BEZBEDNOST ILI NAIVNOST

Priručnik digitalne diskrecije za akademske mislioce

Za svakoga ko misli, piše i čuva

IMPRESUM

Naslov:	***Bezbednost ili naivnost***
Podnaslov:	***Izbor je vaš***
Drugi podnaslov:	***Priručnik digitalne diskrecije za akademske mislioce***
Autor:	**Prof. dr Zoran Čekerevac**
Izdavač:	**Zoran Čekerevac,** samoizdavač
Mesto izdanja:	**Beograd**
Godina izdanja:	**2025**
ISBN:	**978-86-904190-1-2**
Format:	**Elektronsko izdanje (PDF/A), latinica**
Obim:	**1311 kB**
Dostupnost:	https://meste.org/biblioteka/mon.2V.0.pdf

Kontakt: **zce@meste.org**

DOI: **https://doi.org/10.12709/mon.2V.0**

MESTE

9 788690 419012

Biti akademski mislilac danas ne znači samo tragati za znanjem — već ga štititi od rasipanja koje nastaje kada digitalni tokovi preuzmu kontrolu bez autorove dozvole.

Svet u kojem istraživač komunicira, pretražuje, objavljuje i skladišti podatke više nije neutralan prostor, već mreža kroz koju prolaze algoritmi, enkripcije, metapodaci i pravila tuđih platformi.

U takvom okruženju, digitalna diskrecija postaje misaoni alat, etička odluka i tehnička praksa.

Ovaj priručnik donosi sistematski pregled strategija, alata i primera koji akademskom istraživaču omogućavaju da sačuva privatnost, sigurnost i intelektualnu autonomiju — bez odricanja od misaone slobode, saradnje i uvida.

Namenjen je svima koji misle, pišu i čuvaju (se).

Zoran Čekerevac
jesen 2025

Namerno ostavljeno prazno

SADRŽAJ

Namerno ostavljeno prazno

1. Uvod u digitalnu diskreciju

Na putu od ideje do realizacije, misao mora prvo da prođe diskretnu, nevidljivu fazu. Diskrecija nije skrivanje — ona je zaštitni sloj u periodu dok ideja traži svoj put, i svoj glas.

1.1. Akademska privatnost kao temelj intelektualne slobode

Savremeno akademsko stvaralaštvo ne odvija se više isključivo u biblioteci, laboratoriji ili zatvorenoj kancelariji. Procesi mišljenja, zapisivanja, saradnje i razmene sve su više podložni algoritamskom posmatranju, automatskom arhiviranju i često nevidljivim oblicima analize. Diskrecija u tom kontekstu nije bekstvo — ona je aktivno pravo na neometanu misaonu tišinu i kontrolu nad ritmom intelektualnog stvaralaštva.

Diskrecija je misaona sposobnost da se odlučuje kada, kako i zašto se ideja izlaže — uz poštovanje konteksta, autorstva i etike deljenja.

Osnovne pretnje akademskoj privatnosti uključuju:

- neautorizovano praćenje digitalnih navika (search history, cloud activity),
- gubitak konteksta u moru opcija koje nude algoritmi koji tumače nedovršene misli kao „gotove podatke”,
- potencijalna krađa ili prerana eksploatacija idejnih nacrta.

Istovremeno, **vrednosti privatnosti** ogledaju se u:

- očuvanju autentičnosti misli od spoljašnjih interpretacija,
- stvaranju prostora za eksperimentisanje bez pritiska javnosti,
- odgovornosti prema sopstvenom istraživačkom putu.

1.2 Zašto misao zaslužuje diskretan tretman

Nacrt, skica, fragment — sve to u akademskom kontekstu ne nosi samo informaciju, već i emocionalni i intelektualni zamah. Diskretan tretman takvog materijala obezbeđuje:

- **Zaštitu od neželjenog spoljnog uticaja** — kroz prepravku, plagiranje ili pritisak

- 🔄 **Kontrolu nad evolucijom misli** — jer svaka faza može da bude ranjiva bez adekvatne zaštite
- □ **Mogućnost kasnije refleksije** — kada znamo da su naše ideje sačuvane od spoljnog uticaja, lakše ih kritički sagledavamo

Digitalna diskrecija je, prema tome, više od tehničke mere — ona je misaona zaštita intelektualnog razvoja — prostor u kojem misao sazreva bez spoljašnjih pritisaka.

Tabela 1 Šta digitalna diskrecija pokriva?

Segment kreativnog procesa	Diskretna praksa	Cilj
Zamisao / ideja	lokalno čuvanje, pseudonimno zapisivanje, offline beležnice	izbegavanje idejnog "sniffinga" od strane algoritama
Radni nacrt	šifrovani fajlovi, privremeni profili, sandbox okruženja	sprečavanje krađe, kompromitovanja ili neželjenog uvida
Kolaboracija	End-to-End (E2E) komunikacija, restriktivni pristup dokumentima	kontrolisano deljenje i izbegavanje curenja
Verifikacija / izveštavanje	timestamp preko blockchaina, checksum za integritet	zaštita autentičnosti i vremenske oznake
Publikovanje	anonimizacija metapodataka, etički izbor platforme	očuvanje privatnosti i zaštita od manipulacije sadržajem

🕶️ 🔁 *E2E komunikacija ovde označava misaono celovit tok razmene — od ideje, preko diskretne faze oblikovanja, do javnog izražavanja, uz očuvanje konteksta, autorstva i etike.*

Ovakva zaštita nije samo tehnička — ona je multidisciplinarna. Delo ne samo da se štiti od krađe, već se štiti od **pogrešnog konteksta**, **izvrtanja značenja** ili **neautorizovanog preuređivanja**. U tom smislu, digitalna diskrecija je alat za **pravilan oblik i pravu poruku** jednog dela.

U svetu gde digitalni podaci postaju sve važniji, akademski mislioci — studenti, istraživači i profesori — suočavaju se sa izazovima očuvanja svoje intelektualne slobode. U ovoj eri algoritamskog nadzora i kvalitetnih podataka, svaka ideja, bez obzira na njen oblik, nosi sa sobom potencijale, ali i rizike.

Ovaj priručnik pruža konkretne alate i tehnike za jačanje kreatorove digitalne diskrecije, omogućavajući mu da oslobodi svoj kreativni proces bez straha od spoljnog uticaja. Važno je da kroz stranice ovog priručnika prepoznate i primenite strategije koje će vam pomoći da sačuvate svoju autonomiju i integritet tokom intelektualnog istraživanja.

💭 *Nadamo se da će ovaj priručnik postati ne samo alat, već i povod za zajedničko promišljanje i razmenu među onima koji razumeju vrednost tihe misli.*

Kroz narednih trinaest poglavlja, ovaj priručnik postepeno razvija ideju digitalne diskrecije od osnovnih pojmova do naprednih strategija.

Obrađuju se teme kao što su:

- Digitalni identitet i kako ga oblikovati u skladu sa sopstvenim ciljevima,
- Autentifikacija kao lična kapija u svet podataka,
- Šifrovanje koje stvara sigurnosni prostor unutar digitalnog okruženja,
- Upravljanje tragovima, kolaboracija i oblak, sve u svetlu diskretne kontrole,
- Blockchain i metapodaci kao tehnički alati sa filozofskim dilemama,
- Arhiviranje i budućnost, gde se diskrecija projektuje unapred.

💭 Ova poglavlja nisu redosled znanja — već misaoni tok digitalne odgovornosti.

Svako poglavlje nudi konkretne tehnike, alate i misaone okvire — da bi akademski mislilac zadržao kontrolu nad svojim idejama, kontekstima i putevima deljenja.

⚠ *Napomena: Autor nema sponzorisani ni poslovni odnos sa proizvođačima navedenih softverskih alata; njihova upotreba u tekstu ima isključivo ilustrativni i obrazovni karakter.*

Digitalna diskrecija nije ograničavanje znanja, već njegovo pažljivo oblikovanje. Ona omogućava da ideje budu deljene kada su spremne — u formi koja poštuje autorstvo, kontekst i slobodu stvaranja, ali i dostojanstvo misaonog procesa koji im prethodi.

▣ *Digitalna diskrecija počinje kao tehnička zaštita — kroz alate, protokole i kontrolu pristupa. Odatle se uzdiže u etički kompas koji usmerava kako delimo, čuvamo i razumevamo podatke. Na vrhu, ona postaje misaoni prostor u kojem misao sazreva slobodno — bez spoljašnjih pritisaka, algoritamskih deformacija i nepromišljenog izlaganja.*

👦💻 2. Upravljanje pripadajućim autentifikacijama

U digitalnom prostoru, pristup podacima — bilo da su to lični istraživački nacrti, komunikacije sa saradnicima ili arhivirani rezultati rada — počiva na **autentifikaciji**. Upravljanje pripadajućim autentifikacijama nije samo sigurnosno pitanje, već i **strategija kontrole pristupa** intelektualnim resursima.

Dok su korisnička imena i lozinke postali svakodnevna rutina, njihova složena organizacija, memorisanje i čuvanje sve više postaju **deo digitalne pismenosti** za akademskog mislioca.

Sledeći slojevi autentifikacije otkrivaju kako sigurnosni alati oblikuju ritam pristupa i misaonu diskreciju unutar digitalnog okruženja.

- dvofaktorska autentifikacija (2FA) i prijavljivanje bez lozinke
- rezervni recovery ključevi i procedure njihovog čuvanja

🧠 2.1 Vežbanje memorisanja "neuronskih šifara"

Lozinka nije samo niz karaktera — ona je misaona struktura. U akademskom kontekstu, lozinka može da postane produžetak mentalnog obrasca, refleks svakodnevnog razmišljanja, pa čak i interni simbol neke nedovršene ideje. Upravo zato, vežbanje memorisanja "neuronskih šifara" predstavlja ne samo tehničku veštinu, već i misaonu disciplinu.

Zahtevi za bezbednim lozinkama (dužina, složenost, jedinstvenost) često dolaze u konflikt sa sposobnošću pamćenja. Da bi se ta tenzija prevazišla, digitalni mislilac koristi strategije poput:

- povezivanja lozinki sa ličnim mentalnim mapama, metaforama ili stihovima (npr. "KaD>SaM>BiO==21!"),
- kreiranja logičkih šablona koji se menjaju u ritmu vremena (sezonski prefiksi, numerički kodirani fragmenti ideja),
- stvaranja misaonih sidara — fraza koje se mentalno vezuju za određeni fajl, aplikaciju ili tip pristupa.

🧩 Zapisana lozinka kojoj je pristupilo drugo lice ne mora biti kompromitovana, ukoliko je sačuvana u opisnom obliku koji zahteva lični misaoni ključ — na primer, kroz metaforu, unutrašnju referencu ili subjektivni kod. Takva forma predstavlja misaonu diskreciju: algoritam koji ne štiti podatke tehnički, već značenjem.

2.2. Menadžeri lozinki i njihova arhitektura

U vremenu kada se digitalni alati koriste za svakodnevne akademske zadatke, **upravljanje velikim brojem pristupnih lozinki** postaje misaoni izazov — ne samo logistički, već i etički. Menadžeri lozinki nude rešenje, ali i otvaraju pitanja: kome poveravamo ključeve sopstvenih misaonih prostora?

Razlikujemo tri glavna modela arhitekture:

- **Lokalni menadžeri** (npr. KeePass): lozinke se čuvaju na lokalnom uređaju, bez cloud sinhronizacije. Prednost je puna kontrola — ali uz rizik gubitka u slučaju kvara.
- **Cloud-based rešenja** (npr. Bitwarden, 1Password): omogućuju pristup sa više uređaja. Nude praktičnost, ali zahtevaju poverenje u enkripciju i u politiku privatnosti servisa.
- **Zero-knowledge sistemi**: kompanija tehnički ne može videti korisničke podatke, jer su šifrovani pre slanja. Ovi modeli postaju standard za diskretnu praksu.

***Preporuka*:** *birati menadžere lozinki koji dozvoljavaju lokalni backup, enkripciju na samom uređaju, i mogućnost kontrole recovery procedura bez spoljne autorizacije.*

Tabela 2 Upravljanje lozinkama

Tip upravitelja	Karakteristike	Diskretna vrednost
Lokalni upravitelj	Fajl sa lozinkama se čuva lokalno, bez sinhronizacije	Potpuna kontrola, ali zavisnost od uređaja
Cloud-based rešenje	Lozinke dostupne preko interneta, višestruki uređaji	Praktičnost, uz potrebu za poverenjem
Zero-knowledge sistem	Enkripcija pre slanja, servis nema pristup sadržaju	Visoka privatnost i kontrola nad podacima

***Preporuka**: birati rešenja sa podrškom za offline bekap, mogućnost lokalne kontrole nad recovery opcijama i transparentnu politiku enkripcije.*

Kada softver čuva misao, on mora znati da ne sme da je tumači. Upravitelj lozinki nije samo alat, već poverenik diskrecije.

2.3. Dvofaktorska autentifikacija (2FA) i prijavljivanje bez lozinke

U svetu gde digitalna prisutnost ostavlja trag, složeni oblici prijave postaju deo zaštite misaone autonomije. **Dvofaktorska autentifikacija (2FA)** donosi dodatni sloj potvrde identiteta — kombinaciju nečega što znamo (lozinka) i nečega što posedujemo (kod, uređaj, biometrijski podatak).

Postoji više pristupa:

- **SMS kodovi**: najšire primenjivani, ali i najranjiviji na presretanje.
- **Authenticator aplikacije** (npr. Authy, Google Authenticator): dinamički kodovi, često offline dostupni.
- **Biometrija**: otisak prsta, lice, glas — visok nivo praktičnosti, ali sa diskretnim dilema o delegiranju pristupa telu.
- **Sigurnosni ključ** (hardware token): fizički uređaji koji potvrđuju prisustvo korisnika — idealni za digitalne istraživačke arhive.

Iako značajno povećava sigurnost, dvofaktorska autentifikacija može biti nekomforna ili preopterećujuća — naročito kada je vezana za specifične uređaje ili kompleksne tokove prijave. Stoga nije neophodno primenjivati je univerzalno; treba je rezervisati za okruženja koja nose povećane rizike ili čuvaju podatke od posebnog značaja.

> ***Preporuka**: birati metode koje ne oslanjaju zaštitu na servise koji beleže biometrijske podatke, već one koje nude lokalnu verifikaciju i nezavisnost od trećih sistema.*

2.4. Prijavljivanje bez lozinke — nova paradigma

Ubrzanim razvojem autentifikacije, javljaju se metode koje u potpunosti eliminišu lozinke. Koristi se:

- **Magic Link** (link za pristup bez lozinke, putem mejla),
- **Biometrijsko automatsko prepoznavanje**,
- **Passkeys** – šifrovani ključevi vezani za uređaj, a ne za korisničko ime i lozinku.

Za akademske korisnike koji prelaze na platforme bez lozinke, diskrecija zahteva **praćenje gde se ključevi čuvaju, ko ih može obnavljati**, i da li je pristup vezan za pojedinca ili uređaj.

Napomena: *Pristup nije samo tehnički — on je filozofska odluka o granici između prisustva i identiteta. Prijava bez lozinke ne znači manju bezbednost, već veću potrebu za svesnom kontrolom nad mehanizmom ulaska.*

2.5. Rezervni recovery ključevi i procedure njihovog čuvanja

Autentifikacija ne sme biti jednokratna misao — ona zahteva mogućnost oporavka. Rezervni ključevi, backup kodovi i recovery metode često odlučuju da li će misaoni rad biti obnovljen ili izgubljen.

Diskretna praksa podrazumeva da rezervni ključevi:

- budu generisani nezavisno od primarne lozinke, po mogućstvu offline,
- budu čuvani na različitim lokacijama — fizički (USB sa enkripcijom, štampana kopija), digitalno (poseban cloud bez sinhronizacije sa glavnim nalogom),
- ne sadrže personalizovane oznake koje bi ih identifikovale kao "ključ" pri površnom pregledu.

***Primer dobre prakse**:* Backup kodovi se mogu sačuvati na sigurnosnoj fleš memoriji koja se koristi isključivo za recovery svrhe — bez drugih fajlova, bez oznaka, na odvojenoj fizičkoj lokaciji.

Tabela 3 Pregled rezervnih recovery metoda, strategija čuvanja i rizika pri nepažnji

Recovery metoda	Preporučeno čuvanje	Rizik pri nepažljivom tretiranju
Backup kodovi	Štampana kopija u neoznačenom fizičkoj formi	Moguća identifikacija ako se zadrže pored uređaja
Enkriptovani fajl	USB sa šifrom i bez drugih fajlova	Gubitak ili pristup ako USB nosi oznake kao "key"
Cloud backup (izolovani)	Poseban nalog bez povezivanja sa primarnim profilom	Pristup trećih lica ako je nalog jasan po nazivu
Fizički sigurnosni ključ	Sef sa fizički kontrolisanim pristupom	Kompromitacija ako se čuva u dostupnim, označenim prostorima
Šifrovani papirni zapis	Unutar neutralnog objekta (knjiga, mapa, kutija)	Dekodiranje značenja ako ima lične oznake ili naslov

Napomena: *Diskrecija u čuvanju ključeva podrazumeva ne samo tehničku zaštitu, već i semantičku neutralnost — da se značenje ne može lako odgonetnuti spoljašnjim posmatranjem.*

🧩 *Čuvanje rezervnog ključa ne znači samo zaštitu fajla, već i zaštitu značenja koje taj fajl nosi.*

▣ *Najveći rizik nije u fizičkom gubitku podatka, već u tome da neko — čak i nehotice — prepozna njegovu važnost zbog naziva, mesta gde je sačuvan ili načina na koji je označen. Diskretna zaštita podrazumeva ne samo enkripciju, već i pažljivo oblikovanje konteksta u kojem se ključ nalazi: bez upadljivih oznaka, bez povezivanja sa drugim misaonim slojevima, i sa jasnom namerom da ostane neprimetan čak i ako je fizički vidljiv.*

Autentifikacija nije samo proces prijave — ona je i ogledalo digitalnog identiteta. Svaka lozinka, kod, fizički token ili biometrijski signal jeste potvrda nečije prisutnosti u digitalnom prostoru, ali i način na koji se ta prisutnost oblikuje, evidentira i interpretira.

U tom smislu, praksa upravljanja autentifikacijama predstavlja prvi sloj konstrukcije identiteta: definiše ko smo u datom digitalnom kontekstu, kako se povezujemo sa svojim misaonim sadržajem i koje granice postavljamo prema spoljnim sistemima.

Identitet nije statičan; on je **dinamičan skup podataka, ponašanja i odluka** koje se menjaju u ritmu korisničke interakcije. Način na koji kreiramo pristup, čuvamo recovery ključeve ili biramo 2FA metode direktno utiče na oblik našeg digitalnog "**ja**" — onog koji drugi sistemi prepoznaju, interpretiraju i pamte.

U narednom poglavlju, istražujemo **kako se digitalni identitet formira, šta ga čini jedinstvenim, i na koje načine ga možemo kontrolisati** unutar akademskog i misaonog okruženja. Dok autentifikacija postavlja vrata, identitet definiše prostor iza njih.

3. Šifrovanje diska i fajlova

U digitalnom okruženju, gde granica između privatnog misaonog prostora i kolektivnog sistema često biva nejasna, šifrovanje funkcioniše kao štit. Ono nije samo alat za zaštitu podataka — već i čin kojim autor odlučuje kome, kada i pod kojim uslovima njegov sadržaj postaje vidljiv.

Bez obzira na to da li se radi o nedovršenim istraživačkim beleškama, ličnim dnevnicima razmišljanja, nacrtima akademskih članaka ili poverljivim radnim verzijama — **fajl je misaona jedinica**, a šifrovanje je njena zaštitna struktura.

U ovom poglavlju razmatramo:

- kako se enkripcija primenjuje na čitave diskove, ali i selektivno, na individualne foldere i dokumente,
- kako se oblikuju skrivene volumenske strukture, koje omogućavaju dodatni sloj privatnosti unutar istog medijuma,
- koje vrste šifrovanja se koriste za komunikaciju i razmenu sadržaja (PGP, GPG), i
- kako virtuelni diskovi omogućavaju modularnu zaštitu misaonih oblasti — aktiviranu po potrebi.

Analiza se ne zadržava samo na tehničkim parametrima, već se fokusira na **misaoni ritam enkripcije**: kada enkriptovati, šta enkriptovati, na koji način to oblikuje proces razmišljanja i koji se etički horizonti otvaraju korišćenjem ovih alata.

