoba – NENO”), platforme za izravno dijeljenje sadržaja (WhatsApp, Viber, Twitter, Telegram, Reddit, Discord i dr.), društvene mreže (Facebook, Instagram, LinkedIn, TikTok i dr.) i razne aplikacije (npr. aplikacija „MUP – Sigurnost i povjerenje” za elektroničke dojave sumnjivih događaja)*)
5. Kako biste procijenili Vašu digitalnu pismenost?
6. Kako biste procijenili Vaše poznavanje sigurnosti na internetu?
7. Koje digitalne kompetencije smatrate da biste trebali imati za obavljanje Vašeg posla?
8. Postoje li u Vašoj ustrojstvenoj jedinici pravila ponašanja na internetu? (*ako ne postoje, jesu li potrebna, a ako postoje, jesu li dostatna*)

S obzirom na to da je bilo realno očekivati da će navedena pitanja potaknuti sudionike istraživanja i na razgovor o sadržajima koji nisu direktno obuhvaćeni ovim pitanjima, a mogu biti relevantni za ostvarenje cilja ovoga rada, odlučili smo se za formu polustrukturiranog intervjua.

### **3.3. Postupak**

Tijekom prosinca 2022. godine i siječnja 2023. godine održane su četiri fokusne skupine s deset sudionika istraživanja u svakoj skupini: tri u Policijskoj upravi osječko-baranjskoj i jedna u Policijskoj upravi požeško-slavonskoj. Fokusna skupina u Policijskoj upravi požeško-slavonskoj provedena je 28. prosinca 2022., a fokusne skupine u Policijskoj upravi osječko-baranjskoj provedene su 11. siječnja 2023. godine. Sve fokusne skupine provedene su u radno vrijeme sudionika istraživanja i u dogovoru s njihovim nadređenima da se ne bi ometalo obavljanje posla.

Svaku fokusnu skupinu moderirale su dvije iste istraživačice. Na početku svake fokusne skupine moderatorice su se predstavile i zahvalile sudionicima što su pristali sudjelovati u istraživanju. Zatim je jedna od moderatorica objasnila sudionicima istraživanja da će oni svojim sudjelovanjem dati doprinos identifikaciji ključnih komponenti digitalne komunikacije i potrebnih digitalnih kompetencija u smislu zna-

nja, vještina i stavova koji su bili potrebni u vrijeme globalne pandemije bolesti COVID-19. Zatim je sudionicima istraživanja objasnila da su predmet ovoga istraživanja kanali digitalne komunikacije: tekstna poruka (SMS), videopoziv, elektronička pošta, internetska stranica, *chat* (video), *chatbot*, interaktivni portal („Nacionalne evidencije nestalih osoba – NENO”), platforme za izravno dijeljenje sadržaja (*WhatsApp*, *Viber*, *Twitter*, *Telegram*, *Reddit*, *Discord* i dr.), društvene mreže (*Facebook*, *Instagram*, *LinkedIn*, *TikTok* i dr.) i razne aplikacije (npr. aplikacija „MUP – Sigurnost i povjerenje” za e-dojave sumnjivih događaja). Istaknula je da se jednim dijelom tih kanala digitalne komunikacije svi koristimo u svakodnevnom osobnom životu, a tijekom razgovora u fokusnoj skupini razgovarat će se o uporabi tih kanala u svrhu obavljanja svakodnevnih policijskih poslova. Pri tome je naglasila da sudionici istraživanja kao zaposlenici MUP-a u svom svakodnevnom radu (neki više, a neki manje) kontaktiraju s građanima putem raznih komunikacijskih kanala te su upravo zato referentne osobe za razgovor o navedenoj tematici.

Nakon toga su objašnjeni etički aspekti istraživanja, odnosno istaknuto je da je istraživanje dobrovoljno i anonimno te će se dobiveni podaci upotrebljavati isključivo zbirno i bez ikakvih detalja koji bi mogli indicirati identitet sudionika. Objasnjeno je i da sudjelovanje u ovome istraživanju za sudionike ne nosi nikakav rizik, ali ni direktnu korist, već će pridonijeti boljem razumijevanju digitalnih kompetencija koje su neophodne policijskim službenicima da bi se u obavljanju policijskih poslova mogli učinkovito koristiti digitalnim kanalima komunikacije.

