УНИВЕРЗИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ“ – БИТОЛА
ПРАВЕН ФАКУЛТЕТ – КИЧЕВО

СТУДИИ ОД ТРЕТ ЦИКЛУС

ПРАВНИ ПРЕДИЗВИЦИ И ОДГОВОРИ НА САЈБЕР ИЗМАМИТЕ ВО КОСОВО

Докторски проект

СТУДЕНТ
Арбер Шала

МЕНТОР
Проф. д-р Ице Илијевски

Кичево, 2025

СОДРЖИНА

ПРАВНИ ПРЕДИЗВИЦИ И ОДГОВОРИ НА САЈБЕР ИЗМАМИТЕ ВО КОСОВО

Арбер Шала

Правен факултет – Кичево, Универзитет „Св. Климент Охридски“ – Битола,

Република Северна Македонија

ORCID iD ()

arberb.shala@gmail.com

Апстракт

Сајбер измамата е широко распространет предизвик во дигиталната ера, кој ги засега поединците, бизнисите и јавните институции ширум светот. Зголемената распространетост на дигиталните трансакции ја зголеми ранливоста, наметнувајќи потреба од робусна законска и институционална рамка. Во Косово, брзата дигитализација откри значителни празнини и во законодавството и во спроведувањето, што резултираше со предизвици за превенција, истрага и гонење.

Овој докторски проект користи пристап со мешани методи, комбинирајќи доктринарна правна анализа со емпириско истражување. Интегрира секундарни податоци од отворен извор, вклучувајќи статистика на Косовската полиција, извештаи од Агенцијата за информации и приватност и европски проценки (ENISA, Европска комисија), со студија на случај на измама со државната каса од 2020 година, во која приближно 2 милиони евра беа нелегално префрлени од државни сметки. Овие привремени наоди илустрираат системски слабости во законските одредби, институционалната координација и техничкиот капацитет.

За да се зајакне базата на докази, истражувањето ќе се потпира на официјални збирки податоци од Централната банка на Косово (ЦБК) во врска со финансиски измами и евиденција на случаи од Општинските судови на Косово во врска со гонењата за сајбер криминал. Оваа емпириска димензија ќе обезбеди единствен увид во трендовите на известување, резултатите од гонењата и судските тесни грла.

Студијата има за цел да идентификува правни недоследности, да го процени институционалниот капацитет и да ги спореди практиките на Косово со стандардите на ЕУ и меѓународните стандарди, особено со Будимпештанската конвенција за сајбер криминал. Со справување со недостатоците во спроведувањето, меѓусекторската соработка и прекуграничната соработка, истражувањето формулира целни препораки за законодавна реформа, институционална специјализација и јавно-приватни партнерства.

Наодите ќе придонесат за правни стипендии за сајбер криминал во новите дигитални јурисдикции и ќе обезбедат практични упатства за креаторите на политики,

судските актери и засегнатите страни во сајбер безбедноста. На крајот, студијата има за цел да ја зајакне отпорноста на Косово на сајбер измами, да го усогласи неговото управување со европските и меѓународните рамки и да ја зголеми јавната доверба во дигиталните системи.

Клучни зборови: сајбер измама, Косово, секундарни податоци, правна рамка, Централна банка на Косово, Општински судови, студија на случај, механизми за спроведување, управување со сајбер безбедноста

1. Вовед

Брзата дигитализација на јавниот и приватниот сектор во Република Косово донесе значителен напредок во комуникацијата, финансиите, управувањето и трговијата. Сепак, овие случувања доведоа и до зголемување на дигиталните ранливости, особено во форма на сајбер измами. Сајбер измамите опфаќаат низа криминални активности, вклучувајќи фишинг, кражба на идентитет, неовластен пристап до дигитални системи и финансиски измами - сите тие претставуваат сериозен ризик за интегритетот на економските системи, довербата на граѓаните во јавните институции и ефикасноста на владеењето на правото (Europol, 2021; ENISA, 2023).

И покрај почетните напори за модернизирање на законските рамки и нивно усогласување со меѓународните стандарди, Косово продолжува да се соочува со структурни ограничувања во борбата против сајбер измамите. Националното законодавство вклучува одредби за сајбер криминал во Кривичниот законик (2019 година), но тие остануваат недоволно операционализирани. Институционалниот капацитет за спречување, истражување и гонење на вакви кривични дела е сè уште недоволно развиен. Недостатокот на специјализирани единици за сајбер криминал, недоволната обука меѓу службениците за спроведување на законот и судиите и ограничената меѓусекторска соработка придонесуваат за неефикасноста на сегашните механизми за одговор (KLI, 2022; GITOC, 2021).