U poglavlju ćemo koristiti referenciranje po IEEE sistemu. Broj u uglastim zagradama označava redni broj izvora u bibliografiji knjige. Time potvrđujemo kredibilitet tehničkih detalja, ali i čuvamo autorsku preciznost.

3.1. BitLocker Drive Encryption: kako radi, prednosti i mane

U radu sa istraživačkim nacrtima, ličnim dokumentima i profesionalnim zapisima, pitanje zaštite podataka postaje više od tehničkog zahteva — ono postaje etička odluka. Microsoftov BitLocker, dostupan u profesionalnim i obrazovnim verzijama Windowsa, predstavlja **sistemsku opciju za šifrovanje čitavih diskova i particija** [1]. Njegova svrha je da spreči neovlašćen pristup podacima, čak i ako uređaj fizički dospe u ruke trećeg lica.

Kako funkcioniše BitLocker

BitLocker koristi *Advanced Encryption Standard (AES)* u XTS modu, sa opcijom 128-bitnog ili 256-bitnog ključa [2]. Oslanja se na hardverski modul — *Trusted Platform Module (TPM)* — koji bezbedno čuva kriptografske ključeve [1]. U najstandardnijoj konfiguraciji, korisniku je omogućeno da disk automatski bude otključan pri pokretanju sistema, dok naprednija podešavanja zahtevaju PIN ili USB ključ za dodatnu verifikaciju identiteta [1].

XTS mod (punim imenom *XEX-based Tweaked-Codebook mode with Ciphertext Stealing*), razvijen posebno za šifrovanje diskova, omogućava da svaki sektor bude šifrovan zasebno uz dodatni kontekstualni parametar — što obezbeđuje otpornost na obrasce ponavljanja i povećava bezbednost pri nasumičnom pristupu podacima.

Nakon uspešnog prijavljivanja, podaci su dostupni sistemu — **što znači da su dostupni i procesima koji pretražuju sadržaj**, poput indeksatora i Windows pretraživanja. Stoga, iako fajlovi ostaju šifrovani dok je disk zaključan, nakon otključavanja **njihovi nazivi mogu biti iščitani**, što može kompromitovati diskreciju ako sistem nije dodatno konfigurisan.

💡 *Tehnička enkripcija nije uvek misaona zaštita. Disk se može čuvati kriptografski, ali kada je disk otključan misaoni sadržaj* (nazivi fajlova, beleške, konceptualne strukture) može postati vidljiv sistemu i aplikacijama koje korisnik nije eksplicitno autorizovao

✅ *Prednosti*

- Transparentna enkripcija: nakon otključavanja, radna sesija ne menja tok [1]
- Enkripcija operativnog sistema i podataka iz istog interfejsa
- Integracija u Windows Pro, Enterprise i Education izdanjima [2]
- Hardversko osiguranje ključeva putem TPM-a koje otežava neovlašćeno kopiranje ključeva [1]
- Ugrađene recovery opcije: 48-cifreni recovery kod, čuvanje u Active Directory ili Microsoft nalogu [2]
- Automatske recovery opcije (offline kod), povezivanje sa Microsoft nalogom

⚠ *Ograničenja*

- Nazivi fajlova i drugi metapodaci i dalje su indeksirani od strane OS-a (vidljivo kroz Windows Search)
- Nakon otključavanja, podaci ostaju dekriptovani dok se BitLocker ne suspenduje ili isključi [1]
- Za punu funkcionalnost zahteva *Trusted Platform Module* (TPM 1.2+) ili USB startup ključ; *Home* izdanje podržava samo uređajsku enkripciju s ograničenjima [1]
- Korporativne implementacije zahtevaju postavljanje politika preko Group Policy ili Mobile Device Management rešenja [3]
- Home verzije nemaju punu BitLocker podršku: nude samo ograničenu uređajsku enkripciju

🛠 Preporuke dobre prakse

- Uvek kombinovati TPM protector sa PIN-om za multifaktorsku autentifikaciju [1]
- Onemogućiti indeksiranje sadržaja na enkriptovanim volumenima da bi se zaštitili nazivi fajlova
  `Properties > Advanced > Uncheck indexing`
- Recovery ključeve čuvati offline, na drugom uređaju, ili u bezbednom korporativnom skladištu (AD/Intune) [2]
- Povremeno proveravati status enkripcije komandletom Get-BitLockerVolume ili kroz Control Panel [4].

💭 *Komandlet (cmdlet) je specijalizovana PowerShell komanda za automatizaciju zadataka u Windows okruženju.*

🔍 Šta očekivati?

- Enkripcija se izvršava u pozadini bez prekida rada; trajanje zavisi od veličine diska i opcije “used space only” [2]
- Nakon uključivanja na sistemskom disku, neophodan je restart da bi zaštita bila aktivna [4]
- Ukoliko BitLocker detektuje promenu hardvera ili sistemske komponente, od korisnika se traži recovery ključ pre ponovnog podizanja sistema [1]

▣ *BitLocker ne štiti podatke od korisnika — već od gubitka uređaja. Za misaonu zaštitu, neophodno je razumeti gde prestaje njegova uloga, a gde počinje konfiguracija diskretne prakse.*

3.2 VeraCrypt: otvoreno-sistemska enkripcija

VeraCrypt je besplatan, otvorenog koda alat za enkripciju „on-the-fly" (OTFE), koji omogućava kreiranje virtuelnih zaštićenih diskova unutar fajla, ali i šifrovanje čitavih particija ili skladišnih uređaja pre-boot autentifikacijom. [5]

Korisnik može da izabere između standardnih i skrivenih volumena: prvi pruža uobičajenu zaštitu, dok drugi omogućava plauzibilnu deniabilnost – skrivena sloboda misaonog sadržaja koja ostaje nevidljiva čak i pod pritiskom za otkrivanje lozinke. [6]

VeraCrypt podržava niz jakih algoritama (AES, Twofish, Serpent, Camellia, Kuznyechik) i njihovih kombinacija, radi pojačane otpornosti na napade. Podrazumevane vrednosti za PBKDF2 iteracije kreću se od 200 000 do 500 000, što usporava brute-force napade, a režim XTS-AES obezbeđuje integritet i poverljivost blokova podataka. [5]

U odnosu na zatvorene, sistemske enkripcije, VeraCrypt gradi poverenje na transparentnosti. Kod je dostupan za pregled i reviziju, a razvoj se oslanja na nezavisne audite: Fraunhofer-ov izveštaj iz 2020. ukazuje da su osnovni kriptografski mehanizmi bez ozbiljnih ranjivosti, ali da postoje zamerke na zastarele implementacije RNG-a i RIPEMD-160 hash funkcije, te na prakse razvoja softvera koje ne prate industrijske standarde za kvalitet koda. [7]

✅ ***Prednosti:***

- potpuna autonomija korisnika: nema zavisnosti od TPM-a ni OS-a;
- skriveni volumeni pružaju plauzibilnu deniabilnost;
- otvoreni kod omogućava nezavisne provere i audite;
- više algoritamskih opcija i kaskadiranje dodatno komplikuju napade.

⚠ ***Ograničenja i rizici:***

- performanse mogu opasti na starijim mašinama zbog visokog broja iteracija;
- ako je volumen montiran, fajlovi su dekriptovani u memoriji i ranjivi na napade „evil maid" ili cold-boot;
- uprkos auditima, zastareli kod može skriti skriveni bug;
- zaboravljena lozinka znači trajni gubitak podataka – nema recovery opcije.

▣ Skriveni volumen: Misaona suverenost i zaštita privatnosti

VeraCrypt ne pruža samo sveobuhvatnu enkripciju; on omogućava korisniku da definiše *koji sloj sadržaja je stvarno prisutan*. Kroz funkciju skrivenog volumena, softver omogućava formiranje zaštićene oblasti podataka unutar standardnog volumena, čije postojanje nije tehnički dokazivo bez posebne lozinke. To znači da korisnik može pod pritiskom (pravnim, fizičkim, institucionalnim) da otkrije samo vidljivi volumen, dok se misaoni sadržaj zadržava neotkriven. Ova sposobnost je **pravno i filozofski relevantan mehanizam zaštite misli**. Skriveni volumen je oblik misaone suverenosti: mogućnost da se kaže „to je to“, i da to bude istina, iako nije cela istina. VeraCrypt time ne štiti samo fajl — štiti i odluku o *kom sadržaju se može govoriti*.

Ukoliko je aplikacija na USB-u, a kontejner na lokalnom disku, tragovi u računaru su svedeni na minimum.

💬 *Mogućnost skrivanja nije laž — ona je struktura u kojoj se ne mora reći baš sve da bi se dokazalo da je ono što je rečeno bilo istinito.*

📜 Primer 1 — Istraživački dnevnik

Zamislimo autora koji vodi lični misaoni dnevnik o etičkim temama, političkim strukturama i socijalnim dilemama. Istovremeno čuva beleške o akademskim radovima koji su javno dostupni. Skriveni volumen omogućava da se misaoni zapisi čuvaju od spoljne analize, dok se javni deo otkriva bez rizika po ličnu poziciju.

Ako dođe do provere uređaja, autor otkriva standardni volumen, dok misaoni deo ostaje nevidljiv — ne samo fizički, već i konceptualno.

📜 Primer 2 — Tehnička inovacija i zaštita patenta

Autorski rad na inovaciji koja može da postane patent često zahteva diskreciju u ranoj fazi. U skriveni volumen se smeštaju nacrti, vremenski tok razvoja i internetska korespondencija, dok se u standardni stavlja opšta literatura i nerelevantna dokumentacija.

U slučaju institucionalne inspekcije ili provere pri prelasku granice, standardni volumen se prikazuje kao „celina“, dok misaoni rad ostaje u nedodirljivoj unutrašnjosti — čuvajući pravnu prednost i suverenost nad intelektualnim materijalom.

3.3 PGP/GPG šifrovanje dokumenata i poruka

U akademskom misaonom radu, razmena ideja često ide paralelno sa razmenom dokumenata i poruka. U tim situacijama, sigurnost i integritet sadržaja postaju ključni. PGP (Pretty Good Privacy) i njegova otvorena varijanta GPG (GNU Privacy Guard) kombinuju simetrično i asimetrično šifrovanje kako bi omogućili pouzdanu zaštitu i verifikaciju podataka. [8]

Razlika između šifrovanja fajlova i poruka

- **Šifrovanje fajlova**: PGP/GPG koristi simetrični algoritam (npr. Advanced Encryption Standard, AES) da šifruje ceo fajl, i generiše privremeni „session key". Taj ključ se zatim asimetrično šifruje javnim ključem primaoca — čime se omogućava efikasno šifrovanje velikih podataka bez gubitka brzine. [8]
- **Šifrovanje poruka**: Poruka se prvo kompresuje (radi smanjenja veličine i kriptoanalitičke otpornosti), zatim simetrično šifruje, pa se zajedno sa sesijskim ključem šalje primaocu. Ključ je zaštićen javnim ključem, dok je sadržaj dostupan isključivo korisnicima sa odgovarajućim pravima za dešifrovanje [8].

U oba slučaja, čak i ako neko presretne podatke, bez pristupa privatnom ključu sesijski ključ ostaje nedostupan — i sadržaj ne može biti dešifrovan.

Javni i privatni ključ

- Korisnik generiše par ključeva: **javni** (slobodno deljen) i **privatni** (strogo čuvan). [9] Privatni ključ nikada ne sme biti deljen.
- Javni ključ se koristi za šifrovanje podataka, koje može dešifrovati samo onaj ko ima odgovarajući privatni ključ. Privatni ključ se koristi za kreiranje digitalnog potpisa, što potvrđuje identitet pošiljaoca.
- Upravljanje ključevima može se vršiti putem sistema nazvanog "web of trust", gde korisnici međusobno potpisuju ključeve kako bi potvrdili njihovu autentičnost, ili putem centralizovanih politika koje koriste sertifikate za verifikaciju.

🖋 Digitalni potpis

Digitalni potpis služi kao misaoni pečat — on potvrđuje ***ko*** je nešto rekao i ***šta*** je rečeno, odnosno potvrđuje **autentičnost** i **integritet** poruke ili dokumenta. Proces uključuje nekoliko koraka:

1. Izračunavanje sažetka poruke (hash) funkcijom poput SHA-256
2. Šifrovanje tog sažetka privatnim ključem pošiljaoca.
3. Primalac dešifruje potpis javnim ključem pošiljaoca i upoređuje dobijeni hash sa hash-om sopstvene kopije poruke. [10]

Ako se vrednosti poklope, primalac zna da je sadržaj neizmenjen i da dolazi od verifikovanog autora.

Digitalni potpis time postaje misaoni pečat: on ne samo da svedoči o tome ko je poslao poruku, već i o tome da njen sadržaj pre prijema nikada nije bio promenjen.

💬 *Digitalni potpis ne štiti samo sadržaj — on štiti i nameru iza tog sadržaja.*

📘💡 Šta je hash funkcija?

Hash funkcija je matematički algoritam koji od bilo kog sadržaja (poruke, dokumenta, rečenice) stvara jedinstveni digitalni otisak — niz karaktera poznat kao *hash vrednost*. Taj niz ne otkriva sadržaj, ali je strogo vezan za njega.

🔷 Osobine hash funkcije:

- **Jednosmernost**: iz hash-a nije moguće rekonstruisati originalni tekst
- **Osetljivost na promene**: i najmanja izmena u sadržaju drastično menja hash
- **Efikasnost**: proverava da li je sadržaj promenjen — bez potrebe da ga očitamo

U kontekstu digitalnog potpisa, hash omogućava da se potvrdi **integritet** poruke: da ništa nije promenjeno između slanja i prijema.

📊 **Primer: promena jedne reči menja ceo hash**

📝 Tekst poruke	🔐 SHA-256 hash vrednost (skraćeno)
Misaona sloboda je suština dijaloga	7A9F…BC9D
Misaona sloboda je temelj dijaloga	B12C…7AA0

🔶 Promenom samo jedne reči (“suština” → “temelj”) dobija se potpuno novi hash.

To je osnova za proveru neizmenjenosti — ako se hash razlikuje, sadržaj je menjan.

▣ PGP/GPG šifrovanje ne štiti samo fajlove, bitove na disku ili u mrežnom saobraćaju— ono štiti misaonu razmenu. Kroz kombinaciju jednokratnih ključeva, trajnih identiteta i digitalnih potpisa, akademski mislioci dobijaju kanal u kojem misao ostaje verodostojna, netaknuta i potvrđena. U tom sistemu, **privatni ključ je prostor unutrašnje suverenosti**, dok je javni ključ pozivnica za misaoni dijalog.

🔐 3.4 Virtuelni diskovi (VHD) sa enkripcijom po potrebi

Virtuelni diskovi (VHD/VHDX) su fajl-kontejneri koji operativnom sistemu predstavljaju “pravi” disk. Tako kreiranom VHD-u može se dodeliti slovo, može se formatirati i koristiti kao bilo koji drugi disk. Kada se doda enkripcija po potrebi, VHD postaje modularni, privremeni “sigurnosni džep” za osetljive podatke — montira se samo kad mislilac želi da radi, a potom se demontira i skladišti u zaštićenom okruženju. [11]

⚙️ Kako funkcionišu VHD-ovi s enkripcijom

Da bi virtuelni disk bio funkcionalan i zaštićen, potrebno je proći kroz niz koraka: od kreiranja kontejner-fajla, njegovog formatiranja i montiranja, pa sve do aktivacije enkripcije i bezbednog demontiranja. Sledeća procedura prikazuje standardni tok postavljanja VHD-a sa enkripcijom po potrebi.

1. **Kreiranje VHD-a**: kreira se pomoću Disk Management alata ili PowerShell komandom
   - Disk Management: Action ▶ Create VHD ▶ odabrati VHD ili VHDX, veličinu i lokaciju

- PowerShell: `New-VHD -Path C:\Secure\MyVault.vhdx -SizeBytes 10GB -Dynamic`

2. **Montiranje i formatiranje**:
   - Disk Management ▶ Attach VHD ▶ formatiranje novog diska (npr. NTFS)
   - Sada je moguće upisivanje fajlova na kontejner-disk kao na redovnom particionisanom medijumu.
3. **Enkripcija po potrebi**:
   - Pokrene se BitLocker na montiranom VHD-u (Turn on BitLocker) i odabere lozinka ili TPM+PIN
   - Nakon enkripcije, svaki put kada se VHD fajl montira, sistem automatski traži autentifikaciju.
   - Demontaža (Detach VHD) čuva VHD fajl u šifrovanom stanju, spreman za prenos ili bekap.

✅ *Prednosti*

Virtuelni diskovi pružaju fleksibilnost rada u slojevima, bez potrebe da se ceo sistem opterećuje osetljivim sadržajem. U okruženju koje zahteva povremenu misaonu izolaciju, ova metoda omogućava odvojeno i kontrolisano upravljanje podacima — uz poznate alate i minimalan tehnički prag.

- **Modularnost**: radi se samo na delu podataka, dok je ostatak offline i nevidljiv pretraživačima operativnog sistema
- **Prenosivost**: VHD fajl se može kopirati ili sinhronizovati (npr. na USB ili mrežu) bez rizika
- **Jednostavnost**: koristi isti BitLocker interfejs kao fizički diskovi
- **Kontrola pristupa**: montira se kad je potreban, a demontiranje (Detach VHD) uklanja virtuelni disk iz aktivnog fajl sistema, čime se brišu tragovi sesije rada, dok šifrovani fajl ostaje netaknut — spreman za prenos ili bekap.

⚠ *Virtuelni disk je bezbedan od gubitka podataka ako se pravilno demontira — ali aktivna sesija pri nestanku struje može ostaviti oštećenje u fajl sistemu, kao i kod fizičkih hard diskova kada ne postoji UPS zaštita.*

⚠ *Ograničenja*

VHD sa enkripcijom nije apsolutna zaštita. Kada je montiran, fajlovi su dostupni operativnom sistemu, čime se otvara prostor za neželjene pristupe ili nepažnju. Takođe, upotreba zavisi od verzije Windowsa, što može ograničiti dostupnost alata u obrazovnim ili kućnim okruženjima.

- Potrebno Windows Pro/Enterprise izdanje za BitLocker na VHD-u
- Montirani VHD jeste dešifrovan sistemu dok je aktivan — ranjiv na "evil maid" napade
- Lozinka ili ključ moraju biti pametno čuvani; zaboravljena lozinka je trajni gubitak
- Ne štiti tragove meta-podataka (ime fajla VHD kontejnera otkriva se sistemu)

🛠 Preporuke dobre prakse

Pravilnom primenom, VHD postaje efikasan alat za misaonu segmentaciju i diskreciju. Ključno je da se kontejner koristi promišljeno: ne sme ostati montiran duže nego što je potrebno, lozinka mora biti složena i bezbedno sačuvana, a svaki projekat treba da ima svoj odvojen bezbednosni okvir.

- Čuvajte VHD fajl na odvojenom, šifrovanom skladištu
- Montirajte VHD samo u sigurnom okruženju i odmah demontirajte po završetku rada
- Koristite jaku lozinku ili TPM+PIN kombinaciju za višeslojnu verifikaciju
- Skalabilno: za različite projekte pravite posebne VHD kontenjere — misaona segmentacija

▣ *Virtuelni diskovi sa enkripcijom po potrebi funkcionišu kao misaoni „pauza-tasteri" između slojeva rada. Sve dok je VHD demontiran, osetljivi zapisi ostaju izvan radnog prostora sistema. Montiranjem se pristupa samo pažljivo selektovanim segmentima — nalik otvaranju beležnice posvećene jednoj konkretnoj temi. Zbog toga ovde govorimo o modularnoj diskreciji.*

💬 *Kroz VHD se modeluje misaoni tok: montira se kada se fokusira na određenu oblast, a demontira kada je potrebno privremeno povući misao iz rada.*

Primer upotrebe

Zamislimo doktoranda koji razvija prototip algoritma za mašinsko učenje. U jednom VHD-u drži radne verzije modela, skripte i eksperimentalne podatke. U drugom, beleške i delikatne analize – nedavne hipoteze, napomene o neuspelim testovima.

Dok radi, montira oba kontejnera, ali svakog dana nakon sesije demontira "analitički" VHD i ostavlja montiran samo "kod" volumen. Tako sistem ne "pamti" misaone zapise i ne ostavlja trag u indeksima ili kesiranim fajlovima.