Sudionicima istraživanja također je objašnjeno da će razgovor biti sniman s pomoću više diktafona da bi sve ostalo zabilježeno, a da će snimke biti dostupne isključivo prisutnim istraživačicama. Također, istaknuto je da će snimke biti anonimno obrađene i korištene isključivo za potrebe znanstvenog rada. Nakon što su se sudionici istraživanja s time složili, na stol su raspoređeni diktafoni u modusu snimanja. Na kraju ovoga uvodnog dijela sudionici istraživanja zamoljeni su da na pitanja odgovoraju istinito, odnosno onako kako oni misle i osjećaju.

Intervju sa svakom fokusnom skupinom trajao je između sat i sat i pol, odnosno najkraći sat i 10 minuta, a najdulji sat i 30 minuta. Rezultati su prikazani i analizirani po pitanjima iz strukturiranoga dijela intervjua.

Rezultati fokusnih skupina prikazani su redom po postavljenim pitanjima iz strukturiranoga dijela intervjua. Svako je pitanje analizirano zasebno, a onda su metodama analize i sinteze izvedeni zaključci.

## 4. Rezultati i rasprava

U nastavku razgovora u svakoj se fokusnoj skupini od sudionika istraživanja tražilo da procijene svoje digitalne kompetencije u vrijeme pandemije bolesti COVID-19 i u trenutku provedbe istraživanja. Kao što je prethodno opisano u metodologiji istraživanja, pitanja u ovome dijelu razgovora bila su strukturirana tako da uključuju ključne komponente digitalne komunikacije sukladno relevantnim međunarodnim i nacionalnim dokumentima.

1. Koje digitalne kompetencije imate? (*tekstna poruka (SMS), videopoziv, elektronička pošta, internetska stranica, chat (video), chatbot, interaktivni portal („Nacionalne evidencije nestalih osoba – NENO”), platforme za izravno dijeljenje sadržaja (WhatsApp, Viber, Twitter, Telegram, Reddit, Discord i dr.), društvene mreže (Facebook, Instagram, LinkedIn, TikTok i dr.) i razne aplikacije (npr. aplikacija „MUP – Sigurnost i povjerenje” za e-dojave sumnjivih događaja)*)

Policijski službenici, kao i građani Hrvatske i većine svijeta, ako nisu dotada, morali su se što brže i učinkovitije digitalno opismeniti te prilagoditi korištenju raznih oblika digitalne komunikacije poput elektroničke pošte, tekstnih poruka (SMS), videopoziva te društvenih mreža i platformi za izravno dijeljenje sadržaja. Radni su se sastanci i edukacije tijekom pandemije odvijali putem digitalnih kanala, što je dodatno ubrzalo proces prilagodbe.

*„Ako krenemo od ovih kolegija i sastanaka s postajama, imali smo računalo, kameru, držali smo razmak i održavali mjesečni kolegij, sve je rađeno tako.”*

2. Kako biste procijenili Vašu digitalnu pismenost?

Usprkos stalnom praćenju napretka tehnologije i znanju koje posjeduju o kanalima digitalne komunikacije, policijski su službenici svjesni da je ovo područje konstantno izloženo brzom razvoju i inovacijama. Zbog toga je izazovno održati korak s novim aplikacijama i tehnološkim rješenjima koja postaju sve sofisticiranija. Kako bi uspješno pratili razinu potrebne digitalne pismenosti, smatraju da bi bilo najkorisnije pohađati različite edukacije i radionice.

*„Pa nikad ne možemo znati dovoljno što se konkretno tiče našeg posla. Nedavno smo imali maloljetnika koji je uhvaćen s marihuanom i kad sam obavljala s njim razgovor, čovjek mi je rekao da je putem aplikacije stupio u kontakt, poslao samo nadimak osobi i napisao je koliko grama i ulicu. Nit’ zna tko je, nit’ je tu broj telefona ukucan. Uglavnom, našli su se na jednom mjestu, ovaj je njemu dao i to je to. Znači, toliko ima tih novih aplikacija da se to više ne može pratiti jer nema nikakav potpis ili poveznica s brojem telefona. Jer mi smo svi navikli na neke kanale gdje mi istražujemo, ali dosta je teško ako... Mi smo svi navikli na Viber, WhatsApp... to je to, a u biti ima toliko tih novih aplikacija koje nam uopće nisu poznate. Tako da bi se svatko tko je zainteresiran za ovaj posao trebao educirati... Aplikacija se zove Wickr Me. Nikad čula.”*