Меѓународните конвенции како што е Будимпештанската конвенција за сајбер криминалот (Совет на Европа, 2001 година) и стратешките директиви од Европската Унија служат како нормативни репери. Сепак, делумната интеграција на Косово во глобалните и регионалните мрежи за сајбер криминал ја ограничува неговата способност целосно да се вклучи во размена на разузнавачки информации и заеднички

операции. Покрај тоа, јавно-приватните партнерства кои се од суштинско значење за откривање и спречување на сајбер измами остануваат во голема мера нерегулирани и неформални (Европска комисија, 2023 година).

Овој докторски проект се справува со овие предизвици преку испитување на адекватноста на правните и институционалните рамки на Косово во справувањето со сајбер измамите. Се стреми да истражи до кој степен националните системи се усогласуваат со меѓународните стандарди и да предложи препораки засновани на докази за правна реформа и институционално зајакнување. Истражувањето се фокусира на идентификување на законски празнини, процедурална неефикасност, ограничувања во спроведувањето и можности за регионална и транснационална соработка.

Притоа, студијата има за цел да придонесе кон правната наука за сајбер криминалот и да ги информира процесите на креирање политики во Косово. Таа ја нагласува потребата од координиран, правно издржан и технолошки адаптивен одговор на сајбер измамите во дигиталното општество кое поминува низ брза трансформација. Се очекува наодите да ја поддржат стратешката цел на Косово за интегрирање во европските и глобалните безбедносни рамки, а воедно да ги заштитат основните права во дигиталната доба.

Претстојна конвенција на ОН. Паралелно со постојните инструменти, Конвенцијата на Обединетите нации против сајбер криминалот, која треба да биде отворена за потпишување на 25-26 октомври 2025 година, претставува голем додаток на глобалниот нормативен пејзаж. Нејзиниот акцент на современите кривични модалитети, процедуралната соработка и градењето капацитети ќе се користат во овој проект како идентична реперна точка заедно со Будимпештанската конвенција и законодавството на ЕУ. Каде што е релевантно, анализата ќе ја процени очекуваната конвергенција и дивергенција помеѓу рамката на Косово и одредбите што се очекува да се кристализираат според овој нов инструмент на ОН.

2. Преглед на литературата

Правниот и институционалниот пејзаж околу сајбер измамите во Косово е обликуван од сложена интеракција на домашното законодавство, меѓународните правни инструменти, институционалните практики и еволуирачките сајбер закани. Литературата открива дека иако се преземени почетни чекори за хармонизирање на рамката на Косово со меѓународните стандарди, остануваат значителни предизвици во правните, институционалните и оперативните димензии.

Во сржта на меѓународната нормативна рамка е Будимпештанската конвенција за сајбер криминал (2001) на Советот на Европа, која служи како главен глобален договор што ги води националните напори за борба против сајбер криминалот. Нејзиното значење лежи во поставувањето хармонизирани стандарди за суштинско и процедурално право за сајбер криминал, меѓународна соработка и прекугранични истраги. Иако Косово ги усвои клучните принципи на Конвенцијата, неговиот делумен статус во меѓународните правни механизми го ограничува целосното учество во размената на разузнавачки информации и координираното спроведување (Совет на Европа, 2001).

На домашен план, Кривичниот законик на Косово (2019) вклучува одредби за неовластен пристап до компјутерски системи, прекршувања на безбедноста на податоците и електронски измами. Сепак, правните научници и аналитичари на политиките го посочија недостатокот на сеопфатно секундарно законодавство и оперативни упатства, што резултира со недоследна примена (KLI, 2022). Емпириските докази истакнуваат значителен јаз помеѓу законските текстови и институционалното спроведување, што ја ослабува ефикасноста на обвинителството.

Институционалните извештаи како што се Проценката на заканите од организираниот криминал на интернет (IOCTA, 2021) и анализите на заканите на ENISA (2023) ја нагласуваат зголемената софистицираност на сајбер измамите, особено во фишингот, рансомверот и финансиските измами. Овие документи ја нагласуваат потребата од посилен технички капацитет, меѓуагенциска соработка и континуирано прилагодување на законските рамки. Институционалните ограничувања на Косово се дополнително документирани од страна на Косовскиот правен институт (2022), кој идентификува недостатоци во обуката на судиите, заостанатите случаи и недостатокот на специјализирани единици за сајбер криминал.