▣ *Različiti sistemi enkripcije ne predstavljaju samo tehnička sredstva za zaštitu podataka, već odražavaju različite pristupe misaonoj autonomiji, poverenju i granicama izlaganja. Dok BitLocker nudi jednostavnu zaštitu kroz infrastrukturu operativnog sistema, VeraCrypt omogućava višeslojnu kontrolu nad samom egzistencijom podataka. PGP/GPG pruža sigurnu komunikaciju uz potvrdu integriteta misli, a virtuelni diskovi (VHD) nude modularnu segmentaciju misaonog rada.*

U tom sklopu, enkripcija se ne svodi na tehnologiju, već postaje ***misaoni model pristupa sadržaju, odgovornosti i samodefinisanja granica vidljivosti****. Od izbora alata, do načina korišćenja, svaki korak reflektuje ne samo digitalnu sigurnost, već i misaonu strategiju korisnika.*

🧠 *Enkripcija nije štit od spoljnog sveta — ona je misaona odluka o tome šta sme da postoji, kako sme da se deli i kome je poverenje zaista namenjeno.*

👣 4 Upravljanje digitalnim tragovima

Svaki rad na mreži — bilo da se radi o akademskoj pretrazi, uređivanju dokumenata ili razmeni podataka — ostavlja tragove koje sistem beleži automatski. Ti tragovi nisu samo tehnički; oni predstavljaju misaone repove prethodnih odluka, radnih verzija i ličnih navika.

U kontekstu zaštite mišljenja, intelektualne suverenosti i profesionalne diskrecije, upravljanje digitalnim tragovima postaje praksa očuvanja misaonog integriteta. Bilo da se radi o uklanjanju nevidljivih podataka iz fajlova, korišćenju anonimnih okruženja ili kontroli mrežnih identifikatora — svaki korak doprinosi oblikovanju toga šta *ostaje dostupno,* a šta *misaono povučeno*.

Prva metoda u ovoj oblasti bavi se **metapodacima u dokumentima i slikama** — nevidljivim informacijama koje često izmiču pažnji, a mogu kompromitovati privatnost autora ili tok misaonog rada.

🖌 4.1 Čišćenje metapodataka iz dokumenata i slika

U digitalnom okruženju, svaki dokument nosi više od onoga što je vidljivo na ekranu. Word fajl, PDF ili fotografija ne sadrže samo tekst i slike — već i niz *nevidljivih podataka* poznatih kao **metapodaci**. To su informacije o autoru, vremenu kreiranja, uređaju, verzijama, komentarima, pa čak i GPS koordinatama kod slika.

U kontekstu akademskog rada, metapodaci mogu nenamerno otkriti identitet autora, tok izmena, prethodne verzije rada ili tehničke detalje koji nisu namenjeni deljenju. Zato je **čišćenje metapodataka** prvi korak u upravljanju digitalnim tragovima — ne samo radi privatnosti, već i radi profesionalne diskrecije.

🧹 Čišćenje metapodataka iz Word dokumenata

Važno je napomenuti da je pre svakog uklanjanja metapodataka iz dokumenta, poželjno sačuvati kopiju dokumenta pod drugim nazivom, npr. *naziv_dokumenta.rezerva.docx*, ili *god_mes_dat_naziv_origin.docx*. Navođenje datuma je uvek korisno kod vođenja evidencija o međuverzijama. Datumi koje operativni sistem dodeljuje fajlovima nisu uvek pouzdani — čak i najmanja izmena u fajlu može promeniti vremensku oznaku i zamagliti stvarni redosled verzija.

Word sadrži ugrađeni **Document Inspector** za lociranje i uklanjanje skrivenih podataka. Postupak je sledeći:

1. Otvoriti dokument u Microsoft Word-u.
2. Kliknuti na **File** → **Info** → **Check for Issues** → **Inspect Document**.
3. U dijalogu ***Document Inspector*** označiti sve kategorije (author, comments, revisions, custom properties) i kliknuti na **Inspect**.
4. Nakon pregleda, kliknuti **Remove All** pored svake pronađene stavke.
5. Na kraju selektovati **Close** i sačuvati dokument pod novim imenom ili prepisati preko postojećeg fajla.

Ovaj proces eliminiše većinu skrivenih podataka direktno u Word fajlu, ali se preporučuje provera ponovnim inspekcijama nakon svake izmene ili deljenja dokumenta. [12]

Kao jednostavna alternativa lokalnom Document Inspector-u, mogu se koristiti besplatni online servisi. Najčešće opcije su:

- **GroupDocs Metadata Remover** (GroupDocs.Metadata) [13]
- **PDFCandle Word Metadata Remover** [14]

Opšti koraci su isti:

1. Posetiti stranicu izabranog alata.
2. Prevući ili odabrati Word (.docx) fajl za upload.
3. Nakon pregleda dokumenta, označiti koji se metapodaci brišu (autor, komentar, verzija, kompanija, datum) i pokrenuti uklanjanje.
4. Kliknuti **Save** ili **Download** da bi se dobio očišćeni fajl.

Saveti za bezbednost:

- Koristiti servis sa HTTPS enkripcijom i jasnom politikom uklanjanja fajlova nakon obrade.
- Ne ostavljati dokumente duže nego što je potrebno – preuzeti očišćenu kopiju i odmah izbrisati upload.
- Za osetljive radove, razmotriti self-hosted rešenje ili lokalni alat kako bi se izbeglo čuvanje fajla na eksternim serverima.

🧹 Čišćenje metapodataka iz Excel, PowerPoint i Visio dokumenata

I Excel radne sveske (.xlsx) i PowerPoint prezentacije (.pptx) mogu sadržati niz metapodataka koji nisu vidljivi tokom rada, ali se beleže automatski. Uključuju imena autora, komentare, beleške, datume izmene, eksternu povezanost i skriveni sadržaj — sve što može da otkrije misaoni tok, tehničku pozadinu ili identitet autora.

Microsoft Office koristi **Document Inspector** za čišćenje u oba slučaja, uz malu razliku u nazivima inspekcije. [15]

Za Excel (.xlsx ili .xls):

- Otvoriti radnu svesku
- Kliknuti **File** → **Info** → **Check for Issues** → **Inspect Workbook**
- Označiti sve kategorije (skriveni redovi/kolone, komentari, lične informacije, veze)
- Kliknuti **Inspect**, zatim **Remove All** za svaku pronađenu stavku
- Sačuvati fajl pod novim imenom

Napomena: ako je aktiviran **Shared Workbook**, mora se prvo deaktivirati da bi inspekcija bila moguća.

Za PowerPoint (.pptx ili ppt):

- Otvoriti prezentaciju
- Kliknuti **File** → **Info** → **Check for Issues** → **Inspect Presentation**
- Označiti sve dostupne kategorije (beleške, komentari, lične informacije, skriveni objekti)
- Pokrenuti inspekciju i kliknuti **Remove All** po potrebi
- Sačuvati očišćeni fajl

Napomena: prezentacije često sadrže **template informacije**, imena recenzenata i beleške ispod slajdova — koje nisu direktno vidljive publici, ali mogu da otkriju misaonu pozadinu rada.

Za Visio (.vsdx ili .vsd):

1. Otvoriti dokument u programu Visio.
2. Kliknuti na **File** → **Info** → **Check for Issues**
3. Izabrati ***Remove Personal Information***.

4. U **Personal Information** tabu, selektovati ***Remove these items from the document***.
5. Za uklanjanje potencijalno osetljivih podataka iz spoljnih izvora, treba selektovati ***Remove data from external sources stored in the document***. Selektovanje ovog polja ne uklanja podatke koji su povezani sa dokumentom. Uklanja samo izvor podataka sa crteža. Ako se neki podaci iz izvora podataka nalaze na crtežu, potrebno ih je ručno ukloniti.
6. Sačuvati dokument pod novim imenom ili prepisati postojeći fajl.

Korišćenjem istih koraka kao u Word-u, korisnici postižu doslednu sanitaciju Office fajlova i sprečavaju neželjeno izlaganje misaonih tragova.

🧹 Čišćenje metapodataka iz PDF fajlova

PDF dokumenti mogu sadržati nazive autora, ključne reči, datum kreiranja, komentare i čak skriveni tekst. Dva metodološka pristupa:

- **Adobe Acrobat Pro DC:**
  1. Otvoriti PDF i odabrati **Tools → Redact → Remove Hidden Information**.
  2. Acrobat skenira metapodatke, komentare i skrivene slojeve; kliknuti Remove i sačuvati izmenjeni fajl.
- **Osnovno brisanje kroz Properties**:
  1. U Acrobat Reader-u (ili sličnom alatu) izabrati **File → Properties → Description**.
  2. Izbrisati polja (**Title, Author, Subject, Keywords**) i sačuvati novi PDF.

Za potpunu sanitaciju pogodna je opcija **Sanitize Document** jer uklanja i skriveni tekst i elemente koje standardni Properties panel ne vidi.

🧩 Prilikom kreiranja PDF fajla iz Word dokumenta (npr. putem funkcije **Save as → PDF**), većina metapodataka iz Word-a automatski se prenosi u PDF, uključujući **naslov**, **autora**, **komentare**, pa i nevidljive revizije. Ako polje **Title** u Word dokumentu nije eksplicitno popunjeno, naziv PDF fajla u prozoru prikaza može biti generisan iz generičkih podataka — što dovodi do **neodgovarajućeg ili zbunjujućeg naslova jezička** na ekranu.

💬 *Preporučuje se da se metapodaci u Word dokumentu proveravaju i očiste pre konverzije u PDF, ili da se naknadno izvrši inspekcija u Acrobat-u radi potpune kontrole*

🖌️ Čišćenje metapodataka iz slika

Digitalne fotografije često sadrže EXIF metapodatke (model kamere, datum, GPS koordinate). U Windows 10/11 sistemu može se koristiti sledeći postupak:

1. U File Explorer-u pronaći slikovni fajl (.jpg, .png i sl.).
2. Desni klik → **Properties** → kartica **Details**.
3. Kliknuti na **Remove Properties and Personal Information**.
4. Izabrati "*Create a copy with all possible properties removed*" ili "*Remove the following properties*" i označiti željene stavke.
5. Kliknuti **OK** da se generiše kopija ili prepiše original.

Ovaj metod efikasno briše GPS i ostale senzorne podatke, ali za napredniju sanitaciju (batch proces i skriveni kanalni podaci) treba koristiti specijalizovane alate.

🎗️ Uklanjanje metapodataka putem Windows File Explorer-a

Windows omogućava osnovno uklanjanje metapodataka iz različitih fajlova (npr. slika, dokumenata, PDF-ova) direktno iz File Explorer-a, koristeći opciju u svojstvima fajla.

Koraci:

1. **Pronaći fajl** u File Explorer-u (npr. `.jpg`, `.docx`, `.pdf`)
2. **Desni klik** na fajl → izabrati **Properties**
3. Otvoriti karticu **Details**
4. Na dnu prozora kliknuti na **Remove Properties and Personal Information**
5. U dijalogu koji se otvori, izabrati jednu od dve opcije:
   - *Create a copy with all possible properties removed* – pravi kopiju fajla bez metapodataka
   - *Remove the following properties from this file* – omogućava ručno biranje koje metapodatke ukloniti
6. Označiti željene stavke (npr. Author, Date taken, Camera model, Tags)
7. Kliknuti OK da se izmene primene

🧩 - *Ovaj metod ne uklanja sve vrste metapodataka (npr. skriveni slojevi u PDF-u, revizije u Word-u)*
- *Za naprednije čišćenje preporučuju se specijalizovani alati ili inspektori unutar Office aplikacija*

▣ *Kroz lokalnu kontrolu podataka — uklanjanjem metapodataka direktno iz File Explorer-a — korisnik preuzima osnovnu kontrolu nad vidljivošću fajla, bez dodatnog softverskog posredovanja. Taj gest predstavlja početni korak ka misaonoj diskreciji: definisanju sadržaja bez otisaka njegovog porekla.*

▣ *Nevidljivi slojevi dokumenta se ogledaju u metapodacima koji, iako neprimetni tokom čitanja, svedoče o misaonim tokovima i tehničkim tragovima autora. Čišćenjem tih metapodataka briše se arhiva kognitivnih zaokreta, ostavljajući isključivo ono što je namenjeno javnom uvidu.*

💬 *Brisanjem nevidljivih slojeva, definiše se granica između misaonog puta i javne staze.*

🧪 4.2 Rad u "sandbox" okruženjima i privremenim profilima

Privremeno izolovana okruženja i korisnički profili stvaraju radni prostor koji omogućava eksperimentisanje bez ostavljanja trajnih tragova na glavnom sistemu. Ovi alati funkcionišu kao **misaono neutralne zone**: unutar njih se izvršavaju zadaci, testiraju ideje i sprovodi rad, a po završetku sesije sve promene se automatski brišu.

U akademskom kontekstu, sandbox rad i privremeni profili omogućavaju korisniku da **odvoji misaoni eksperiment od trajnog toka rada**, čime se čuva integritet glavnog digitalnog okruženja.

🗃 Windows Sandbox

Windows Sandbox je ugrađena funkcija u Windows 10 Pro/Enterprise i Windows 11 koja omogućava brzo pokretanje čiste, kratkotrajne instance operativnog sistema. Sve promene u sandboxu se poništavaju zatvaranjem prozora.

Koraci pri upotrebi:

1. Omogućiti Sandbox u **Control Panel → Programs → Turn Windows features on or off** → označiti ***Windows Sandbox*** → ***Restart***.
2. Pokrenuti Windows Sandbox iz Start menija.
3. U sandbox prozor kopirati ili instalirati aplikacije i izvršiti zadatak.
4. Zatvoriti sandbox – svi fajlovi, instalacije i promenjeni registry automatski se brišu.

Privremeni korisnički profili

Kreiranje izolovanog, privremenog profila unutar istog sistema omogućava rad bez uticaja na glavni korisnički folder.

Na Windows-u:

1. Kreirati novi lokalni nalog bez administratorskih privilegija (*Settings → Accounts → Family & other users → Add someone else to this PC*)
2. Prijaviti se na taj nalog i izvršiti radne zadatke
3. Odjaviti se i vratiti na glavni nalog
4. (Opcionalno) Izbrisati profil kroz *System Properties → Advanced → User Profiles → Settings → Delete* ili ručno iz **C:\Users**

Na Linux-u:

```
sudo useradd tmpuser
su - tmpuser
# rad u privremenom okruženju
exit
sudo userdel -r tmpuser
```

✅ ***Prednosti***

- Efikasno poništavanje svega urađenog nakon zatvaranja okruženja
- Izolacija od glavnog sistema smanjuje rizik od neželjenih tragova
- Brza dostupnost ugrađenih alata bez potrebe za dodatnim softverom
- Vraćanje u čisto radno stanje bez manuelne sanitacije

⚠ *Ograničenja*

- Windows Sandbox zahteva Pro/Enterprise ili Education verziju sistema
- Ne može se pokrenuti više sandbox instanci istovremeno u standardnoj konfiguraciji
- Privremeni profili mogu ostaviti tragove u Event Log-u ako se ne uklone sistemski
- Sandbox ne prenosi softverske licence i ne koristi konfiguracije host sistema

🛠 Preporuke dobre prakse

- Kopirati samo neophodne fajlove u izolovani prostor
- Nakon rada obavezno ukloniti privremene naloge i izvršiti sanitaciju keša
- Ne oslanjati se na sandbox kao jedinu zaštitu, već ga kombinovati sa drugim metodama diskrecije
- Razmotriti napredne alate poput *Sandboxie* ili *VMware Player* za kompleksne scenarije

▣ *Sandbox okruženja i privremeni profili predstavljaju digitalne laboratorijume u kojima se ideje mogu testirati bez trajnosti ni obaveze. Po završetku, prostor se vraća u prvobitno stanje, a tragovi misaonih koraka nestaju kao da se nisu ni dogodili.*

4.3 Anonimni pretraživači, VPN, Tor i Tails

U digitalnom prostoru, svaki klik, pretraga ili otvaranje stranice može ostaviti trag koji se povezuje sa identitetom korisnika. Da bi se misaoni rad zaštitio od neželjenog profilisanja, praćenja ili izlaganja, koriste se alati koji **zamagljuju digitalni otisak** — od anonimnih pretraživača do specijalizovanih operativnih sistema.

U ovoj sekciji razmatramo četiri ključna pristupa:

- **Anonimni pretraživači** koji ne beleže istoriju pretrage niti identitet korisnika
- **VPN servisi** koji šifruju saobraćaj i maskiraju IP adresu
- **Tor mreža** koja preusmerava podatke kroz više slojeva kako bi se sakrila lokacija i aktivnost

- **Tails operativni sistem** koji omogućava rad bez ostavljanja tragova na računaru

Ovi alati ne predstavljaju samo tehničku zaštitu — već i misaonu odluku o tome kako, kada i pod kojim uslovima se sopstveni rad prikazuje spoljašnjem svetu.

Anonimni pretraživači

U pitanju su pregledači koji ne čuvaju istoriju pretraživanja, ne vezuju pretraživanje za korisnički nalog i blokiraju većinu pratioca (trackera).

Korišćenjem DuckDuckGo, Brave ili sličnih pregledača korisnik dobija:

- pretraživanje bez vezivanja za svoje korisničko ime ili nalog
- automatsko blokiranje oglasa i tracker skripti
- zaštitu od osnovnog fingerprintinga

Na šta treba obratiti pažnju:

- IP adresa ostaje vidljiva sajtu, osim ako se dodatno ne koriste VPN ili Tor
- mobilne i desktop verzije se razlikuju po obimu zaštite
- napredne funkcije (kao što su ekstenzije) mogu biti ograničene

VPN servisi

VPN (Virtual Private Network) uspostavlja šifrovani tunel između korisnikovog uređaja i VPN servera, sakrivajući korisnikov stvarni IP i štiteći saobraćaj od lokalnih nadzora.

Osnovne koristi:

- enkriptovanje celine korisnikovog internet saobraćaja
- maskiranje IP adrese i lokacije
- zaobilaženje geo-ograničenja za pristup akademskim bazama i publikacijama

Ključne tačke za proveru:

- politika čuvanja logova („no-logs“ ili „delimični logovi“)
- zemlja registracije i nadležnost provajdera
- brzina konekcije i broj dostupnih servera
- podrška za više uređaja i kill-switch opcija
- cena pretplate i mogućnost besplatnih/probnih verzija

Tor mreža

Tor (The Onion Router) je decentralizovana mreža za anonimnu komunikaciju putem interneta. Funkcioniše kao **peer mreža sa dobrovoljnim učešćem**, u kojoj svaki korisnik može pokrenuti sopstveni čvor (relay) i time doprineti ukupnoj anonimnosti sistema. Tor koristi tehniku **onion routing** — višeslojno šifrovanje koje čini da nijedan deo mreže ne zna ko šalje podatak i kuda on ide.

Otuda naziv "onion routing" — jer se poruka obavija slojevima šifrovanja, kao luk.

Princip rada

Kada korisnik otvori stranicu putem Tor Browser-a, njegov zahtev se:

1. **Šifruje u tri sloja**, kao slojevi crnog luka
2. **Putuje kroz tri nasumično odabrana čvora**:
   - Ulazni čvor zna identitet korisnika, ali ne zna krajnju destinaciju
   - Srednji čvor zna samo prethodni i sledeći čvor
   - Izlazni čvor zna samo krajnju destinaciju, ali ne zna identitet korisnika
3. **Svaki čvor dešifruje svoj sloj** i prosleđuje zahtev dalje — pri čemu **nijedan čvor ne poseduje celokupnu informaciju o korisniku i njegovim aktivnostima**

Zahvaljujući ovoj arhitekturi, Tor uspešno štiti korisnika od mrežnog nadzora, cenzure i profilisanja.

Primer iz prakse

Korisnik se nalazi u javnoj biblioteci i koristi Tor da bi pristupio sajtu o ljudskim pravima. Njegova sesija se šifruje i prolazi kroz tri čvora: ulazni u Nemačkoj, srednji u Kanadi i izlazni u Švedskoj. Sajt vidi samo izlaznu IP adresu iz Švedske — bez ikakve veze sa korisnikom u biblioteci. Ni lokalna mreža biblioteke ne zna koji sadržaj je prikazan — samo da je korišćen Tor.

Tor kao peer mreža

Tor se oslanja na **hiljade dobrovoljnih čvorova** koje pokreću pojedinci i organizacije širom sveta. Vrste čvorova:

- **Ulazni (guard)** – prvi čvor u sesiji
- **Srednji (middle)** – prenosi šifrovanu poruku

- **Izlazni (exit)** – poslednji čvor, koji komunicira sa spoljnim sajtom

Pokretanjem relaya, korisnici direktno doprinose stabilnosti i anonimnosti mreže.