Razgovor o digitalnoj pismenosti otvara i pitanje tehničkih problema s kojima se suočavaju policijski službenici prilikom korištenja tehnologije. Dio službenika koji se nije mogao prilagoditi otišao je u mirovinu, a drugi dio mora naučiti kako se koristiti novom tehnologijom. Međutim, tehnička podrška koja prati njihove zahtjeve nije adekvatna zbog već spomenutih zastarjelih računala ili spore brzine interneta, što doводи do problema s kojima se zaposlenici suočavaju prilikom obavljanja svakodnevnih poslovnih zadataka koji zahtijevaju korištenje tehnologije.

*„Oni koji se nisu privikli kod nas su otišli u mirovinu, oni kojima je ta tehnologija bila strana.”*

*„Policijski će se službenici priviknuti. Naučit će, ali tehnička podrška koja prati te naše zahtjeve nije na adekvatnom nivou. Mi imamo računala stara 12, 15 godina.”*

*„Ne možeš sa sedmicom raditi, moraš imati Windows 10. Pa što je četiri megabita u sekundi, što je tri, četiri megabita u sekundi, a mobitel ti je, ne znam koliko, 50. A tu je na našem službenom internetu četiri megabita. Pa ne možeš ništa, on vrti, pa vrti, ne možeš otvoriti ništa.”*

*„To sam baš jučer gledao kad smo pisali onaj dopis u e-gopu, pa vrti, vrti pola sata, izbaci me i ne može poslati. I onda sam išao namjerno vidjeti kolika mi je brzina na internetu, četiri megabitno. Normalno da nisam mogao poslati dopis.”*

### 3. Kako biste procijenili Vaše poznavanje sigurnosti na internetu?

Iz odgovora policijskih službenika na pitanja o sigurnosti na internetu može se zaključiti da postoji određena grupacija djelatnika koji su prošli odgovarajuću edukaciju o zaštiti od krađe podataka prilikom elektroničkog plaćanja te kako prepoznati internetske stranice koje su potencijalno opasne. Međutim, većina operativnog sastava još uvijek nema dovoljno znanja o sigurnosti na internetu, što stvara poteškoće ne samo na poslu, već i u njihovom privatnom životu.

*„Seminar u Njemačkoj koji smo imali preko Tispola, sad je to Roadpol, imaju posebnu tehničku grupu koja se bavi s tim. Tako da su nas oni i upoznali sa sigurnosnim adresama, s TFT-om, s krađom podataka na blizinu, da znamo da takve neke stvari postoje i da su moguće. E sad, dal' je to dovoljno?”*

*„Ali imamo mi i tečajeve koji obučavaju policijske službenike i na faksu i ovako u Valbandonu... krivotvorina, računalna sigurnost.”*

*„Događalo se isto da su pokušaji prijave bili izvedeni na onoj stranici od Pošte. Bilo je i da su naši kolege nasjeli na to.”*

Jedan djelatnik kriminalističke policije izjavio je da je prošao tečajeve GDPR-a i edukaciju o sigurnosti u kibernetičkom prostoru putem e-učionice koju organizira MUP. Iako je takva mogućnost dostupna i drugim djelatnicima, odaziv je na ovu edukaciju slab s obzirom na to da je sudjelovanje na dobrovoljnoj osnovi.

*„Imate raspored i prijavite se. I bude vam on-line. Samo što bude u radno vrijeme pa morate uzeti slobodno da odslušate. I to je to. Ovisi tko je što htio slušati.”*

Pojedini policijski službenici smatraju da ne posjeduju dovoljno znanja o sigurnosti na internetu za obavljanje svog posla te su izrazili potrebu za daljnjom edukacijom na tom području. Tijekom razgovora o provođenju dopunskog stručnog usavršavanja spomenuta je mogućnost da se edukacija o sigurnosti na internetu provodi kroz suradnju s vanjskim stručnjacima koji nisu dio MUP-a.