Од компаративна перспектива, програмскиот документ на Европол (2021–2023) и извештаите на Европската комисија служат како критични репери за усогласување на косовските системи со најдобрите практики на ЕУ. Овие извори ја нагласуваат потребата од соработка меѓу повеќе засегнати страни, интегрирани системи за податоци и јавно-приватни партнерства - елементи кои остануваат недоволно развиени во Косово. Извештајот на GITOC (2021) се продлабочува на овие точки, дискутирајќи како транснационалниот организиран криминал ја експлоатира институционалната фрагментација и ограничената регионална координација.

Дополнително, UNODC (2021) и други глобални стратешки актери повикуваат на поширока меѓународна соработка, зајакната соработка меѓу обвинителите и договори за меѓусебна правна помош, области каде што Косово се соочува со правни и политички пречки поради неговиот меѓународен статус.

При синтетизирање на овие придонеси, станува очигледно дека управувањето со сајбер измамите во Косово страда од три меѓусебно поврзани недостатоци: (1) недоволна правна хармонизација со меѓународните стандарди; (2) слаб институционален капацитет за спроведување; и (3) ограничено учество во регионалните и глобалните работни групи за сајбер криминал. Иако неодамнешните законски реформи ветуваат, сè уште недостасува сеопфатен и координиран одговор. Затоа, овој преглед на литературата го утврдува критичниот контекст и истражувачкиот јаз што овој докторски проект се стреми да го реши преку доктринарна, емпириска и компаративна правна анализа.

2.1. Меѓународни правни рамки за сајбер криминалот

Сајбер криминалот, вклучувајќи ги и сајбер измамите, е регулиран со растечки корпус на меѓународни правни инструменти насочени кон поттикнување на хармонизирани пристапи низ јурисдикциите. На чело е Будимпештанската конвенција за сајбер криминал (2001) на Советот на Европа, која служи како основен договор за справување со кривични дела против компјутерските системи и електронските податоци, како и за олеснување на прекуграничната соработка. Конвенцијата го промовира усогласувањето на домашното законодавство со заедничките стандарди за дефиниции, процедурални алатки (на пр., забрзано зачувување на податоци) и механизми за меѓусебна правна помош. Иако Косово ги вклучи основните принципи на Будимпештанската конвенција во својата домашна правна рамка, неговото ограничено признавање како потписник, поради неговиот политички статус, продолжува да го ограничува формалното учество во глобалните мрежи за спроведување и заедничките операции (Совет на Европа, 2001).

Нова рамка на ОН. Како дополнување на стандардите на Советот на Европа, Конвенцијата на Обединетите нации против сајбер криминалот, која ќе биде отворена за потпишување на 25-26 октомври 2025 година, е дизајнирана да ги одрази најновите трендови во сајбер криминалот, вклучувајќи типологии на измами, електронски докази и меѓународна соработка. Иако е нов инструмент, се очекува неговиот договорен текст да даде приоритет на практичната меѓусебна правна помош, забрзаното зачувување/производство на податоци и механизмите за градење капацитети. Затоа,

овој докторски проект ќе се повика на Конвенцијата на ОН како непосредна глобална основа при формулирање препораки за усогласување на законодавството и практиките за соработка на Косово.

Дополнителните придонеси од UNODC (2021) и GCTF (2021) ја нагласуваат потребата од интегрирање на стратегиите за сајбер криминал во пошироките напори за борба против организираниот криминал. Овие извори истакнуваат како транснационалните мрежи ги искористуваат дигиталните системи низ слабите јурисдикции и ја нагласуваат важноста на градењето капацитети, законодавната кохерентност и меѓународната размена на разузнавачки информации.

2.2. Национален правен и институционален контекст во Косово

Косово започна законодавни напори за справување со сајбер измамите, првенствено преку одредби во Кривичниот законик (2019), кои го криминализираат незаконскиот пристап, мешањето во податоците, мешањето во системот и разните форми на електронска измама. Сепак, анализата од Косовскиот правен институт (2022) покажува дека правната рамка страда од недостаток на упатства за имплементација, институционална фрагментација и застарени дефиниции кои не ја земаат предвид еволутивната природа на дигиталните закани.