📱 *Dostupnost Tor aplikacije*

Tor Browser se može besplatno preuzeti i koristiti na više platformi:

- **Za računar**: Windows, macOS i Linux — dostupno na zvaničnoj stranici Tor projekta (https://www.torproject.org/download/)
- **Za mobilni telefon**: zvanična aplikacija **Tor Browser for Android** dostupna je na Google Play prodavnici
- **Za iOS korisnike**: trenutno ne postoji zvanična Tor aplikacija, ali se preporučuju alternativni pregledači sa podrškom za Tor mrežu (npr. Onion Browser)

Ova dostupnost omogućava korisniku da koristi Tor i na ličnim i na javnim uređajima, uz zadržavanje anonimnosti i zaštite saobraćaja.

🛠 Kako pokrenuti Tor čvor (Tor relay)

Preporuka za početnike je da pokrenu **srednji ili ulazni čvor** — bez izlaznog saobraćaja koji nosi dodatne pravne rizike. Osnovni postupak na Linux sistemima (npr. Ubuntu):

```
# Instalacija Tor paketa
sudo apt update
sudo apt install tor

# Uređivanje konfiguracije
sudo nano /etc/tor/torrc
```

Dodati sledeće linije:

```
Nickname MojTorCvor
ContactInfo mojemail@primer.com
ORPort 443
ExitRelay 0
ExitPolicy reject *:*
RelayBandwidthRate 5 MB
RelayBandwidthBurst 10 MB
```

Zatim pokrenuti servis:

```
sudo systemctl restart tor
sudo systemctl enable tor
```

Nakon nekoliko sati, čvor će postati vidljiv u Tor mreži i može se pratiti putem zvaničnih stranica **Tor projekta**.

Prednosti

- Višeslojna anonimnost u komunikaciji
- Pristup cenzurisanom sadržaju i .onion servisima
- Otporna mreža zasnovana na zajednici
- Tor Browser ne čuva istoriju pretrage niti kolačiće

Ograničenja

- Sporije učitavanje stranica zbog više slojeva šifrovanja
- Neki sajtovi blokiraju Tor izlazne čvorove
- Internet provajderi mogu primetiti da se koristi Tor (iako ne znaju šta se pretražuje)
- Dodaci i ekstenzije mogu kompromitovati anonimnost — treba ih izbegavati u Tor Browser-u

Tor projekt ohrabruje korisnike da učestvuju kao releji, ali ističe važnost razumevanja svojih pravnih obaveza i mrežne politike.

Tails operativni sistem

Tails (The Amnesic Incognito Live System) je Linux distribucija koja se pokreće sa USB-a ili DVD-a, ostavljajući minimalne tragove na računaru. Na USB uređaju se nalaze i **operativni sistem** i **folderi sa podacima**, uključujući opcioni *persistent storage* — šifrovani prostor za čuvanje fajlova, lozinki i podešavanja. Po završetku rada, korisnik jednostavno uklanja USB iz računara, čime se prekida sesija i ne ostavljaju se tragovi na lokalnom disku — što je naročito korisno kada se radi na **tuđem ili javnom računaru**.

*Pošto se sistem učitava direktno sa USB-a, performanse mogu biti **sporije** u poređenju sa radom na lokalnom disku — naročito pri radu sa većim fajlovima, otvaranju aplikacija ili pokretanju više procesa. Preporučuje se korišćenje **USB 3.0** ili **3.1 uređaja** radi boljeg odziva i stabilnosti.*

Ključne karakteristike:

- sve veze idu kroz Tor mrežu (forced routing)
- sistem radi isključivo u RAM-u i briše sve po isključivanju

- dolazi s unapred konfigurisanim alatima za enkripciju fajlova, elektronske pošte i čišćenje metapodataka

Na šta treba obratiti pažnju:

- boot kod računara mora podržavati pokretanje sa eksternih medija (USB/DVD)
- čuvanje podataka u persistent storage-u nosi rizik ako neko fizički dođe do USB-a
- performanse mogu biti ograničene na starijim ili slabijim mašinama
- korisnička greška (npr. neproveren integritet Tails imidža) može smanjiti nivo zaštite

🧩 *Priručnik, pa time i sledeća sekcija zasnivaju se na aktuelnim i javno dostupnim informacijama o alatima i servisima koji se koriste u svrhu zaštite privatnosti u digitalnom prostoru. Opisi funkcionalnosti, prednosti i ograničenja napravljeni su u formi praktičnog pregleda i ne predstavljaju zvanične preporuke za pojedinačne proizvode.*

Pre svake upotrebe navedenih alata, preporučuje se da se korisnik upozna sa zvaničnom dokumentacijom i politikom korišćenja svakog servisa, kako bi se donela odluka u skladu sa sopstvenim potrebama i stepenom digitalne izloženosti.

Priručnik služi kao orijentacija u izboru metoda zaštite, a ne kao tehnička specifikacija. Detaljnu konfiguraciju, licenciranje ili sistemske zahteve treba proveriti direktno kod proizvođača, jer se vremenom menjaju.

4.4 Smanjenje vidljivosti akademskih aktivnosti na mreži

Radi očuvanja profesionalne diskrecije i zaštite digitalnog identiteta, preporučuje se primena tehničkih mera koje smanjuju mogućnost neželjenog nadzora i automatizovanog profilisanja u akademskom kontekstu. Poseban fokus stavlja se na upravljanje kolačićima, blokiranje elemenata za praćenje (trackera) i zaštitu od digitalnog otiska (browser fingerprinting).

Upravljanje kolačićima

Kolačići predstavljaju male podatke koje veb-sajtovi smeštaju na korisnički uređaj radi čuvanja podešavanja i praćenja sesije. Iako doprinose funkcionalnosti veb-stranica, mogu se koristiti za prikupljanje podataka o obrascima pretraživanja.

- Preporučuje se onemogućavanje kolačića trećih strana u podešavanjima pregledača:
  - **Chrome**: *Settings → Privacy and security → Cookies and other site data → Block third-party cookies*.
  - **Firefox**: *Preferences → Privacy & Security → Enhanced Tracking Protection → Custom* → označiti *"Cookies"*.
- Savetuje se aktiviranje režima potvrde za svaki zahtev (tzv. „ask first" opcija).
- Periodično brisanje kolačića i keš memorije može se obaviti putem funkcije *Clear browsing data* ili kombinacijom tastera **CTRL+SHIFT+DEL**.
- Korišćenje ekstenzija kao što je **Cookie AutoDelete** omogućava automatsko uklanjanje neaktivnih kolačića.
- Privremeni režimi rada (*incognito/private mode*) sprečavaju zadržavanje kolačića nakon zatvaranja sesije.

Digitalni identitet se gradi i kompromituje u neprimetnim mikrosekvencama podataka. Kolačići trećih strana predstavljaju kanal za neregulisano profilisanje.

Onemogućavanje kolačića trećih strana ne utiče na osnovnu funkcionalnost većine akademskih platformi, ali značajno umanjuje površinu za pasivno prikupljanje podataka.

Blokiranje elemenata za praćenje (trackera)

Trackeri služe za identifikaciju korisničkog ponašanja i kreiranje profilnih obrazaca zasnovanih na višestrukim izvorima. Njihovo blokiranje umanjuje količinu podataka dostupnih trećim stranama.

- Preporučuje se instaliranje ekstenzija za blokiranje trackera, kao što su:
  - **uBlock Origin** – širok spektar filtera za oglašavanje i trackere.

  - **Privacy Badger** – automatski prepoznaje i blokira skripte za praćenje.
  - **NoScript** – selektivno omogućavanje kriptovanog sadržaja.
- Pregledači sa ugrađenim mehanizmima zaštite:
  - **Brave** – blokira reklame i trackere "out-of-the-box."
  - **Firefox** (Enhanced Tracking Protection) – zaštićeni režim, dodatno smanjuju rizik od praćenja.
- Blokiranje automatskog učitavanja skripti trećih strana putem alata kao što su **uMatrix** ili **NoScript**..
- Redovno ažuriranje listi blokiranja (npr. EasyPrivacy, Fanboy's Tracking List) preporučuje se radi praćenja novih oblika prikupljanja podataka.

 Ekstenzije koje automatski prepoznaju i blokiraju skripte (Privacy Badger, uBlock Origin) ne zahtevaju dodatna podešavanja i kompatibilne su sa većinom preglednika bez primetnog usporenja.

 Ponašanje korisnika nije samo algoritamska meta — ono postaje model koji oblikuje digitalne reakcije, reklamne tokove i akademsku vidljivost. Upravljanje trackerima je preventivna strategija, ne luksuz.

Zaštita od digitalnog otiska (browser fingerprinting)

Fingerprinting obuhvata metodu identifikacije korisnika kroz analizu jedinstvenih karakteristika sistema, kao što su operativni sistem, jezička podešavanja, instalirani fontovi i rezolucija ekrana.

- Preporučuje se korišćenje pregledača otpornih na fingerprinting:
  - **Tor Browser** – nasumično menja niz parametara pri svakoj sesiji.
  - **Firefox** – podešen u režim Strict ili Custom u okviru Enhanced Tracking Protection, automatski blokira poznate metode fingerprintinga.
- Dodatne preporuke uključuju onemogućavanje komponenti:
  - ***WebGL:*** `webgl.disabled = true`
  - ***WebRTC:*** `media.peerconnection.enabled = false`
- Standardizacija veličine prikaza prozora i rezolucije ekrana smanjuje mogućnost identifikacije.
- Korisna je primena ekstenzija za ublažavanje fingerprintinga:

- ***CanvasBlocker*** *– detektuje i sprečava pokušaje identifikacije putem canvas metode.*
- ***Trace*** *– integrisana zaštita* od praćenja i fingerprintinga.

- Preporučuje se povremena provera izloženosti putem servisa kao što su *amiunique.org* ili *fingerprintjs.com*.

❗ *Internet pregledači otporni na fingerprinting ne garantuju anonimnost, ali složenost njihovih identifikacionih parametara otežava pasivnu analizu korisničkog profila u okviru mrežnog saobraćaja.*

🧠 Digitalni otisak ne zavisi od aktivnog ponašanja, već od sistemskih karakteristika — zato je kontrola parametara prikaza i komponenti jednako važna kao i ponašajna disciplina.

Primena navedenih tehničkih i proceduralnih mera doprinosi očuvanju autonomije istraživača u digitalnom okruženju, smanjenju neautorizovanog nadzora i očuvanju akademske diskrecije. Detalji o zaštiti na mobilnim uređajima i u oblaku obrađeni su u sledećoj sekciji.

📱☁ 4.5 Zaštita na mobilnim uređajima i u oblaku

Digitalna autonomija istraživača obuhvata ne samo radnu stanicu, već i mobilne uređaje i infrastrukturu u oblaku. S obzirom na njihovu sveprisutnost, preporučuje se primena specifičnih tehničkih i organizacionih mera radi smanjenja rizika od neautorizovanog pristupa i pasivnog nadzora.

📱 Zaštita na mobilnim uređajima

Mobilni telefoni i tableti predstavljaju značajan faktor izloženosti, naročito zbog kontinuirane povezanosti, fizičke dostupnosti i niskog nivoa hardverske izolacije.

- **Šifrovanje uređaja**: Aktivacija sistemskog šifrovanja (npr. File-Based Encryption na Androidu ili Data Protection na iOS-u) omogućava zaštitu podataka u mirovanju.
- **Kontrola dozvola aplikacija**: Preporučuje se periodična revizija dozvola aplikacija, posebno pristupa lokaciji, mikrofonu, kameri i kontaktima.
- **Deaktiviranje unifikovanih identifikatora**:
  - Android: Resetovanje "Advertising ID";
  - iOS: Ograničavanje praćenja putem "Limit Ad Tracking".

- **Privatni DNS servisi**: Korišćenje DNS-over-HTTPS (DoH) ili DNS-over-TLS (DoT) onemogućava pasivno praćenje DNS zahteva.
- **Firewall aplikacije**: Alati kao što su NetGuard (Android) omogućavaju granularnu kontrolu mrežnog saobraćaja aplikacija bez root pristupa.
- **Automatsko zaključavanje ekrana i biometrijska autentifikacija**: Podešavanje kratkog perioda neaktivnosti pre zaključavanja, uz dvofaktorsku autentifikaciju kada je to moguće, može da bude zamorno, ali je i korisno

📦 *Mobilni uređaj nije samo alat — on je proširena radna površina čiji su podaci često nevidljivo izloženi.*

☁ Zaštita u okruženju oblaka

Korišćenje cloud servisa za skladištenje, sinhronizaciju i saradnju zahteva dodatne mere opreza, kako bi se očuvala akademska diskrecija i kontrolisao tok osetljivih informacija.

- **End-to-End šifrovanje datoteka**: Preporučuje se lokalno šifrovanje pre otpremanja na oblak (npr. VeraCrypt, Cryptomator).
- **Odabir provajdera sa evropskom jurisdikcijom**: Servisi koji podležu GDPR regulativi (npr. Tresorit, pCloud EU) imaju strože politike privatnosti.
- **Dvofaktorska autentifikacija (2FA)**: Aktivacija dodatne zaštite za pristup nalogu, posebno kod servisa kao što su Google Drive, OneDrive, Dropbox.
- **Revizija deljenja**: Periodični pregled javno dostupnih ili deljenih fajlova i mapa.
- **Ograničenje sinhronizacije**: Onemogućavanje automatske sinhronizacije na uređajima koji nisu u aktivnoj upotrebi.
- **Logovanje pristupa**: Praćenje vremena, lokacije i uređaja sa kojih je pristup realizovan.

🧠 *Oblak ne briše odgovornost — samo je decentralizuje. Očuvanje kontrole nad datotekama podrazumeva aktivnu i promišljenu konfiguraciju.*

Info-box: Preporučeni alati i servisi za zaštitu privatnosti

Kategorija	Preporučeni alati / servisi	Namena
Mobilni uređaji	NetGuard (Android)	Lokalni firewall bez root pristupa
	DNS-over-HTTPS (npr. NextDNS, Cloudflare)	Privatno rešavanje DNS zahteva
	Privacy Dashboard (Android 12+)	Vizuelna kontrola dozvola aplikacija
	App Tracking Transparency (iOS)	Onemogućavanje praćenja od strane aplikacija
	Tor Browser (Android/iOS)	Pregledanje uz zaštitu od praćenja
Oblak	Cryptomator, VeraCrypt	Lokalno šifrovanje fajlova pre otpremanja
	Tresorit, pCloud (EU serveri)	Cloud provajderi pod GDPR jurisdikcijom
	2FA (Google, Microsoft, Dropbox, itd.)	Dodatni sloj bezbednosti pri pristupu
	Rclone (CLI alat za sinhronizaciju sa enkripcijom)	Sigurna sinhronizacija prema više servisa
	Boxcryptor (do 2023, sada nasleđen od Cryptomator-a)	Transparentno šifrovanje cloud foldera (nasleđeni alati)

Prilikom odabira cloud servisa, posebno za akademsku upotrebu, preporučuje se provera jurisdikcije i uslova čuvanja podataka, uz izbegavanje rešenja koja automatski indeksiraju sadržaj radi komercijalne analize.

🤝 5. Sigurna kolaboracija i komunikacija

U akademskom okruženju, poverenje ne počiva samo na stručnosti sagovornika, već i na infrastrukturnim mehanizmima koji omogućavaju sigurnu razmenu ideja, nacrta i dokumentacije. Savremeni komunikacijski kanali — od emaila do kolaborativnih platformi — sve češće podležu automatizovanim filterima i protokolima nadzora, čime se komunikacija pretvara u tehnički izazov, a ne samo sadržajni zadatak.

U slučaju kada filter iz nekog razloga zaključi da je sadržaj priloga (npr. PDF dokument) povezan sa domenom koji se nalazi na crnoj listi, on blokira prenos imejla uprkos tome što sam pošiljalac nije u vezi sa tim domenom. Iz ovog primera, jasno se uočava kako filteri funkcionišu bez konteksta i nužne preciznosti. Takvi primeri ne samo da otežavaju svakodnevnu komunikaciju i oduzimaju kreativno vreme mislioca, već stvaraju potrebu za sistemskom izgradnjom poverljivih kanala razmene koji podrazumevaju otpornost na pasivne forme nadzora.

U ovom poglavlju analiziramo:

- alate za šifrovanu elektronsku komunikaciju,
- platforme za sigurni čet i zajednički rad,
- pravila digitalnog bontona u akademskoj kolaboraciji.

🔐 5.1 Alati za šifrovanu elektronsku komunikaciju

U prenosu osetljivih akademskih podataka, end-to-end enkripcija postaje osnovni preduslov poverenja. Kroz kombinaciju specijalizovanih email servisa i PGP ekstenzija, istraživačima se omogućava da svaka razmena poruka ostane privatna i autentična — čak i kada prolazi kroz nepoznate servere, automatizovane filtere i heurističke mehanizme nadzora.

🧠 *U moru nadzora, nešifrovana poruka je razotkrivena misao – enkripcija je ključ koji odvaja dijalog od špijuna.*

📨 Enkriptovani email servisi

Odabrani servisi nude unapred konfigurisan sistem zaštite, uz podršku za enkripciju tela poruke i priloga, kao i transparentnost u pogledu čuvanja metapodataka.

- **ProtonMail**
  - Automatska end-to-end enkripcija unutar domena.
  - Mogućnost slanja šifrovanih poruka korisnicima van sistema.
  - Švajcarska jurisdikcija sa fokusom na nezavisnost podataka.
- **Tutanota**
  - Šifruje kompletno sanduče — uključujući kalendar i kontakte.
  - Ne zahteva unos ličnih podataka pri registraciji.
  - Nemačka jurisdikcija, usklađenost sa GDPR regulativom.
- **Mailfence**
  - PGP-kompatibilno okruženje sa mogućnošću upravljanja ključevima.
  - Kombinacija privatnosti i funkcionalnosti (kalendari, dokumenti).
  - Belgijska jurisdikcija.

End-to-end enkripcija obezbeđuje diskreciju sadržaja, ali ne štiti uvek zaglavlja, vremenske žigove ili IP podatke. Za dodatnu zaštitu može se kombinovati sa VPN servisima ili pristupom putem Tor mreže.

PGP plug-inovi za postojeće email klijente

Za korisnike koji već poseduju email naloge (npr. Gmail, Outlook), mogu se koristiti PGP dodatci radi uvođenja šifrovanih poruka bez promene celog sistema komunikacije.

- **Mailvelope** (Chrome / Firefox)
  - Web-ekstenzija koja dodaje OpenPGP podršku u interfejs poznatih servisa.
  - Korisnici samostalno upravljaju ključevima.
  - Dobar izbor za brzu integraciju bez instalacije dodatnog softvera.
- **Mozilla Thunderbird**
  - Desktop email klijent sa ugrađenom podrškom za OpenPGP.
  - Omogućava digitalno potpisivanje i šifrovanje direktno iz programa.
  - Pogodan za korisnike koji žele potpunu kontrolu.
- **FlowCrypt**
  - Gmail ekstenzija koja automatski enkapsulira šifrovane poruke u MIME format.

- Omogućava laku razmenu ključeva i kompatibilnost sa drugim PGP korisnicima.

📦 *Šifrovan email nije samo tehnička prepreka pred radoznalim očima — to je izjava o autonomiji akademskog dijaloga i poštovanju intelektualne slobode.*

📊 *Pregled alata za šifrovanu elektronsku komunikaciju*

Alat / Servis	Tip rešenja	Enkripcija	Jurisdikcija / privatnost	Tehnička složenost	Preporučeno za početnike
ProtonMail	Email servis	End-to-end (unutar domena) + eksterni pristup	Švajcarska	Niska	✅ Da
Tutanota	Email servis	End-to-end + metapodaci	Nemačka / GDPR	Niska	✅ Da
Mailfence	Email servis	PGP kompatibilnost	Belgija / GDPR	Srednja	⚠️ Uz osnovno predznanje
Mailvelope	Web-ekstenzija	OpenPGP (lokalni ključevi)	Zavisi od klijenta	Srednja	✅ Da (uz vodič)
Thunderbird	Email klijent	OpenPGP	Nezavisno	Srednja	⚠️ Za tehnički upućenije
FlowCrypt	Gmail ekstenzija	MIME + OpenPGP	SAD (servis zavisi)	Srednja	✅ Da (uz Gmail nalog)

📘 U slučaju nepostojanja prethodnog iskustva sa enkriptovanim porukama, preporučuje se kombinacija specijalizovanog email servisa (npr. ProtonMail) sa jednostavnom PGP ekstenzijom (npr. Mailvelope). Takva kombinacija omogućava bezbednu komunikaciju bez naprednog tehničkog znanja.