*„Ne znam. Baš nisam siguran da smo previše educirani što se tiče sigurnosti na internetu.”*

4. Koje digitalne kompetencije smatrate da biste trebali imati za obavljanje Vašeg posla?

Policijski su službenici općenito upoznati s osnovnim digitalnim vještinama kao što su korištenje programa za obradu teksta i numeričkih podataka, komunikacija elektroničkom poštom te pretraživanje interneta. Većina smatra da su ove vještine dovoljne za obavljanje njihovog posla jer službena komunikacija uglavnom teče putem službene elektroničke pošte koja je jedini digitalni kanal koji svi posjeduju. No postoje i policijski službenici koji smatraju da im nedostaje digitalnih vještina te se žale da nisu prošli potrebne edukacije vezane za digitalne tehnologije.

*„Tko ga je obučio? Tko je mene obučio za Word, Excel. Nitko mi u životu nije...”*

*„Osnovna obuka, to sam isto danas pričao s kolegicom. Znači, nitko se nije udostojao, u postaji, u upravi, bilo gdje. Ono osnovno jer uvijek ima onih kolega, kolegica koji ne znaju. Znači neke osnove rada na računalu. Otvaranje dokumenata u Wordu. Otvaranje dokumenata u Excelu. Kopiranje, prebacivanje, dakle neke osnove rada koje im trebaju. Znači to fali, jer ljudi bi morali sami sebi ili nešto uplaćivati ili najčešće kako kolega kaže: ‘de Roberte, ajde dođi, pokaži mi kako se to radi’. To fali. Fali ta edukacija ljudi. Ono osnovno, tko ne zna, ne mora za sve. Bit će jednom mjesečno neka edukacija sat, dva, tri. Koga zanima doći do ovdje. Znači educirati o osnovama rada na računalu.”*

*„Slanje mailova, kopiranje mailova, zaprimanje mailova. Znači te neke osnovne stvari. A oni nama pošalju prezentaciju u PDF-u za e-gop, naučite sami.”*

U mnogim zemljama, uključujući i Hrvatsku, policija se sve više koristi tehnologijom u svom radu. U to su uključeni različiti uređaji i aplikacije koje im olakšavaju obavljanje posla. No, tako se povećava i rizik od potencijalnih problema koji mogu nastati pri upotrebi tih uređaja i aplikacija te su potrebne razvijenije digitalne kompetencije da bi se problemi savladali te da bi se tako izbjegli i eventualni problemi.

*„Policajci ne bi imali, ne bi mogli ni smjeli imati mogućnost mijenjati nikakve postavke na računalu... Ne može instalirati nove programe bez administratora, ali može isključiti internet, pa onda se drugi dan ne mogu spojiti na internet. A odoh 50 kilometara od postaje. I onda mora doći ovdje da mu se uključi internet ...*

Nabava opreme također može rezultirati problemima ako se ne uzmu u obzir potrebe korisnika, a da se ne provjeri jesu li specifikacije opreme u skladu s njima

vim potrebama. To se može dogoditi kada se oslanjamo na procjene ili pretpostavke umjesto da se konzultiramo s krajnjim korisnicima da bismo saznali njihove zahtjeve i potrebe.

*„To je isto problem nabave te opreme. Možda zato što se ne konzultiraju dovoljno policijski službenici na terenu da se vide njihovi zahtjevi, recimo zadaće koje trebaju obavljati. Kriminalistička policija dobila je dosta prijenosnih računala, što je za svaku pohvalu, a ono što nije za pohvalu je taj tko je naručivao, nije se konzultirao pa vidio da bi možda na tom računalu trebalo biti više od 2 USB ulaza, pa možda da bude predviđeno da se može DVD medij koristiti. Video-nadzor koji dobijemo je na DVD mediju, sadržaji pretrage koji dobijemo su na DVD mediju. Imaš problem da to ne možeš koristiti.”*

*„Dobili smo i tablete, ali predviđeni su za policajce pozornike koji bi trebali nositi torbicu s tabletom i onaj printer... Znači, oni su isključivo bili namijenjeni za pješake, policijske službenike pozornike. Tablet i printer, onaj zebra koji ovako ima velik [...]i k'o pol kutije cipela.”*

5. Postoje li u Vašoj ustrojstvenoj jedinici pravila ponašanja na internetu? (ako ne postoje, jesu li potrebna, ako postoje, jesu li dostatna)

MUP nema posebno definirana pravila ponašanja na internetu, pa se policijski službenici pridržavaju općih pravila. Poštivanje tih pravila posebno je relevantno u manjim sredinama gdje je općepoznato tko je policajac, pa se i u virtualnom svijetu stav, ponašanje, komentar pojedinca gotovo bez iznimke odražavaju na policiju u cjelini.