📬 *Scenario primene: akademska razmena sa PGP podrškom*

Istraživač koristi Tutanota za slanje šifrovane poruke, dok saradnik koristi Gmail sa Mailvelope dodatkom. Poruka se automatski enkriptuje, dok primaocu stiže uz instrukcije za dešifrovanje ili direktnu PGP obradu putem ekstenzije. Standardizovani format OpenPGP omogućava

međusobnu razmenu bez obzira na servis, pod uslovom da su javni ključevi prethodno razmenjeni.

💬 5.2 Bezbedni chat i platforme za zajednički rad

U akademskoj saradnji u realnom vremenu, povjerenje se gradi na sigurno zaštićenim kanalima, a ne na pretpostavkama o dobronamjernosti svih posrednika. Bez end-to-end enkripcije, svaka razmena poruka i dokumenata ostaje izložena pasivnom nadzoru, čuvanju metapodataka[1] i mogućim zloupotrebama.

🧠 *Pri nešifrovanom razgovoru svaka reč je potencijalno vidljiva svima.*

🔒 Secure chat

Niški nivoi interakcije — jedan-na-jedan poruke i grupni četovi — mogu biti zaštićeni specijalizovanim aplikacijama:

- **Signal**
  - Open Whisper Systems protokol: end-to-end enkripcija za privatne i grupne razgovore.
  - Minimalni metapodaci na serveru i opcija samouništavanja poruka.
  - Otvoreni kod, redovna revizija sigurnosti.
- **Matrix / Element**
  - Decentralizovana arhitektura: korisnik bira svoj homeserver[2] ili koristi javni.
  - Olm/Megolm protokoli za end-to-end (E2E) enkripciju u direktnim i grupnim sobama.
  - Kompatibilnost sa raznim klijentima, podrška za bridge ka drugim mrežama.

🧩 *E2E enkripcija skriva samo sadržaj poruka. Metapodaci poput liste učesnika, vremenskih oznaka i broja poruka i dalje mogu ostati vidljivi serverima. Za minimalizaciju vidljivosti, preporučuje se korišćenje prilagođenih homeservera ili VPN-a.*

[1] - metapodaci → podaci o podacima — npr. vreme slanja, IP adrese, broj poruka
[2] - homeserver → server koji korisnik koristi za povezivanje na mrežu, lokalni ili javni.

Kolaborativni alati sa end-to-end šifrovanjem

Pored četova, akademski rad zahteva zajedničko uređivanje dokumenata, rokove i deljenje fajlova:

- **CryptPad**
  - Web-bazirani editor za dokumente, tabele, prezentacije i beleške.
  - Sveobuhvatna E2E enkripcija sadržaja, serveri ne vide čist tekst.
  - Open source i besplatan za osnovnu upotrebu.
- **Nextcloud Talk + E2E plugin**
  - Integracija četova, video-poziva i deljenja fajlova unutar Nextcloud okruženja.
  - Opcionalna E2E enkripcija za razgovore i fajlove.
  - Mogućnost hostovanja na sopstvenom serveru.
- **Keybase**
  - Timovi, kanali i fajl deljenje sa OpenPGP-baziranom enkripcijom.
  - Automatska razmena javnih ključeva putem Keybase profila.
  - Integracija sa Git repozitorijumima za transparentno verzionisanje.

Pregled bezbednih chat i kolaborativnih alata

Alat	Tip rešenja	Enkripcija	Jurisdikcija / privatnost	Tehnička složenost	Preporučeno za početnike
Signal	Mobilni/desktop chat klijent	Open Whisper Systems (E2E)	Global (serveri u SAD)	Niska	✅ Da
Element (Matrix)	Decentralizovan chat klijent	Olm/Megolm (E2E)	Zavisi od homeservera	Srednja	⚠ Uz osnovno znanje
CryptPad	Web kolaboracija	Sveobuhvatna E2E enkripcija	Francuska	Srednja	⚠ Uz vodič
Nextcloud Talk	Video + chat + fajlovi	Opcionalna E2E enkripcija	Zavisi od hostovanja	Srednja / složena	⚠ Za tehnički upućenije
Keybase	Chat + fajl deljenje	OpenPGP-bazirana E2E	SAD / varijabilno	Srednja	⚠ Uz privatan ključ

📘 Za početak bezbedne real-time saradnje, može se kombinovati Signal za bogatu mobilnu i desktop komunikaciju sa CryptPad-om za zajedničko uređivanje dokumenata. Ovo osigurava brzu, a opet poverljivu razmenu, bez složenih server-postavki.

Scenario primene: interdisciplinarni tim

Tim istraživača deli kratke poruke i fajlove preko Element klijenta na sopstvenom homeserveru, dok paralelno vodi beleške i verzije izveštaja u CryptPad-u. Svi članovi koriste iste public-key servere za automatsku razmenu ključeva, a periodično resetovanje sobe smanjuje rizik od prekomernog gomilanja metapodataka.

Najbolje prakse

- *Uvek ažurirati aplikacije na najnovije verzije radi bezbednosnih zakrpa.*
- *Razmeniti i verificirati javne ključeve van samih platformi (licem u lice ili video-poziv).*
- *Koristiti „privatne sobe“ ili kanale sa ograničenim trajanjem.*
- *Kombinovati E2E alate sa VPN-om kako bi se sakrili metapodaci o lokaciji i IP adresi.*

5.3 Pravila digitalnog bontona pri deljenju informacija

U digitalnoj kolaboraciji, čak i najsuptilniji komentar može oblikovati autorovu ideju – zato je poštovanje i jasnoća u komunikaciji jednako važna kao i sama sadržina dokumenta.

Deljenje nacrta i komentara u elektronskom obliku nije samo tehnički čin, već oblik akademske interakcije. Dokumenti u radnoj fazi predstavljaju misao u razvoju, a komentari mogu biti podsticajni, ali i zbunjujući ako nisu jasno strukturirani. Zbog toga je važno uspostaviti zajednička pravila razmene: kako se imenuju fajlovi, kako se obeležavaju promene, i na koji način se komentari unose i uklanjaju. Ove prakse doprinose ne samo tehničkoj urednosti, već i kulturi međusobnog uvažavanja saradnika.

📘 *Pravila digitalnog bontona osiguravaju da razmena nacrta protekne uz jasnoću verzija, konstruktivan ton u komentarima i kontrolu pristupa. Ovakav pristup štedi vreme i štiti intelektualni rad svih učesnika.*

Evidentiranje izmena u zajedničkim dokumentima

- Naslovi fajlova treba da odražavaju status i datum:
  - Draft_v0.1_2025-07-16.pdf
  - Review_v0.2_2025-07-20.docx
- Svaka promena kreira novu verziju da bi se izbegao konflikt i zadržala hronologija izmene.
- Preporučuje se upotreba standardnih formata (PDF za konačne verzije; DOCX/ODT sa uključenim komentarima za radnu razmenu).

Struktura i ton komentara

- Koristiti alate za praćenje izmena (Track Changes, Google Suggestion mode) kako bi se razlikovalo šta je autor predložio, a šta dodao recenzent.
- Formulisati komentare konstruktivno i kratko:
  - • „Predlaže se pojašnjenje hipoteze na strani 3.“
  - „Ovaj pasus je vrlo jasan; moguće je proširiti primer.“
- Izbegavati višebojne markere i „sticky notes“ koje mogu zbuniti prilikom daljeg uređivanja.
- Nakon završene razmene, ukloniti zastarele komentare pre konačnog slanja.

Kontrola pristupa i povlačenje verzija

- Ograničiti pristup dokumentu samo na direktno uključene saradnike.
- Koristiti verzionisane foldere ili alate (npr. GitLab/GitHub za LaTeX projekte) kako bi se obezbedila transparentnost i rollback mogućnost.
- Za osetljive materijale primeniti dodatnu zaštitu — lozinke ili enkripciju fajlova prije deljenja.

Praktični saveti

- Držati se minimalizma u komentarima: bolje je par jasnih zapažanja nego mnoštvo neorganizovanih beleški.
- Verifikovati da svi saradnici vide najnoviju verziju pre završne diskusije.
- Navesti rok za povratne informacije i na kraju procesa poslati kratki rezime dobijenih komentara.

☁🗄 6. Privatnost u oblaku i referentni menadžeri

U digitalnoj svakodnevici akademskih mislilaca, granica između dostupnosti i izloženosti postaje sve tanja. Fajlovi se čuvaju, razmenjuju, verzionišu i komentarišu kroz mreže čije tehničke mogućnosti prevazilaze lokalni hardver. Ali paralelno sa tom fleksibilnošću dolaze i nova pitanja: da li su podaci zaista privatni, da li se reference dele bez pristanka, i da li se može sinhronizovati bez odavanja?

Ovo poglavlje razmatra alate i prakse koji omogućavaju sigurnu upotrebu cloud servisa i referentnih menadžera – bez kompromisa po pitanju diskrecije.

☁🔐 6.1 Izbor cloud provajdera koji poštuje privatnost

U savremenom akademskom radu, sinhronizacija podataka preko oblaka mora biti pouzdana, etička i tehnički otporna. Cloud provajder ne čuva samo fajlove — već poverenje, rukopis u nastajanju, ideje koje još nemaju oblik i dokumente koji ne bi smeli da završe na neproverenim serverima.

🧠 *Privatnost u oblaku je nevidljiva spona poverenja – birati one koji čuvaju misli, a ne prodaju ih.*

Iako se mogućnosti deljenja, verzionisanja i timske sinhronizacije često reklamiraju kao praktične, najvažniji aspekt je zapravo **pravna i tehnička struktura servisa**. Nisu svi oblaci bezbedni, i nisu svi podatci pod istim zakonskim režimom — što može direktno uticati na integritet akademske razmene. Zbog toga se preporučuje pažljiva selekcija cloud provajdera, prema sledećim kriterijumima.

🔐 Kriterijumi za selekciju

- **Zero-knowledge enkripcija**: server ne zna sadržaj fajla — ni u kom trenutku. Korisnik jedini poseduje ključ.
- **End-to-end enkripcija tokom prenosa i u mirovanju**: podaci nisu vidljivi ni dok putuju ni dok „stoje“.
- **Transparentna politika privatnosti**: jasno definisano ko ima pristup, koliko dugo se zadržavaju podaci i koje se informacije čuvaju.

- **Lokacija servera**: preporučuju se provajderi u jurisdikcijama koje poštuju akademsku i komunikacijsku slobodu (npr. Švajcarska, Island, EU).
- **Usklađenost sa GDPR-om i dodatnim regulatornim okvirom**: obavezno za evropske saradnike.
- **Dvofaktorska autentifikacija (2FA)**: štiti nalog čak i pri kompromitaciji lozinke.
- **Bezbednosni auditi**: nezavisne revizije i javno objavljeni rezultati pomažu transparentnosti.
- **Minimalno logovanje aktivnosti**: izbegava se čuvanje IP adresa, vremena prijave, tipa fajla itd.
- **Open-source kod**: omogućava inspekciju sigurnosnih protokola od strane nezavisnih stručnjaka.
- **Precizna kontrola pristupa**: detaljno podešavanje ko, kada i kako može da vidi ili menja sadržaj.

💡 *Provajderi sa visokim stepenom privatnosti*

Provajder	Enkripcija	Jurisdikcija	Otvoren kod	Posebna prednost
Tresorit	End-to-end	Švajcarska / EU	Ne	GDPR-compliant, poslovna upotreba
Sync.com	Zero-knowledge	Kanada	Ne	Lični i timski planovi uz E2E zaštitu
pCloud	E2E opcionalna	Švajcarska	Delimično	Offline pristup i sopstveni klijent
Internxt	E2E + open-source	Španija / EU	✅ Da	Fokus na etičku zaštitu podataka
Proton Drive	E2E + integracija	Švajcarska	✅ Da	Usklađen sa Proton ekosistemom (Mail, Calendar)

📘 Prilikom izbora cloud provajdera, ne odlučuje se samo o tome gde će fajl „stajati“, već o tome kako će ideja biti čuvana, ko može da je prati, u kojoj meri je deo ekosistema slobode ili sistema kontrole. Pravi provajder štiti sadržaj čak i od sebe samog — jer zna da znanje pripada onome ko ga je stvorio.

6.2 Enkripcija pre slanja na udaljene servere

Zaštita podataka počinje pre samog prenosa na cloud: lokalno šifrovanje stavlja ključeve pod kontrolu istraživača i eliminiše rizik od neovlašćenog pristupa na strani provajdera.

Nezaštićeni fajl u oblaku je kao otvoreno pismo u izlogu – enkripcija pre slanja je nevidljiva koverta.

Pri lokalnom šifrovanju pre sinhronizacije preporučuju se sledeće prakse:

- **Folder-level kontejneri** – virtualni šifrovani folder koji se montira kao disk. Fajlovi unutar njega vidljivi su tek nakon otključavanja.
  Koristiti alate poput **Cryptomator** ili **VeraCrypt** za kreiranje šifrovanih virtuelnih diskova. Svi fajlovi unutar kontejnera automatski se enkriptuju i mogu biti otključani samo sa pravilnom lozinkom ili ključ-fajlom.
- **File-level šifrovanje**: svaki fajl se pojedinačno šifruje — bez pravljenja dodatnih foldera ili diskova.
  Alati poput **rclone crypt** ili **gpg** omogućavaju da se svaki fajl pojedinačno šifruje pre upload-a. Ovaj pristup je idealan za skripting i automatizovane tokove rada.
  Transparentni sync alati sa enkripcijom. Transparentna enkripcija omogućava da korisnik vidi fajlove i radi s njima kao i obično, dok se u pozadini dešava automatska zaštita.
  Rešenja kao **Boxcryptor** ili **EncFS** integrišu se sa lokalnim fajl sistemom, pa korisnik radi kao da je sve nešifrovano, dok alat u pozadini šifruje i sinhronizuje promene.
- **Hardware-zaštićeni ključevi**
  Korišćenje USB-tokena ili pametnih kartica (npr. YubiKey) za čuvanje lozinki i privatnih ključeva podiže sigurnost na viši nivo, jer se ključ nikada ne izlaže u memoriji računara.
- **Automatizacija enkripcije**
  Treba konfigurisati skripte ili sistemske task-ove da prave šifrovane bekape i potom ih šalju na cloud, umesto ručnog kopiranja fajlova.

Koraci za lokalnu enkripciju fajlova:

1. Instalirati odabrani alat (Cryptomator, VeraCrypt, rclone, GPG).
2. Generisati novu šifrovanu jedinicu ili ključ (lozinka + salt/fajl).

3. Montirati (ili otvoriti) šifrovani kontejner lokalno.
4. Prebaciti ili sinhronizovati radne fajlove u taj kontejner.
5. Demontirati (zatvoriti) jedinicu nakon završetka rada.
6. Potvrditi da na cloud servisu nikada nisu vidljivi nešifrovani fajlovi.

🔎 ***Salt*** je nasumična vrednost dodata lozinki pre enkripcije, koja obezbeđuje jedinstvenost rezultujućeg heša i štiti od predefinisanih napada. ***Pepper*** je dodatna tajna komponenta, čuvana van baze, koja dodatno zamagljuje rezultate. ***Key stretching*** produžava proces šifrovanja, usporavajući pokušaje nasilnog otkrivanja ključa. Zajedno čine temelje misaone arhitekture digitalne bezbednosti.

🧠 *Lokalna enkripcija nije samo tehnološka praksa, već filozofija rada u kojoj misao ne napušta prostor kontrolisan od strane autora. U vreme kada se sadržaj automatski sinhronizuje, odlučiti da se prethodno zaštiti znači vratiti sebi suverenitet nad sopstvenim idejama.*

📘 Lokalno šifrovanje pre prenosa na udaljeni server garantuje da čak ni cloud provajder, ni napadač ko god pristupio serverima, ne može doći do čistog teksta ili originalnih dokumenata.

🗄️🔐 6.3 Softver za citiranje (Zotero, Mendeley) i zaštita baze

U akademskoj praksi, bibliografska baza nije tek zbir citata – već digitalni ekvivalent lične biblioteke misaonih tragova. Njena nezaštićenost, bilo kroz otvorene priloge ili nešifrovane podatke, može dovesti do izlaganja ranjivih nacrta, beležaka i neobjavljenih radova.

🧠 *Bibliotečka baza je skladište misli – treba je zaštititi kao što se čuva rukopis u sefu.*

🏛️🔐 Zotero: arhitektura i zaštita

Zotero čuva sve podatke lokalno u jednom SQLite fajlu (zotero.sqlite – baza podataka u jednom lokalnom fajlu koji sadrži sve unose, beleške i povezane metapodatke), dok prilozi (PDF, slike, beleške) mogu biti sinhronizovani preko Zotero oblaka ili putem WebDAV-a.

Ključne komponente sistema skladištenja i sinhronizacije su:

- Lokalna baza: `zotero.sqlite` u profilu korisnika
- Sinhronizacija priloga:

- Zotero cloud (podrazumevano nešifrovano)
- WebDAV (protokol za pristup udaljenim folderima kao lokalnim diskovima) – može se hostovati samostalno i enkriptovati.

- Autentifikacija: dvofaktorska zaštita naloga
- Kod: open source, klijent i server dozvoljavaju nezavisne bezbednosne provere

🧩 ***Preporuke:***

- Šifrovati folder baze (npr. VeraCrypt ili Cryptomator)
- Koristiti sopstveni WebDAV sa E2E enkripcijom za priloge
- Praviti redovne offline bekape biblioteke (File → Export Library)

🏛🔐 Mendeley: arhitektura i zaštita

Mendeley čuva lokalnu bazu takođe u SQLite fajlu, a prilozi se sinhronizuju na Elsevier-ove servere bez dodatne enkripcije.

- *Lokalna baza*: SQLite u korisničkom direktorijumu
- *Sinhronizacija priloga*: Elsevier cloud (nešifrovano)
- *Autentifikacija*: opcioni 2FA na nalogu
- *Kod*: zatvoreno / delimično proprietary

🧩 ***Preporuke:***

- Enkriptovati lokalnu biblioteku eksternim alatom
- Redovno izvoziti .bib ili .ris fajl biblioteke
- Čuvati priložene fajlove u šifrovanom folderu izvan Mendeley direktorijuma

🧠 *Reference menadžer ne čuva samo bibliografiju — on beleži trag kretanja kroz znanje. Štititi tu bazu znači štititi mapu sopstvene intelektualne ekspedicije.*

🧩 *Većina korisnika koristi menadžere bez dodatne zaštite — ali to ne znači da je to i bezbedan izbor.*

💡 ***Zaštita bibliografske baze u tri koraka***

1. *Izabrati alat za lokalnu enkripciju (VeraCrypt, Cryptomator).*
2. *Šifrovati glavni folder u kojem se nalazi zotero.sqlite ili Mendeley baza.*
3. *Konfigurisati sinhronizaciju priloga preko bezbednog kanala (WebDAV E2E) ili izbeći cloud sinhronizaciju.*

📊 *Pregled Zotero vs Mendeley*

Funkcija	Zotero	Mendeley
Lokalna baza	SQLite (`zotero.sqlite`)	SQLite
Enkripcija lokalne baze	Ne (zahteva eksterno šifrovanje)	Ne (zahteva eksterno)
Sinhronizacija priloga	Zotero cloud (nešifrovano) ili WebDAV	Elsevier cloud (nešifrovano)
Samostalno hostovanje	Da, putem WebDAV	Ne
Dvofaktorska autentifikacija	Da	Da
Kod	Open source	Delimično / zatvoreno

📘Zaštita reference manager baze podrazumeva više od zaštite fajlova: to je pitanje intelektualne autonomije. Lokalno šifrovanje SQLite baze i sigurni kanali za priloge čine biblioteku otpornom na napade i neovlašćeni uvid.

📚🕰 6.4 Arhiviranje starih verzija u offline skladišta

Čuvanje starih verzija dokumenta nije samo tehnička mera predostrožnosti – to je čuvanje toka istraživanja i tragova intelektualnog rada. Offline arhiva postaje ključna kada mrežni servisi zakažu, kada se desi napad ili kada je potrebno vratiti se na verziju od pre mesec ili godinu dana.

🧠 *Bez arhive, prošlost se briše – offline skladište je digitalni sef memorije*

Deljenje fajlova u „oblaku“ donosi mobilnost, ali ne garantuje dugoročnu sigurnost. Zato se preporučuje paralelna arhiva — na mestu koje nije povezano sa internetom, van domašaja mrežnih rizika i sistemskih grešaka. Offline skladište je prostor autonomije. Za uspešno arhiviranje starih verzija u offline okruženju preporučuju se sledeće prakse:

- Organizacija foldera po verzijama
  - Imenovati direktorijume po datumu i verziji (npr. `Project_v1.0_2025-07-31/`, `Project_v1.1_2025-08-05/`).
  - Zadržati jasnu hijerarhiju: godišnji, mesečni, fazni fajlovi.
- Korišćenje write-once medija
  - Optički diskovi visokog trajanja (M-DISC, Blu-ray) za dugoročno čuvanje.
  - Verifikovanje zapisa posle pisanja i čuvanje liste serijskih brojeva.
- Diskretni eksterni diskovi
  - Eksterni HDD ili SSD, odvojeni od svakodnevnog rada, čuvani na drugoj fizičkoj lokaciji.
  - Naizmenično korišćenje više diskova po principu „rotate-and-store“ podiže stepen otpornosti.
- Šifrovani backup alati
  - Softveri kao BorgBackup, Restic i Duplicity nude enkripciju, deduplikaciju i kompresiju — uz mogućnost vraćanja prethodnih stanja.
- Immutable snimci / snapshot-i
  - ZFS/ZFS-on-Linux snapshot–i ili WORM (write-once-read-many) konfiguracije pružaju zaštitu starih verzija od izmena.
  - Onemogućavanje brisanja starijih verzija bez adekvatnih privilegija.
- Redovna provera i obnavljanje
  - Jednom mesečno otvoriti staru verziju i potvrditi da je funkcionalna.
  - Evidentirati datum kreiranja i poslednje testiranja kopije.

Pravilo 3-2-1 za offline arhivu

1. *Tri kopije podataka (original + dve rezervne).*
2. *Dva različita medija (disk + optički disk / tape).*
3. *Jedna kopija van mesta rada (fizički udaljena lokacija)*

🧠 *Arhiva je odnos prema prošlosti, ne prema rezervi. Kao rukopis na pergamentu, stara verzija nosi tragove misaonog procesa, grešaka, rasta. Offline skladište nije samo bezbedno — ono štiti kontekst i priču iza svakog dokumenta.*

📘 Offline arhiva starih verzija podiže sigurnost istraživanja na viši nivo: štiti od gubitka podataka, omogućava vraćanje na tačno određenu fazu rada i garantuje dugoročno očuvanje intelektualnih tragova.

⚠🔄 6.5 Upravljanje rizicima i preporuke za periodičnu reviziju praksi

Upravljanje rizicima i stalna revizija procesa ključni su za održavanje dugoročne bezbednosti i poverljivosti akademskih podataka. Bez kontinuiranog praćenja i prilagođavanja, čak i najbolje podešene procedure mogu s vremenom postati neefikasne.

🧠 *Upravljanje rizicima je dijalog sa neizvesnošću – svaki pregled vraća kontrolu u ruke autora.*

Delovanje po ustaljenom planu bez periodične kontrole rizika stvara novi rizik, da se ne reguje na nove ranjivosti. Zato je neophodno uspostaviti strukturu pregleda i ažuriranja praksi koja obuhvata tehnologiju, ljude i procedure.

🔍 Ključne aktivnosti za održavanje sigurnosti

- **Redovni sigurnosni auditi**
  - Provera sistema, enkripcije, pravila pristupa i sinhronizacije.
  - Može se obaviti interno ili uz pomoć nezavisnih alata.
- **Procena pristupnih privilegija**
  - Mesečni pregled ko ima pristup bazama, alatima i skladištima.
  - Uklanjanje suvišnih naloga i redefinisanje dozvola.
- **Ažuriranje softvera i kriptografskih ključeva**
  - Instalacija najnovijih verzija enkripcionih alata i reference menadžera.
  - Ključevi se obnavljaju na svake 1–2 godine ili pri sumnji na kompromitaciju.

💡 *Kriptografski ključ je niz znakova koji omogućava šifrovanje i dešifrovanje podataka.*

- **Testiranje oporavka podataka**
  - Povremeno vraćanje bekapa iz offline arhive ili šifrovanih kontejnera.
  - Verifikacija da se fajlovi otvaraju i da nisu oštećeni.
- **Monitoring i logovanje aktivnosti**
  - Aktiviranje beleženja važnih događaja (logovanje): pokušaji pristupa, promene naloga, korišćenje novih uređaja.
  - Analiza mesečnih izveštaja.
- **Obuka i usavršavanje tima**
  - Polugodišnje radionice o digitalnoj diskreciji i bezbednosnim praksama.
  - Deljenje vodiča pri prelasku na nove alate ili metode.

💡 Periodični bezbednosni kalendar

Frekvencija	Aktivnost
Svakog meseca	Pregled pristupa i analiza logova
Svakog kvartala	Audit sistema i ažuriranje softvera
Polugodišnje	Obnavljanje ključeva i interne obuke
Godišnje	Test oporavke podataka iz arhive

Periodična revizija nije znak sumnje u sistem, već znak poverenja u sopstvenu disciplinu. Ona potvrđuje da intelektualni rad zaslužuje ne samo zaštitu, već i pažnju u vremenu.

📘 Upravljanje rizicima podrazumeva spremnost za prilagođavanje — ne kao izuzetak, već kao temelj bezbednosti. Mislilac koji redovno osvežava sopstvene procedure štiti ne samo podatke, već i etiku svog rada.

🧱🌐 7. Blockchain i decentralizovane tehnologije

U akademiskim krugovima se sve češće raspravlja o nezavisnosti, transparentnosti i nepovredivosti podataka. Decentralizovane mreže i pametni ugovori otvaraju nove mogućnosti za verifikaciju autorstva, čuvanje i distribuciju istraživačkih fajlova, ali i za inovativne tokove recenzije i zaštitu od cenzure.

🧠 *Blockchain je knjiga poverenja koju pišu svi, a ne samo izdavač.*

⏱📜 7.1 Verifikacija izvornog autorstva putem vremenskog pečata u smart ugovorima

Sve češće se postavlja pitanje kako u digitalnom okruženju dokazati da je određeni tekst, podatak ili vizuelni prikaz zaista nastao u rukama konkretnog autora i u tačno određenom trenutku. Pametni ugovori zasnovani na blockchain tehnologiji nude rešenje: kriptografski otisak rada se trajno beleži na mreži, čime se uspostavlja digitalni pečat originalnosti.

🧠 *Kada se ideja zabeleži na lancu blokova, ona prestaje da bude pretpostavka i postaje dokaz.*

🔍 Objašnjenje ključnih pojmova

- **Kriptografski otisak (hash)**
  - Jedinstveni digitalni „potpis“ fajla – ako se ijedan znak u sadržaju promeni, hash se menja.
  - Primer: fajl „Rukopis.docx“ generiše hash `a7b9...` putem SHA256 algoritma.
- **Pametni ugovor (smart contract)** – kod koji se automatski izvršava na blockchainu – u našem kontekstu, on beleži hash i vremensku oznaku bez potrebe za posrednikom.
- **Timestamping** – proces u kome pametni ugovor beleži tačan trenutak kada je dokument registrovan – vremenska oznaka postaje neizbrisiv deo lanca.

🗀 Proces verifikacije autorstva

1. Autor završava rad (npr. nacrt članka u PDF formatu).
2. Koristi alat za generisanje hasha (npr. Hasher, lokalni SHA256 generator).
3. Hash se unosi u pametni ugovor na blockchain mreži (npr. Ethereum, Polygon).
4. Ugovor beleži hash i datum upisa.
5. U svakom trenutku, bilo ko može proveriti da li dokument ima dokaz o autorstvu za konkretan datum – upoređivanjem hasha dokumenta sa onim na mreži.

💡 Zašto je ovo važno za akademskog mislioca?

- 📌 **Dokaz o vremenu nastanka** – idealno za istraživačke podatke, radne verzije, idejna rešenja.
- 📌 **Prevencija plagijata** – dokument sa ranijim hash zapisom na blockchainu potvrđuje prvenstvo autorstva.
- 📌 **Nezavisnost od izdavača** – dokaz postoji bez obzira da li je rad objavljen u časopisu.
- 📌 **Interdisciplinarna primena** – primenljivo na tekstove, audio beleške, modele, vizualizacije, pa i datasetove.

💡 *Kako započeti*

Korak	Preporučeni alat / platforma
Generisanje hasha	Hasher.online, OpenSSL, hashdeep
Izbor blockchain mreže	Ethereum, Polygon, Arweave
Kreiranje pametnog ugovora	EtherStamp, OriginStamp, Timestamp.org
Deljenje dokaza	Preporučuje se deljenje ugovora (ID/link) sa saradnicima koji žele da potvrde vremenski pečat.

U svetu u kome se digitalna reč lako kopira, pravi pečat autorstva nije logo ni potpis — to je kriptografski trag zapisan u vremenskom sloju koji niko ne može promeniti.

7.2 Distribucija i skladištenje podataka na IPFS-u

U akademskim krugovima se sve češće raspravlja o načinima da se istraživački podaci i radovi očuvaju izvan centralizovanih sistema. IPFS (InterPlanetary File System) predstavlja decentralizovani sistem za čuvanje i deljenje fajlova, u kome se dokumenti ne identifikuju po adresi servera, već po sopstvenom sadržaju. Svaki fajl ima jedinstveni digitalni otisak — koji garantuje da su sadržaj i integritet zaštićeni.

U sistemu gde adresa više nije mesto, već sadržaj, autor vraća kontrolu nad sopstvenim radom.

Objašnjenje osnovnih pojmova

- **Content addressing.** Umesto da se fajl traži po URL adresi (lokaciji), IPFS koristi hash fajla kao identifikator — svaka izmena u fajlu menja njegov identifikator.
- **Swarm (mreža čvorova).** Grupa računara širom sveta koja razmenjuje i čuva delove fajlova — bez centralnog servera.
- **Pinning.** Akt „kačenja“ fajla na određeni čvor, čime se garantuje dugoročna dostupnost. Može se zamisliti *kao kačenje dokumenta na oglasnu tablu: dok je zakačen, dostupan je svima*.
- **Gateway.** Veza između IPFS-a i klasičnog weba — omogućava korisnicima da pristupe sadržaju putem internet pregledača (npr. `https://ipfs.io/ipfs/Qm...`).

Primer iz akademskog konteksta

Zamislimo istraživača koji želi da dataset ostane dostupan i nakon objavljivanja rada. Umesto klasičnog linka koji može zastariti, on postavlja fajl na IPFS i u fusnoti članka navodi njegov hash. Taj hash vodi direktno do sadržaja — nepromenjenog, proverljivog i trajnog.

Koraci za upotrebu IPFS-a

1. **Instalacija IPFS klijenta.** Preuzeti **IPFS Desktop** za jednostavno korišćenje, ili **go-ipfs** za naprednije korisnike.
2. **Dodavanje fajlova.** Korišćenjem komande `ipfs add dokument.pdf`, dobija se jedinstveni hash (npr. `QmXy…`).
3. **Pinovanje sadržaja.** Fajl se „kači“ na čvor — bilo lokalno ili kroz servis kao što su **Pinata** ili **Infura**.

4. **Deljenje hash adrese.** Hash se može podeliti putem e-maila, uključiti u publikaciju ili dodati pametnom ugovoru (v. tačku 7.1).
5. **Pristup sadržaju.** Bilo ko može otvoriti `https://ipfs.io/ipfs/QmXy...` i preuzeti fajl — bez obzira na lokaciju originala.

💡 **Zašto IPFS ima smisla za akademsku zajednicu**

- ✅ **Otpornost na cenzuru**: čak i ako se glavni server ugasi, fajl ostaje dostupan na drugim čvorovima.
- ✅ **Integritet podataka**: svaka izmena menja hash — obezbeđuje nepromenljivost.
- ✅ **Fleksibilna dostupnost**: radovi, prilozi i datasetovi mogu se podeliti bez posrednika.
- ✅ **Sinergija sa blockchainom**: hash fajla može se timestampovati (vidi 7.1) radi dokazivanja autorstva.

💡 *Preporučeni alati i servisi*

Alat / servis	Namena	Posebna prednost
IPFS Desktop	Grafički klijent za IPFS	Intuitivan interfejs za dodavanje fajlova
go-ipfs	Komandna linija za napredne	Napredne mogućnosti kontrole i integracije
Pinata	Pinning servis	Automatski pinovanje i API pristup
Infura IPFS	Gateway i pinning servis	Povezivanje sa blockchain aplikacijama
Textile Powergate	Dugoročno skladištenje + enkripcija	Skaliranje i šifrovanje akademskih datasetova

Decentralizovana mreža nije samo tehnologija otpora – to je manifest autonomije znanja, gde svaki istraživač postaje čuvar sopstvenog doprinosa.

📘 IPFS omogućava da se akademski materijali čuvaju i dele bez oslanjanja na centralizovane servise — uz garanciju dostupnosti, nepromenljivosti i sinergije sa blockchain verifikacijom. Time se stvara novi okvir poverenja u deljenje znanja.

7.3 Sledljivost i evidencija toka digitalnih sertifikata

U akademskim krugovima raste potreba za jasnom evidencijom svih koraka u izdavanju, potvrđivanju i prenosu dokumenata i sertifikata. Decentralizovani zapisi na blockchainu omogućavaju vidljiv, neizmenjiv trag procesa — od prvog unosa do opoziva.

🧠 Transparentnost je novi ugovor poverenja: svaka transakcija postaje javni testament odgovornosti.

Ključni pojmovi

- **Zapis događaja (transaction log) -** Svaka akcija — kreiranje, izmena, prenos — beleži se u lancu kao transakcija sa autorom i vremenom.
- **Digitalni sertifikat (tokenized credential) -** Pametni token koji predstavlja diplomu, uverenje ili dozvolu, sa metapodacima o izdavaču i vlasniku.
- **Governance smart ugovor -** Pravila ugrađena u kod: definišu ko i kako može da emituje, potvrđuje ili opozove sertifikat.
- **Audit trail -** Hronološki, nepovrediv zapis svih interakcija — dostupan svim akterima, bez centralnog posrednika.

Kako funkcioniše proces

1. **Emitovanje sertifikata**
   - Izdavalac kreira token putem smart ugovora (npr. Blockcerts).
   - Token sadrži metapodatke: ime, datum izdavanja, identifikator izdavača.
2. **Distribucija i verifikacija**
   - Student ili istraživač prima link ili hash tokena.
   - Bilo ko (poslodavac, saradnik) proverava validnost putem blockchain explorer-a.
3. **Opoziv i obnova**
   - Ako je certifikat opozvan ili ažuriran, novi token beleži promenu, a stari ostaje u istoriji.
   - Uvid u status: validan / opozvan / izmenjen.
4. **Integracija u tokove rada**
   - Lokalni akademski informacioni sistem, servisi za elektronsko potpisivanje i institucionalni repozitorijumi mogu se povezati sa blockchain slojem.

- Beleženje događaja, poput odbrane teze ili završetka kursa, može se automatizovati putem pametnih ugovora.

💡 **Zašto transparentnost logistike i digitalnih certifikata ima smisla za akademsku zajednicu**

- ✅ Vidljivost svih koraka garantuje odgovornost izdavača i nosioca certifikata.
- ✅ Brza, jednostavna provera validnosti — bez poziva ili e-maila univerzitetu.
- ✅ Otpornost na falsifikate i lažne dokumente; svaka promena je javno zabeležena.
- ✅ Dugoročna dostupnost zapisa čak i kada originalni portal ili izdavač prestane s radom.

Svaki digitalni sertifikat je priča o poverenju: kada se unese u decentralizovanu knjigu, autoritet postaje transparentan, a verifikacija — kolektivna.

💡 **Preporučeni alati i platforme**

Platforma / alat	Svrha	Posebna prednost
Blockcerts	Open-source za izdavanje sertifikata	Standardizovani JSON-LD tokeni
Hyperledger Indy	Digital ID i verifikacija	Fokus na decentralizovanu identifikaciju
Ethereum / Polygon	Opšti blockchain sloj	Široka podrška smart ugovorima
Sovrin	Decentralizovani ID ekosistem	Specijalizovan za verifikaciju dozvola
uPort / Veramo	Wallet rešenja za korisnike	Intuitivno čuvanje i prikaz tokena

📘 Transparentna logistika i tokenizacija certifikata na blockchainu podižu izdavanje i proveru akademskih dokumenata na nivo javne evidencije. Svi koraci postaju proverljivi, a sistem — otporan na manipulacije.

⚖️🛡️ 7.4 Scenariji upotrebe za peer review i izbegavanje cenzure

Zamislimo recenzentski proces u kome izveštaji ostaju anonimni, nepromenljivi i dostupni bez dozvole izdavača. Decentralizovane mreže to već omogućavaju: uz IPFS i blockchain, recenzije, članci i komentari mogu se trajno očuvati, bez zavisnosti od platformi koje kontrolišu pristup.

🧠 Recenzija nije samo tehnička procena — to je misaoni trag koji zaslužuje trajnost i slobodu.

📂 Primeri primene decentralizovanih tehnologija

- **Anonimni depozit recenzija**
  Recenzentski izveštaji se postavljaju na IPFS; njihov digitalni otisak (hash) beleži se na blockchainu.
  - Autor i urednik dobijaju potvrdu o prijemu izveštaja, ali identitet recenzenta ostaje zaštićen.
  - Hash je digitalni pečat fajla — menja se čak i ako se dodaje samo razmak u tekstu.
- **Otvoreni repozitorijumi radova**
  Naučni članci mogu se hostovati na decentralizovanim čvorovima, bez zavisnosti od jedne platforme.
  - Ako se centralni server ugasi ili se pristup ograniči, članak ostaje dostupan na drugim IPFS čvorovima.
  - Time se omogućava trajna dostupnost istraživačkih rezultata.

  Tokenizacija recenzentskog rada
  Svaki objavljeni komentar ili izveštaj može biti nagrađen digitalnim tokenom.
  - Pametni ugovor beleži doprinos, a reputacija recenzenta raste sa brojem verifikovanih doprinosa.
  - Tokeni se ne odnose na novac, već na potvrdu rada i doprinos akademskoj zajednici.
- **Otpornost na cenzuru**
  Decentralizovano čuvanje članaka i podataka onemogućava da izdavač jednostavno ukloni sadržaj.
  - Istraživač može podeliti rad sa zajednicom bez potrebe za dozvolom ili validacijom centralnog sistema.
  - Time se štite misaona sloboda i distribucija ideja.

💡 Koraci za prvu primenu decentralizovanih rešenja

1. Izabrati mrežu za deployment pametnog ugovora (Ethereum, Polygon, Tezos).
2. Generisati hash radnog fajla pomoću lokalnog alata (npr. SHA256).
3. Kreirati pametni ugovor koji beleži vremenski pečat (timestamping).
4. Postaviti dokument na IPFS pomoću lokalnog čvora ili pinning servisa.
5. Hash dokumenta i podatke iz ugovora podeliti sa saradnicima radi transparentne verifikacije.
6. Istražiti alate poput Arweave-a i Textile-a za dugoročno, šifrovano skladištenje.

Recenzija je susret mišljenja — kada se ona oslobodi od platformi koje odobravaju ili odbacuju, znanje dobija svoj sopstveni prostor. Decentralizacija ne štiti samo dokumente, već slobodu akademske razmene.

📘 Primena blockchaina i IPFS-a u recenzentskom procesu omogućava anonimnost, neizmenjivost i dostupnost bez ograničenja. Od depozita izveštaja do tokenizacije doprinosa, istraživački rad dobija trajni otisak — nezavisan od institucionalnih barijera i izdavačkih ograničenja.

8. Upravljanje digitalnim identitetom

U digitalnom okruženju, identitet istraživača više nije samo ime i prezime — to je skup povezanih naloga, publikacija, adresa, metapodataka i tragova aktivnosti. Od ORCID-a i DOI oznaka, preko institucionalnih profila, do alternativnih persona i pseudonima, akademski mislilac mora da balansira između vidljivosti, kredibiliteta i zaštite.

Digitalni identitet nije samo potpis — to je misaoni otisak koji ostaje i kad se svetlost interfejsa ugasi.

Razmotrićemo kako se identitet gradi, štiti i prilagođava različitim kontekstima: od javnog nastupa u akademskoj zajednici, do diskretne komunikacije u osetljivim istraživačkim tokovima.

8.1 Balans između akademskog kredibiliteta i anonimnosti

U digitalnom svetu istraživački identitet zahteva vidljivost za karijeru, ali i diskreciju kad se bavimo osetljivim temama. Pravi balans omogućava da objektivnost, reputacija i zaštita privatnosti koegzistiraju bez kompromisa.

Vidljivost gradi kredibilitet, ali pametna nevidljivost čuva slobodu mišljenja.