*„U biti mi svi znamo kako bi se trebalo ponašati, gdje su nekakve granice. Mi u biti nitko nismo, barem u Požegi, tko god nas pozna svi znaju da smo policajci i teško je tu odrediti onu granicu gdje si ti fizička osoba i službena osoba. Onda je najbolje ništa jer se sve drukčije gleda ako mi nešto komentiramo ili objavljujemo.”*

Policijski službenici, međutim, ipak smatraju da im nedostaju interna pravila za ponašanje na internetu. Također im smeta što građani često iznose neistine o radu policije i što MUP ne reagira na takve navode. Kao jedino reagiranje MUP-a izdvajaju postupanje u slučajevima vrijeđanja i omalovažavanja policijskih službenika putem društvenih mreža, zbog čega se počinitelje procesuiraju za prekršaje iz „Zakona o prekršajima protiv javnog reda i mira”. Za odnose s javnošću ustrojena je linija rada u svim policijskim upravama, kao i u Ravnateljstvu i Ministarstvu, a sudionici istraživanja zaključuju da bi ta služba trebala reagirati na objavljene neistine, a ne da to čine pojedini policijski službenici.

*„Gledajte, u MUP-u radi 25 000 ljudi i kad bi mi dozvolili svakom da piše o svemu, to bi bio kaos. Radi davanja nekakvog ujednačenog stava, onda je bolje da to rade osobe koje su za to zadužene.”*

## 5. Zaključak

Kada je riječ o sposobnosti policijskih službenika da koriste informacijsko-komunikacijsku tehnologiju za razmjenu službenih informacija, može se zaključiti da su one vrlo različite od pojedinca do pojedinca, s obzirom na to da još ne postoje standardi digitalnih kompetencija za sva radna mjesta u hrvatskoj policiji.

Pokazalo se da su policijski službenici u Hrvatskoj vrlo samokritični u pogledu digitalne pismenosti i digitalnih kompetencija kojima raspolažu, ali da ograničena digitalna komunikacija policije u vrijeme pandemije bolesti COVID-19 nisu bila vezana samo za njihove digitalne kompetencije nego i za objektivne organizacijske okolnosti. Pri tome se na prvom mjestu ističe potreba za većim brojem djelatnika jer je najlošija opcija ponuditi građanima opciju digitalne komunikacije, a onda ne biti u stanju dosljedno tu opciju i provoditi u praksi. Prepreku intenzivnijoj uporabi digitalne komunikacije s građanima predstavlja do izvjesne mjere i nedostatak regulative i jasnih uputa za korištenje kanala digitalne komunikacije na pojedinim radnim mjestima u policiji. Iz toga proizlazi i nedostatak edukacije kojom bi policijski službenici bili osposobljeni ne samo u smislu digitalnih kompetencija nego i u smislu internih uputa za njihovo korištenje na konkretnim radnim mjestima.

U perspektivi je svakako potrebno istražiti aktualne potrebe policijskih službenika za digitalnim kompetencijama te definirati standarde digitalnih kompetencija policije u odnosu na rod policije i konkretne kategorije radnih mjesta.

## Literatura

1. Beesley, P. (2021). Competency-based Management Framework for Digital Competencies in Canadian Policing. *Canadian Police Knowledge Network*. <https://www.cpkn.ca/en/news/competency-based-management-framework-for-digital-competencies-in-canadian-policing/> (1. svibnja 2022.)
2. Bieber, R. (2022). Digital competences for the Police-A new ECDL. U *Central and Eastern European eDem and eGov Days*, 335, 447–456. <https://doi.org/10.24989/ocg.v335.37>
3. CEPOL (2021). *European Union Strategic Training Needs Assessment 2022–2025*. <https://www.cepola.europa.eu/sites/default/files/EU-STNA-2022-CEPOL.pdf> (11. svibnja 2022.)
4. Deneff, S., Kaptein, N., Bayrel, P. S. i Ramirez, L. (2012). *Best Practice in Police Social Media Adaptation*. *COMPOSITE – Comparative Police Studies in the EU*. <http://hdl.handle.net/1765/40562> (28. lipnja 2022.)
5. Jarolimek, S. (2019). Using Smartphones in Police Operations: The Necessity of Media Literacy in Police Forces in the Age of Transparency. *European Journal for Security Research*, 5 (4), 105–114. <https://doi.org/10.1007/s41125-019-00059-4>
6. Koprić, I. (2016). Reforma javne uprave u Hrvatskoj: ni bolni rezovi ni postupne promjene – nužna je nova upravna paradigma. *Političke analize*, 7 (26), 3–12.