Objašnjenje ključnih pojmova

- **ORCID (Open Researcher and Contributor ID).** Jedinstveni, trajni identifikator istraživača koji povezuje sve autorove publikacije, projekte i grantove.
- **DOI (Digital Object Identifier).** Metapodatak dodeljen radu ili datasetu radi trajnog, pouzdanog referenciranja i citiranja.
- **Pseudonim.** Alternativno ime ili alias koji štiti vašu privatnost u osetljivim diskusijama ili publikacijama.

Ključne strategije za uspostavljanje balansa

- **Javna i privatna lica**
  - ORCID i profesionalni profil (LinkedIn, ResearchGate) koristite za zvanične publikacije i saradnje.
  - Pseudonim ili drugi nalog pogodan je za blogove, forume ili istraživanja o kontroverznim temama.

- **Segmentacija komunikacije**
  - Poslovna e-adresa i privatni email za saradnju pod imenom.
  - Upotreba zasebne e-mail adrese na enkriptovanim servisima (ProtonMail, Tutanota) za komunikaciju pod pseudonimom.
- **Dosledno upravljanje metapodacima**
  - Svakom radu se dodeljuje DOI, koji se povezuje sa ORCID nalogom radi potvrde autorstva i kredibiliteta.
  - Veza između stvarnog imena i pseudonima beleži se u zaštićenoj evidenciji — radi eventualne verifikacije.
- **Rezervni digitalni profili**
  - Za pseudonime koji imaju kontinuitet u istraživačkom radu može se kreirati zaseban praćenja doprinosa i reputacije — bez povezivanja sa stvarnim identitetom. profil radi
  - Pristupni podaci se čuvaju u posebnoj aplikaciji za upravljanje lozinkama, odvojeno za svaki digitalni identitet.

💡 *Kratki saveti*

Cilj	Preporučena praksa
Vidljivost i kredibilitet	Ažuriranje ORCID naloga, uparivanje DOI oznaka, uključivanje biografskih podataka
Diskrecija i zaštita privatnosti	Korišćenje pseudonima i šifrovanih email servisa
Organizacija i praćenje	Vođenje evidencije profila i lozinki u bezbednoj aplikaciji za upravljanje poverljivim podacima (npr. Bitwarden, KeePassXC, Proton Pass)

🧠 Pravi akademski otisak nije onaj koji je najvidljiviji, već onaj koji ostaje istinit i autentičan čak i u senkama anonimnosti.

📘 Balans između ORCID-a i pseudonima štiti reputaciju i sigurnost. Segmentacijom komunikacije i doslednim upravljanjem metapodacima, možete istovremeno sticati kredibilitet i čuvati privatnost istraživanja.

🧑‍💻 8.2 Kreiranje i čuvanje rezervnih digitalnih persona

Rezervne digitalne persone (alternativni identiteti) deluju kao nezavisni entiteti koji omogućavaju slobodu izražavanja i dodatnu zaštitu misliocu kada se bavi osetljivim temama ili anonimizovanim diskusijama. Pružaju

misaonu fleksibilnost u komunikaciji, bez gubitka kontrole nad integritetom glavnog digitalnog identiteta.

🧠 Rezervna persona nije bekstvo od odgovornosti, već misaoni instrument koji štiti originalni identitet i hrabri na eksperiment.

🔍 Objašnjenje ključnih pojmova

- **Digitalna persona**
  Online identitet kreiran pod pseudonimom, koji obuhvata alias (korisničko ime), posebnu e-adresu, profilnu sliku i prateće metapodatke. Koristi se za diskretnu komunikaciju i anonimizovane doprinose.
- **Rezervni profil**
  Poseban nalog koji se koristi samo u određenim kontekstima, odvojen od glavnog istraživačkog identiteta.
- **Upravljanje aliasima**
  Postupak kreiranja, čuvanja i ažuriranja više pseudonima bez međusobnog otkrivanja.

📋 Ključne strategije za kreiranje i čuvanje

- **Definisanje svrhe**
  Određuje se kontekst u kome će rezervna persona biti aktivna (npr. diskusije o osetljivim temama, eksperimentalni blog, recenzentski doprinos).
- **Izbor platformi**
  Biraju se servisi koji ne zahtevaju lične podatke i podržavaju end-to-end enkripciju (ProtonMail, Tutanota, decentralizovane mreže).
- **Kreiranje identiteta**
  Odabira se jedinstven alias, registruje odgovarajuća e-adresa i profil sa minimalnim metapodacima.
- **Zaštita pristupa**
  Lozinke se čuvaju u bezbednoj aplikaciji za upravljanje poverljivim podacima (npr. Bitwarden, KeePassXC). Aktivira se dvofaktorska autentifikacija gde je moguće.
- **Dokumentovanje veze**
  Veza između glavnog i rezervnog identiteta beleži se u zaštićenoj evidenciji — bez deljenja s trećim stranama.

- **Redovno održavanje**
  Periodično se proverava validnost naloga, ažuriraju lozinke i brišu neaktivni profili.

💡 Koraci za izradu rezervne digitalne persone

1. Definisati cilj upotrebe (npr. anonimizovana publika, neusmerena recenzija).
2. Izabrati alias i kreirati novu e-adresu na enkriptovanom servisu.
3. Registrovati naloge na odabranim platformama uz minimalne metapodatke.
4. Konfigurisati sigurnosne postavke (2FA, end-to-end enkripciju).
5. Uneti belešku o vezi između identiteta u zaštićenoj evidenciji.
6. Svakih 3–6 meseci proveriti i ažurirati pristupne podatke.

🧠 Rezervna persona oslobađa istraživača da eksperimentiše s idejama bez straha od reputacionih posledica, a istovremeno čuva integritet glavnog identiteta.

🎭 Ilustracija: Rezervna persona u istraživanju osetljivih tema

Todor je filozof koji istražuje **etiku manipulacije u geopolitici**. Njegovi radovi problematizuju političku odgovornost elita i izazivaju žive akademske rasprave. Iako je njegovo glavno digitalno prisustvo vezano za univerzitetski profil, odlučuje da kreira rezervnu digitalnu personu — pod pseudonimom ***Ethikos78***.

Ova persona mu omogućava:

- Da diskutuje sa recenzentima bez predrasuda vezanih za njen dosadašnji rad
- Da pristupa zatvorenim forumima gde se traži diskrecija i zaštita identiteta
- Da deli nacrte istraživanja bez straha od institucionalnih reakcija

Svi tekstovi koje objavi preko *Ethikos78* ostaju misaono usklađeni sa njenim integritetom — ali joj daju prostor za slobodno izražavanje, eksperimentaciju i dijalog koji inače ne bi bio moguć.

💡 *Todor koristi rezervnu personu ne kao masku koja skriva istinu, već kao misaoni alat za proširenje mogućnosti promišljanja bez kompromisa po svoj glavni identitet.*

📘 Kreiranje i pravilno čuvanje rezervnih digitalnih persona obezbeđuje anonimnost i fleksibilnost u radu na osetljivim temama, dok glavnom profilu ostavlja netaknutu profesionalnu reputaciju.

Dok su rezervne digitalne persone stub anonimnosti, e-mail adrese i domeni ostaju primarna tačka na koju napadači ciljaju. Sledeća tema bavi se zaštitom ovih ulaznih tačaka od neželjene i zlonamerne pošte.

✉🛡 8.3 Zaštita e-mail adresa i domena od spam i phishing napada

🧠 *Neželjena pošta i phishing nisu samo tehnički problemi, već pretnja poverenju i bezbednosti istraživanja.*

🔍 Objašnjenje ključnih pojmova

- **Spam –** Neželjena elektronska pošta s promotivnim ili zlonamernim sadržajem.
- **Phishing –** Tehnika obmane radi krađe poverljivih podataka, maskiranjem kao legitimna komunikacija.
- **Domen –** Deo e-mail adrese iza znaka @, koji predstavlja organizaciju ili pojedinca.
- **SPF** (Sender Policy Framework) – DNS-zapis koji definiše koji serveri smeju da šalju poštu s datog domena.
- **DKIM** (DomainKeys Identified Mail) – Kriptografski potpis u zaglavlju poruke, koji potvrđuje integritet i autentičnost.
- **DMARC** (Domain-based Message Authentication, Reporting & Conformance) – Politika koja određuje kako postupiti s porukama koje ne prođu SPF ili DKIM proveru i šalje izveštaje o takvim slučajevima.

📋 Ključne strategije za zaštitu

- Konfigurisati SPF zapis u DNS-u i navesti sve legitimne poštanske servere.
- Implementirati DKIM potpisivanje za svu izlaznu poštu.
- Usmeriti politiku DMARC na „quarantine“ ili „reject“ i pratiti izveštaje o neuspelim proverama.
- Koristiti alias adrese i poddomene za različite svrhe: zvaničnu, internu i pseudonim skupljanje.
- Aktivirati dvostepenu autentifikaciju (2FA) na svim e-mail nalozima.

- Redovno proveravati DMARC izveštaje radi identifikovanja zlonamernih pokušaja.
- Sprovoditi edukaciju o prepoznavanju phishing poruka među saradnicima.

💡 *Kratki saveti*

Cilj	Preporučena praksa
Očuvanje reputacije domena	SPF, DKIM i DMARC zapisi u DNS-u
Smanjenje neželjene pošte	Alias adrese, filtriranje i beleženje spam-listi
Zaštita od phishinga	Dvostepena autentifikacija, ažuriranje lozinki, redovna obuka

🧠 *Pažljivo podešen sistem e-pošte ne čuva samo poruke, već i poverenje koje one nose.*

📘 Primena SPF, DKIM i DMARC politika, upotreba aliasa i 2FA čine e-mail adrese i domen otporni na neželjenu poštu i phishing, čime se štiti akademski identitet i integritet komunikacije.

9. Metapodaci, etički izazovi i otvorena nauka

Nakon što su digitalni identiteti i komunikacione zaštite postavili temelje bezbednosti, prelazimo na sloj informacija koji je često nevidljiv — metapodatke.

Oni imaju moć da obogate istraživanje, poboljšaju dostupnost i interoperabilnost, ali ako se koriste neodgovorno, mogu ugroziti privatnost učesnika, narušiti integritet saradnika i oslabiti poverenje u nauku.

U kontekstu otvorene nauke, metapodaci predstavljaju ključnu tačku susreta između transparentnosti i etičke odgovornosti — i zahtevaju precizno, refleksivno postupanje.

9.1 Objašnjenje ključnih pojmova

- **Metapodaci** – Podaci o podacima: opisne, strukturne ili administrativne oznake koje olakšavaju organizaciju, pretragu i ponovno korišćenje istraživačkog materijala.
- **Geolokacija** – Koordinatni podaci mesta prikupljanja uzorka, često automatski ugrađeni u fotografije, audio ili video fajlove.
- **Lične oznake** – Informacije koje mogu otkriti pojedinca, kao što su pseudonim, adresa e-pošte, ID uređaja, ime ispitanika u transkriptu.
- **FAIR principi** (videti 9.2) – Skup smernica za upravljanje podacima: Findable (pronađivo), Accessible (pristupačno), Interoperable (međusobno povezivo), Reusable (ponovno upotrebljivo).
- **Otvorena nauka** – Praksa transparentnog deljenja istraživačkih rezultata i metoda, uz poštovanje granica privatnosti i etičke dozvole.

9.2 Metapodaci

Metapodaci su dodatni sloj informacija o istraživačkom materijalu — kada i gde je kreiran, ko je učestvovao, pod kojim uslovima je analiziran i kako se može ponovo upotrebiti.

Pravilno oblikovani metapodaci olakšavaju pronalaženje, razumevanje i povezivanje podataka između različitih sistema.

Međutim, nepromišljeno otkrivanje detalja poput geolokacije ili ličnih oznaka može izložiti učesnike riziku i narušiti integritet istraživačkog procesa.

🧠 *Metapodaci su glas koji priča priču o podacima — ako taj glas ne štiti poverljivost, narušava etiku.*

📋 Ključne strategije za odgovorno postupanje

- **Uklanjanje ili maskiranje geolokacije i ličnih oznaka**
  - Pre distribuiranja fajlova (fotografija, GIS podaci) izbrisati ili anonimizovati GPS tagove.
  - U tekstualnim transkriptima i tabelama zameniti imena ili specifične lokacije pseudonimima ili generičkim opisima ("Lokacija A", "Ispitanik 1").
  - Metapodatke uskladiti sa međunarodnim šemama (Dublin Core, DataCite) radi meĐuplatformske interoperabilnosti.
  - Navesti izvor podataka i metodologiju u metapodacima, ali skrivati osetljive detalje u zasebnom, kontrolisanom dokumentu.
  - U referencama koristiti trajne identifikatore (DOI, Handle) umesto putanja do lokalnih fajlova.

💡 *Kratki saveti*

Cilj	Preporučena praksa
Zaštita privatnosti ispitanika	Brisanje GPS tagova, anonimizacija ličnih oznaka
Unapređenje dostupnosti i interoperabilnosti	Standardizovani metapodaci (Dublin Core, DataCite)
Transparentnost bez ugrožavanja poverljivosti	Odvajanje osetljivih detalja, upotreba DOI i trajnih identifikatora

🧠 Metapodati grade mostove između istraživanja i zajednice — ali bez etičkih temelja, ti mostovi ne vode poverenju, već ranjivosti.

📘 U sledećim tačkama razmatramo kako etičko deljenje podataka i transparentno povezivanje izvora produbljuju ovaj most i učvršćuju strukturu otvorene nauke.

⚖️🗁 9.3 Etičko deljenje podataka i FAIR principi

Otvorena nauka podrazumeva dostupnost istraživačkih podataka, ali dostupnost ne znači odsustvo odgovornosti.

Deljenje podataka mora biti utemeljeno na etičkim principima — uz poštovanje privatnosti ispitanika, autorskih prava, tehničke interoperabilnosti i dugoročnog integriteta informacija.

🧠 *Otvorenost bez etike nije transparentnost — već izloženost.*

🔍 Objašnjenje ključnih pojmova

- **Etičko deljenje podataka –** Praksa koja obezbeđuje da se podaci dele uz saglasnost, zaštitu identiteta i jasno definisane granice upotrebe.
- **Licenciranje –** Pravna oznaka koja definiše kako se podaci mogu koristiti.
  U okviru otvorenog pristupa često se koristi licenca **CC-BY-4.0** (Creative Commons – Atribucija), koja omogućava slobodno korišćenje, adaptaciju i redistribuciju sadržaja, uz obavezno navođenje izvora.
  - Oznaka *CC-BY* označava obavezu atribucije autora.
  - Oznaka *CC-NC* (Nekomercijalno) zabranjuje komercijalnu upotrebu.
  - Oznaka *CC-ND* (Bez prerade) zabranjuje modifikaciju sadržaja.
  - Oznaka *CC-SA* (Deljenje pod istim uslovima) zahteva da se adaptirani sadržaj deli pod istom licencom.
  - Licenca *CC0* (Creative Commons Zero) označava potpuno odricanje od autorskih prava — sadržaj se stavlja u javno vlasništvo i može se koristiti bez ograničenja, bez obaveze navođenja autora.

📋 Preporučene prakse

- **Priprema podataka za deljenje**
  - Podaci se organizuju u strukturisane formate (CSV, JSON, XML) uz jasne opise i metapodatke.
  - Osetljivi podaci se uklanjaju, maskiraju ili izdvajaju u zasebne, kontrolisane skupove.

- **Primena FAIR principa**
  - FAIR principi (videti objašnjenje u tački 9) podrazumevaju tehničku i etičku pripremu podataka za deljenje, uz jasno definisane uslove pristupa i ponovne upotrebe.
  - Metapodaci se usklađuju sa standardima kao što su Dublin Core, DataCite ili schema.org.
  - Podaci se objavljuju na repozitorijumima koji podržavaju trajne identifikatore (DOI, Handle).
  - Pristup se definiše kroz licence koje jasno navode dozvoljene oblike korišćenja.
- **Etika u otvorenosti**
  - Pre deljenja podataka, pribavlja se saglasnost učesnika (ako je primenljivo).
  - U slučaju sekundarne upotrebe, navodi se izvor i poštuju se ograničenja prvobitne dozvole.
  - Podaci se ne dele ako postoji rizik od identifikacije ili štete za učesnike.

💡 ***Kratki saveti***

Cilj	Preporučena praksa
Priprema za deljenje	Strukturisani formati, jasni metapodaci, uklanjanje osetljivih informacija
Usklađenost sa FAIR principima	Standardizovani metapodaci, trajni identifikatori, jasne licence
Etika i odgovornost	Saglasnost učesnika, poštovanje ograničenja, izbegavanje štetnih objava

🧠 *Podaci nisu samo brojevi — oni nose priče, učesnike i kontekste. Deljenje bez razumevanja tih slojeva može otvoriti vrata zloupotrebi, umesto saradnji.*

📘 Etičko deljenje podataka podrazumeva tehničku pripremu, pravnu jasnoću i moralnu doslednost. U otvorenoj nauci, poverenje se ne podrazumeva — ono se gradi postupkom.

9.4. Transparentno povezivanje izvora bez ugrožavanja poverljivosti

Transparentnost u istraživanju podrazumeva jasno navođenje izvora, metoda i konteksta. Međutim, kada se radi o osetljivim podacima, prekomerna otvorenost može ugroziti privatnost učesnika ili saradnika. Potrebno je pronaći ravnotežu između dostupnosti informacija i zaštite poverljivosti.

🧠 *Otvoreno ne znači izloženo — izvor može biti vidljiv, ali ne mora biti otkriven do poslednjeg detalja.*

Objašnjenje ključnih pojmova

- **Transparentnost izvora**
  Jasno navođenje porekla podataka, metodologije i konteksta u kojem su prikupljeni.
- **Poverljivost**
  Zaštita identiteta, lokacije i drugih osetljivih informacija koje mogu dovesti do identifikacije učesnika.
- **Trajni identifikatori**
  Standardizovane oznake (npr. DOI, Handle) koje omogućavaju stabilno povezivanje sa izvorima bez otkrivanja lokalnih putanja ili ličnih podataka.

Preporučene prakse

- **Korišćenje trajnih identifikatora**
  - Umesto direktnih linkova ka lokalnim fajlovima, koristi se DOI, Handle ili drugi repozitorijumski identifikatori.
  - Time se obezbeđuje stabilnost izvora bez otkrivanja infrastrukture ili ličnih podataka.
- **Odvajanje opštih i osetljivih metapodataka**
  U javnim dokumentima navode se opšti podaci o izvoru (npr. metod, godina, tip uzorka), dok se osetljivi detalji (npr. tačna lokacija, identitet učesnika) čuvaju u zasebnoj evidenciji sa ograničenim pristupom.
- **Obeležavanje izvora bez direktne atribucije**
  - Kada je potrebno zaštititi identitet saradnika, koristi se neutralna oznaka („Izvor A“, „Partner 3“) uz opisni kontekst.

- U internim dokumentima može se voditi evidencija o stvarnim identitetima, ali bez javnog objavljivanja.

- **Usklađivanje sa etičkim smernicama**
  Transparentnost se prilagođava etičkim okvirima projekta, uz konsultaciju sa etičkim odborima ili smernicama institucije.

💡 *Kratki saveti*

Cilj	Preporučena praksa
Stabilno povezivanje izvora	Korišćenje DOI, Handle i drugih trajnih identifikatora
Zaštita osetljivih informacija	Odvajanje javnih i poverljivih metapodataka, ograničen pristup
Diskretna atribucija saradnika	Neutralne oznake u javnim dokumentima, interna evidencija stvarnih identiteta

🧠 Transparentnost nije samo čin otkrivanja, već veština balansiranja između dostupnosti i zaštite. Dobro obeležen izvor ne mora biti potpuno razgolićen — dovoljno je da bude misaono dostupan.

📘 Transparentno povezivanje izvora zahteva tehničku preciznost, etičku osetljivost i jasno razgraničenje između javnog i poverljivog. Korišćenjem trajnih identifikatora i neutralnih oznaka, moguće je očuvati integritet istraživanja bez ugrožavanja učesnika.

Transparentnost i etika u deljenju podataka imaju smisla samo ako se podaci mogu očuvati kroz vreme.

Arhiviranje nije samo tehnički proces — to je misaona odluka o tome šta ostaje dostupno, kako se čuva, i pod kojim uslovima se prenosi budućim generacijama istraživača.

🗂️ U tački 10 razmatraju razmatraju se strategije za dugoročno čuvanje podataka — od izbora formata i repozitorijuma, do očuvanja dostupnosti kroz vreme.

.

10. Arhiviranje i dugoročno čuvanje

Otvorena nauka ne završava objavljivanjem — ona se nastavlja kroz očuvanje. Dugoročno čuvanje podataka zahteva planiranje, tehničku preciznost i misaonu odgovornost.

Cilj nije samo da podaci prežive, već da ostanu dostupni, razumljivi i proverljivi i za naredne generacije istraživača.

🧠 Arhiviranje je oblik misaone brige — o budućem korisniku, o trajnosti znanja, o odgovornosti prema vremenu.

Objašnjenje ključnih pojmova

- **Arhiviranje** — Organizovano čuvanje dokumentacije u fizičkom ili elektronskom obliku, uz klasifikaciju, indeksiranje i zaštitu
- **Dugoročno čuvanje** — Obezbeđivanje dostupnosti, integriteta i upotrebljivosti podataka tokom više godina ili decenija
- **Trajni identifikatori** — DOI, Handle i slični sistemi koji omogućavaju stabilno povezivanje sa dokumentima bez obzira na promene infrastrukture
- **Format pogodan za čuvanje** — Otvoreni, dokumentovani formati (npr. PDF/A, XML, CSV) koji ne zavise od vlasničkog softvera
- **Formatna diverzifikacija** — Čuvanje istog sadržaja u više tehničkih formata (npr. PDF/A, TXT, XML) radi otpornosti na zastarevanje softvera.
- **Fizička diverzifikacija** — Skladištenje kopija na različitim medijima i lokacijama, npr. lokalni disk, eksterni SSD, institucionalni repozitorijum, decentralizovana mreža.
- **Verifikacija integriteta** — Provera da li se sadržaj promenio — pomoću kontrolnih suma (checksum) ili naprednih metoda kao što je blockchain anchoring.
- **Migracija formata** — Prelazak sa zastarelog formata na savremeniji, uz očuvanje sadržaja i metapodataka.

Preporučene strategije

- Odabir formata pogodnih za dugoročno čuvanje
  - Koristiti otvorene formate sa dokumentovanom strukturom i izbegavati vlasničke formate bez garancije kompatibilnosti u budućnosti

    - Dokumenti se čuvaju u više formata: PDF/A za arhivsku stabilnost, TXT za čitljivost, XML za strukturu.
- Izbor repozitorijuma i arhivskih standarda:
    - Kopije se raspoređuju na različite lokacije: lokalni disk, institucionalni server, decentralizovani sistem (npr. IPFS).
    - Objavljivati podatke u repozitorijumima koji podržavaju trajne identifikatore i metapodatke (npr. Zenodo, OpenAIRE)
    - Uskladiti arhiviranje sa nacionalnim i međunarodnim standardima (npr. Uredba o elektronskom arhiviranju)
- Redovna verifikacija integriteta
    - Na svakih 6–12 meseci preporučuje se provera kontrolnih suma (SHA-256, MD5) radi detekcije neovlašćenih promena.
    - Za kritične podatke može se koristiti blockchain anchoring — upisivanje hash vrednosti u javni blokčejn radi trajne potvrde autentičnosti.
- Migracija formata i dokumentacija procesa
    - Prilikom prelaska na novi format, preporučuje se vođenje evidencije o datumu, softveru i metodologiji konverzije.
    - Metapodaci se ažuriraju kako bi se očuvala interoperabilnost i ponovljivost.

💡 *Kratki saveti*

Cilj	Preporučena praksa
Otpornost na tehničko zastarevanje	Višestruki formati (PDF/A, TXT, XML), redovna migracija
Očuvanje dostupnosti	Fizička diverzifikacija lokacija i medija
Provera autentičnosti	Kontrolne sume, blockchain anchoring, evidencija promena
Usklađenost sa propisima	Praćenje zakona o arhivskoj građi, elektronskom dokumentu i zaštiti podataka

🧠 Arhiviranje je most između sadašnjeg istraživača i budućeg tumača — ako je most krhak, znanje ne prelazi.

📘 Dugoročno čuvanje podataka zahteva tehničku preciznost, pravnu usklađenost i mislenu odgovornost. Ono podrazumeva fizičku

diverzifikaciju i različite formate, redovnu verifikaciju integriteta i pažljivo dokumentovanu migraciju. Arhiva nije samo tehnička infrastruktura — ona je misaona garancija trajnosti znanja. U otvorenoj nauci, ona je temelj poverenja koje traje duže od jednog istraživačkog ciklusa.

11. Preporučeni alati i resursi za očuvanje digitalnog integriteta

Za realizaciju principa digitalne diskrecije, etičkog postupanja i dugoročnog čuvanja, akademskom misliocu su potrebni odgovarajući alati. Ovde se ne daje tehničko uputstvo za instalaciju, već pregled alata prema nameni — uz smernice za izbor u skladu sa potrebama i kontekstom primene.

Tabela 4. Tabela preporučenih alata

Kategorija	Alati / Protokoli	Kratko objašnjenje
Upravljanje lozinkama	1Password, Bitwarden	Centralizovani „vault“ za čuvanje lozinki; omogućava deljenje kredencijala sa saradnicima
Disk enkripcija	BitLocker, VeraCrypt	BitLocker je integrisan u Windows; VeraCrypt nudi nezavisnu enkripciju za sve sisteme
Sigurna komunikacija	Signal, ProtonMail, Thunderbird+Enigmail	Signal za glas i tekst; ProtonMail za e-poštu; Enigmail dodatak za PGP u Thunderbirdu
Privatan pretraživač	DuckDuckGo, Startpage, Tor	DuckDuckGo i Startpage blokiraju trackere; Tor omogućava višeslojnu anonimnost
Decentralizovana infrastruktura	Ethereum, IPFS, Hyperledger Fabric	Ethereum za pametne ugovore; IPFS za trajno skladištenje; Hyperledger za privatne mreže
Verifikacija integriteta	SHA-256, MD5, blockchain anchoring	Kontrolne sume za proveru fajlova; blockchain anchoring za trajnu potvrdu autentičnosti
Arhiviranje i repozitorijumi	Zenodo, Figshare, OSF	Repozitorijumi za dugoročno čuvanje i deljenje podataka uz podršku za DOI identifikatore
Anonimizacija metapodataka	ExifTool, Metadata Cleaner	Alati za uklanjanje GPS i ličnih oznaka iz fajlova pre objave
Sigurno pretraživanje fajlova	Cryptomator, Tresorit	Enkriptovane aplikacije za čuvanje i deljenje fajlova sa kontrolom pristupa

Tabela preporučenih alata prikazuje ključna rešenja prema kategoriji, funkciji i misaonoj nameni.

🧠 *Alat nije samo tehničko sredstvo — on je misaona odluka o tome kako se štiti, deli i čuva znanje. Od izbora lozinke do arhiviranja podataka, svaki korak oblikuje digitalni integritet korisnika*.

📘 Ova sekcija je pružila misaono organizovan pregled alata koji podržavaju bezbednost, etiku i dugoročnu dostupnost.

Korisnik može birati rešenja prema sopstvenim potrebama, tehničkom znanju i kontekstu primene — uz svest da svaki alat nosi odgovornost, a ne samo funkciju.

Pregled alata iz ove tačke dobija punu vrednost tek kroz primenu u konkretnim situacijama.

U narednoj sekciji prikazani su sažeti primeri iz prakse — kako se digitalna diskrecija, etičko postupanje i tehnološka rešenja primenjuju u stvarnim istraživačkim kontekstima.

12. Studije slučaja i primeri

U ovoj sekciji prikazujemo konkretne scenarije u kojima se principi digitalne diskrecije, etičkog postupanja i dugoročnog čuvanja primenjuju u praksi. Svaki pregled prati kratak opis slučaja, ključne korake i misaonu refleksiju.

12.1 Zaštita istraživačkog prototipa pred patentiranjem

Istraživačka grupa na Univerzitetu **X** razvila je prototip senzora za ekološki nadzor. Pre podnošenja patenta, morali su da:

- skladište dizajn u šifrovanom repozitorijumu uz kontrolisani pristup
- potpišu višestepene NDA-e (non-disclosure agreements) sa svakim spoljnim partnerom
- koriste verzionisanje (Git+GPG) za praćenje promena bez izlaganja izvornog koda

Zaštita prototipa nije samo pravno pitanje, već i odluka o tome ko i u kojoj meri ima uvid u proces inovacije [16].

🧠 *Inovacija traži poverenje — ali poverenje mora biti tehnički i etički zaštićeno.*

12.2 Sigurni kanali za saradnju sa međunarodnim timom

Tim istraživača iz Srbije, Nemačke i Brazila koordiniše rad na higijenskoj studiji patogena. Da bi zaštitili podatke:

- uspostavili su sopstveni Matrix server uz end-to-end enkripciju
- za fajl-transfer koristili SFTP sa ključevima, uz rotaciju svakih 30 dana
- administratori su kontrolisali pristup kroz dvofaktorsku autentifikaciju (2FA)

Odabir kanala saradnje oblikuje način na koji tim deli poverenje — tehnološki i organizaciono [17].

🧠 *Daljina između istraživača briše se enkripcijom, ali uvek ostaje oprez u rukovanju podacima.*

12.3 Korišćenje blockchain ugovora za peer review proces

U pilot-projektu časopisa **Y**, evaluacija rukopisa sprovođena je putem pametnih ugovora na Ethereum testnet mreži:

- autor postavlja rukopis u šifrovani IPFS direktorijum
- recenzenti dobijaju vremenski ograničene tokene za pristup dokumentu
- nakon završetka vrednovanja, hash izveštaja se usidrio u blokčejn radi trajnog dokaza nepromenljivosti

Transparentnost i anonimnost recenzentskog procesa mogu koegzistirati uz promišljenu primenu decentralizovanih protokola [18].

🧠 Peer review na blokčejnu briše granice između poverenja i dokaza — ali zahteva novi etički kompas.

12.4 Pisanje izveštaja i originalnih naučnih članaka

U timu istraživača koji priprema pregledni rad i originalne članke, proces izgleda ovako:

- **Pretraživanje literature**
  - Napredno pretraživanje u bazama kao što su Scopus i Web of Science
  - Organizacija i deljenje referenci pomoću Zotero ili Mendeley
- **Korišćenje AI za podršku pisanju**
  - Alati poput ChatGPT, Copilot ili SciSpace za sažimanje koncepata i kreiranje nacrta
  - Stroga provera činjenica i referenci pre inkorporacije u tekst
- **Prevođenje i terminološka preciznost**
  - DeepL za konzistentan prevod stručnih termina
  - Ručna provera ključnih izraza kako bi se izbegla semantička odstupanja
- **Jezičko i stilsko uređivanje**
  - Grammarly ili ProWritingAid za gramatičku korekturu i stilsku doslednost
  - Prilagođavanje tona (npr. akademski ili popularno-naučni)
- **Verziona kontrola i saradnja**
  - Overleaf ili Git za praćenje izmena i kolaboraciju uživo
  - Jasna evidencija doprinosa svakog autora i metapodataka

🧠 *Efikasnost AI alata ne sme zaseniti akademsku odgovornost: preciznost termina, tačnost podataka i autentičan glas ostaju u prvom planu* [19].

🧠 *Alat može ubrzati rad, ali ne sme zameniti ljudski sud — svaka rečenica zahteva da je čovek promišljeno preispita*.

13. Pogled unapred: izazovi i trendovi

I dok se osnovni principi digitalne diskrecije i etičkog postupanja već primenjuju, njihov okvir mora biti spreman za nove izazove.

Ovde se ne nude konačni odgovori, već misaona mapa koja akademskom misliocu ukazuje na pojave koje oblikuju digitalnu budućnost.

13.1 Kvantno računanje i post-kvantna enkripcija

Kvantni računari donose mogućnost razbijanja današnjih algoritama enkripcije u razumnim vremenskim okvirima.

Napredne metode poput RSA i ECC gube dugoročnu otpornost, pa to zahteva:

- primenu post-kvantnih algoritama (Kyber, Dilithium – prema preporukama NIST-a)
- reviziju arhiviranih podataka za koje se pretpostavlja trajna enkripcija
- planiranje migracije kriptografskih ključeva i komunikacijskih kanala

Ono što je danas bezbedno, sutra može postati probojno — diskrecija mora biti spremna za tehnološki skok.

13.2 AI-pokriveno praćenje i automatska analiza sadržaja

Napredni AI sistemi sve češće se koriste za:

- klasifikaciju sadržaja bez pristanka autora
- prepoznavanje obrazaca u komunikaciji i formiranje korisničkih profila
- automatizovanu evaluaciju naučnih radova i tekstova

U akademskom kontekstu, to otvara mogućnost da:

- misaoni izrazi budu tumačeni van konteksta
- privatna komunikacija dospe u semantičke algoritme
- AI donosi ocene i procene bez odgovornosti ili obrazloženja

Diskrecija nije samo zaštita sadržaja — već i borba protiv tumačenja bez dozvole.

13.3 Novi modeli decentralizovanog verifikovanja autorstva

Identifikacija autora više se ne oslanja samo na institucionalne naloge. Decentralizovani pristupi nude sledeće mogućnosti:

- korišćenje kriptografskih potpisa putem pametnih ugovora
- verifikacija doprinosa preko NFT-mehanizama u naučnom izdavaštvu
- trajno sidrenje autorstva i rada u blockchain repozitorijume

To omogućava:

- evidenciju doprinosa bez centralizovanih platformi
- otpornost na manipulaciju autorstvom
- transparentno praćenje saradnje među autorima

🧠 Autorstvo više nije samo pitanje imena — već identiteta u mreži poverenja.

📊 *Tabela 5: Novi izazovi i prilike u digitalnoj diskreciji*

Tematski okvir	Rizici	Prilike
Kvantno računanje	Gubitak otpornosti klasične enkripcije (RSA, ECC)	Razvoj post-kvantnih algoritama (Kyber, Dilithium)
AI praćenje i analiza	Profilisanje korisnika, automatizovana interpretacija sadržaja	Brža obrada podataka uz mogućnost etičke kontrole
Decentralizovana verifikacija	Tehnička složenost, moguća zloupotreba pseudonima	Transparentna evidencija doprinosa i autonomna kontrola identiteta

📘 Tehnološki napredak nikada ne dolazi bez etičke cene. Akademski mislilac mora biti spreman da nove alate ne samo koristi — već i razume njihove posledice po poverenje, autorstvo i slobodu izražavanja.

Alat može ubrzati rad, ali ne sme zameniti ljudski sud — svaka rečenica zahteva da je čovek promišljeno preispita.

🧠 14. Zaključak

Digitalna diskrecija kao misaono pravo

Otvorena nauka ne traži da sve bude dostupno — već da ono što se deli bude promišljeno.

U svetu u kojem granice između privatnog i javnog, misaonog i algoritamskog, ličnog i institucionalnog sve češće blede, **diskrecija nije slabost — već oblik misaone snage.**

Ovaj priručnik nije vodič kroz softvere, licencne oznake ili šeme metapodataka — on je poziv da mislimo odgovorno, delimo pažljivo i štitimo ono što čini naš misaoni identitet.

Ne nude se zabrane, već opcije. Ne forsira se strah, već sloboda — ali sa razumevanjem posledica.

Digitalna etika nije samo pitanje tehnologije — već odnos prema znanju koje stvaramo, ljudima sa kojima sarađujemo i svetu kojem to znanje ostavljamo.

Ako postoji jedna poruka koju valja poneti, ona glasi:

> 🧠 *Diskrecija nije zatvaranje. To je misaoni izbor kada, kako i zašto nešto otvaramo.*

Reference

[1] Microsoft, "BitLocker overview," Microsoft, 28 04 2025. [Online]. Available: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/. [Accessed 12 07 2025].

[2] Microsoft, "BitLocker Drive Encryption," Microsoft, 12 08 2024. [Online]. Available: https://support.microsoft.com/en-us/windows/bitlocker-drive-encryption-76b92ac9-1040-48d6-9f5f-d14b3c5fa178. [Accessed 12 07 2025].

[3] Microsoft, "Configure BitLocker," Microsoft, 05 12 2024. [Online]. Available: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/configure?tabs=common. [Accessed 12 07 2025].

[4] Microsoft, "BitLocker operations guide," Microsoft, 05 12 2024. [Online]. Available: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/operations-guide?tabs=powershell. [Accessed 12 07 2025].

[5] Wikipedia, "VeraCrypt," Wikipedia, 30 05 2025. [Online]. Available: https://en.wikipedia.org/wiki/VeraCrypt. [Accessed 12 07 2025].

[6] UMATechnology, "What is VeraCrypt and How to Use it to Encrypt your Secrets," UMATechnology, 25 01 2025. [Online]. Available: https://umatechnology.org/what-is-veracrypt-and-how-to-use-it-to-encrypt-your-secrets/.

[7] "Security Evaluation of VeraCrypt," Fraunhofer Institute for Secure Information Technology, 10 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Veracrypt/Veracrypt.pdf?__blob=publicationFile&v=1. [Accessed 13 07 2025].

[8] H. Kath, "PGP vs. GPG: Key Differences in Encryption," GoAnywhere, 28 03 2019. [Online]. Available: https://www.goanywhere.com/blog/pgp-vs-gpg-whats-the-difference. [Accessed 13 07 2025].

[9] M. Sajid, "Difference between PGP and GPG," Tutorialspoint, 04 04 2023. [Online]. Available: https://www.tutorialspoint.com/difference-between-pgp-and-gpg. [Accessed 13 07 2025].

[10] A. Kothiwal, "Pretty Good Privacy (PGP) and Digital Signatures," Linux Journal, 14 10 2020. [Online]. Available: https://www.linuxjournal.com/content/pretty-good-privacy-pgp-and-digital-signatures. [Accessed 13 07 2025].

[11] UMA Technology, "Encrypt a VHD or VHDX Container file using Bitlocker in Windows," UMA Technology, 6 01 2025. [Online]. Available: https://umatechnology.org/encrypt-a-vhd-or-vhdx-container-file-using-bitlocker-in-windows/. [Accessed 13 07 2025].

[12] T. OfficeBeginner, "How to Remove Metadata from Word Document," OfficeBeginer, 01 02 2023. [Online]. Available: https://officebeginner.com/msword/how-to-remove-metadata-from-word-document/. [Accessed 13 07 2025].

[13] GroupDocs, "Remove Metadata from DOCX," GroupDocs, 13 07 2025. [Online]. Available: https://products.groupdocs.app/metadata/remove-from-docx. [Accessed 13 07 2025].

[14] Pdfcandle, "Remove Word Metadata," Pdfcandle, 2017. [Online]. Available: https://www.pdfcandle.com/word_metadata_remove.aspx. [Accessed 13 07 2025].

[15] Support, "Remove hidden data and personal information by inspecting documents, presentations, or workbooks," Microsoft, 18 04 2025. [Online]. Available: https://support.microsoft.com/en-us/office/remove-hidden-data-and-personal-information-by-

inspecting-documents-presentations-or-workbooks-356b7b5d-77af-44fe-a07f-9aa4d085966f#id0ebd=visio. [Accessed 13 07 2025].

[16] M. Barulli, "IP is a journey: blockchain and encrypted storage are your best friends," *WIPO Magazine, World Intellectual Property Organization,* 2021.

[17] A. Arora, "Bridges across borders: Collaborative strategies for academic and professional success," *Journal of Informatics Education and Research,* vol. 5, no. 2, p. 112–124, 2025.

[18] C. H. Morales-Alarcón, E. Bodero-Poveda, H. M. Villa-Yánez and P. A. Buñay-Guisñan, "Blockchain and Its Application in the Peer Review of Scientific Works: A Systematic Review," *Publications,* vol. 12, no. 4, 2024.

[19] A. Cheng, A. Calhoun and G. Reedy, "Artificial intelligence-assisted academic writing: recommendations for ethical use," *Advances in Simulation,* vol. 10, no. 22, 2025.

📘 O AUTORU

Dr Zoran Čekerevac, redovni profesor i doktor honoris causa, više od pet decenija aktivno učestvuje u razvoju nauke, visokog obrazovanja i istraživačkih praksi u oblasti informacionih tehnologija, akademskog izdavaštva i bezbednosti.

Bio je mentor brojnim doktorandima i masterima, član projekata od nacionalnog i međunarodnog značaja, a njegovo uredničko iskustvo u akademskom časopisu ogleda se u insistiranju na misaonoj preciznosti, profesionalnoj korektnosti i jezičkoj odgovornosti.

Saradnja sa stručnjacima, uključujući i sudske veštake u IT oblasti, doprinela je njegovoj sposobnosti da povezuje tehnološke izazove sa etičkim standardima.

Ovaj priručnik je rezultat njegovog dugogodišnjeg rada — kao mislioca koji razume da znanje nije dovoljno, ako nije sačuvano.

Namerno ostavljeno prazno