7. Lobnikar, B., Christián, L., Balla, J., Kalmár, Á., Cajner Mraović, I., Borovec, K. i Sotlar, A. (2023). Police and Other Plural Policing Institutions in Central and Eastern Europe Facing COVID-19 Pandemic. U: Den Boer, M., Bervoets, E. i Hak, L. (ur.), *Plural Policing, Security and the COVID Crisis Comparative European Perspectives*, str. 107–138. Cham: Palgrave Macmillan. <https://doi.org/10.1007/978-3-031-19177-0>
8. Lobnikar, B., Sotlar, A. i Meško, G. (2013). Razvoj policijske dejavnosti v Srednji in Vzhodni Evropi. *Revija za kriminalistiko in kriminologijo*, 64 (1), 5–18.
9. Meško, G., Sotlar, A. i Lobnikar, B. (2014). Policing in Central and Eastern Europe: Past, Present, and Future Prospects. U: Reisig, M., D. i Kane, R. J. (ur.), *The Oxford Handbook of Police and Policing*, 606–622. Oxford: Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780199843886.013.009>
10. Montasari, R., Carpenter, V. i Masys, A. J. (2023). *Digital Transformation in Policing: The Promise, Perils and Solutions*, [e-book]. Switzerland: Springer. <https://link.springer.com/book/10.1007/978-3-031-09691-4>
11. Newburn, T. (2008). *Handbook of Policing*. Second edition. Culompton: WillanPublishing. <https://doi.org/10.4324/9780203118238>
12. O'Connor, C. D. i Zaidi, H. (2021). Communicating with purpose: Image work, social media, and policing. *The Police Journal*, 94 (3), 333–352. <https://doi.org/10.1177/0032258X20932957>
13. Vitez, D. i Balgač, I. (2016). Menadžment u javnoj upravi – modeli rada i izazovi upravljanja policijom. *Policija i sigurnost*. 25 (1), 1–13.
14. Walby, K. i Wilkinson, B. (2022). The visual politics of police Instagram communication in Canada. *New Media & Society*. <https://doi.org/10.1177/14614448211015805>
15. Warren, F., Gualco, F., Davidson, H. i Edginton, E. (2020). *Part 1 – International policing responses to COVID-19: During lockdown*. Edinburgh: The Scottish Government.



## **Foreign experiences of police digital competencies and perceptions of police officers in Croatia**

### **Abstract**

This paper aims to identify the digital competencies necessary for the uniformed police officers in Croatia during the COVID-19 pandemic when a part of police communication was shifted to cyberspace. The paper consists of two parts: it first provides an overview of relevant foreign examples attempting to regulate the digital competencies of uniformed police officers, followed by a presentation of qualitative research conducted in Croatia. Four focus groups, each with 10 research participants, were held between December 2022 and January 2023: three in the Osijek-Baranja Police Administration and one in the Požega-Slavonija Police Administration. The results of semi-structured interviews indicate that uniformed police officers require two categories of digital competencies: (1) digital literacy and internet usage, and (2) cyber hygiene and cyber security. Both categories are needed at the first two levels of digital literacy and internet usage. The primary limitation of this study is that it was conducted only in one part of Croatia, resulting in prospects for future research in two directions: repeating the same study with police officers from other police administrations in Croatia and exploring the digital communication channel needs of citizens in specific parts of Croatia. This would provide a comprehensive understanding of the need for digital police communication in Croatia and, consequently, the requirements for digital competencies for police officers.

**Keywords:** digital competencies, police, COVID-19 pandemic, Croatia