Спроведувањето на законите за сајбер измами останува недоследно. Судството е недоволно опремено за справување со сложени дигитални докази, а агенциите за спроведување на законот честопати немаат обука и алатки потребни за ефикасна истрага на сајбер криминал. Понатаму, Косово сè уште нема формирано целосно функционални специјализирани единици за сајбер криминал, празнина што ја нарушува неговата способност проактивно да реагира на новите закани. Извештаите сугерираат дека и покрај присуството на формални законски механизми, спроведувањето останува во голема мера реактивно и фрагментирано (KLI, 2022).

2.3. Регионални и ЕУ практики во борбата против сајбер измамите

Спротивно на тоа, земјите-членки на ЕУ работат во рамките на посилна архитектура за управување со сајбер криминалот, поддржана од институции како што се Европол, Евроџаст и Агенцијата на Европската унија за сајбер безбедност (ENISA). Програмскиот документ на Европол (2021–2023) и Проценката на заканите од интернет организиран криминал (IOCTA, 2021) ги опишуваат сеопфатните стратегии што вклучуваат рано откривање, прекугранична соработка и распоредување платформи за разузнавање за закани. Овие документи, исто така, го истакнуваат растечкото

вклучување на недржавни актери, употребата на криптовалути во сајбер измамите и зголемената потреба од техники за спроведување базирани на податоци.

Извештаите на Европската комисија за напредокот на Косово (2021–2023) даваат редовни проценки за усогласеноста со стандардите на ЕУ во правдата и внатрешните работи. Иако признаваат одреден напредок во дигиталното управување, овие извештаи постојано ја нагласуваат потребата на Косово да изгради институционален капацитет, да обезбеди судска независност во сајбер-гонските гонења и да ги унапреди напорите за правна хармонизација (Европска комисија, 2023).

Релевантни директиви на ЕУ. Надвор од институционалните рамки како што се Европол, Евроџаст и ENISA, Европската Унија кодифицираше неколку обврзувачки инструменти кои директно ги обликуваат националните одговори на сајбер измамите. Директивата 2013/40/ЕУ за напади врз информациски системи утврдува кривични дела и процедурални обврски поврзани со хакирање, мешање во податоци и измама. Општата регулатива за заштита на податоци (GDPR, Регулатива (ЕУ) 2016/679) ја подобрува заштитата на личните податоци, клучен елемент во борбата против измамите поврзани со идентитетот. Директивата NIS (2016/1148/ЕУ), неодамна ажурирана преку NIS2 (Директива (ЕУ) 2022/2555), наметнува обврски за безбедност и известување за инциденти на операторите на основни услуги и давателите на дигитални услуги. Дополнително, ревидираната Директива за платежни услуги (PSD2, Директива (ЕУ) 2015/2366) воведува силни правила за автентикација на клиентите и одговорност кои ги ублажуваат измамите во плаќањето. Заедно, овие директиви обезбедуваат сеопфатно acquis кое Косово мора да го приближи за да ја зајакне својата отпорност против сајбер финансискиот криминал и да ја унапреди својата агенда за интеграција во ЕУ.

2.4. Оперативни предизвици и институционални празнини

Литературата постојано укажува на несовпаѓање помеѓу формалните законски одредби и оперативните реалности во Косово. Случаите на сајбер измами често се недоволно пријавуваат, или поради недостаток на доверба од страна на жртвите во властите или поради ниска свест за ризиците. Отсуството на централизиран механизам за пријавување и недостатокот на обучени сајбер истражители го усложнуваат проблемот. Анализата на случаи од GITOC (2021) и регионалните брифинзи за политики потврдуваат дека судските одложувања, тешкотиите во зачувувањето на дигиталните докази и бирократската неефикасност дополнително ги ослабуваат можностите за спроведување.

Покрај тоа, агенциите за спроведување на законот работат со застарена технолошка инфраструктура, што ја ограничува нивната способност за следење, анализа или реагирање на сајбер закани во реално време. Компаративните студии со системите на ЕУ покажуваат дека на Косово му недостасуваат меѓуагенциски протоколи за споделување податоци и стандардизација на сајбер безбедноста во јавните институции (GITOC, 2021; KLI, 2022).

2.5. Улогата на јавно-приватни партнерства и меѓународна соработка

Сè повеќе нагласувана област во литературата е улогата на јавно-приватни партнерства (ЈПП) во откривањето и спречувањето на сајбер измами. Според ENISA (2023) и Европол (2021), партнерствата меѓу органите за спроведување на законот, финансиските институции, телекомуникациските даватели на услуги и фирмите за сајбер безбедност се од клучно значење за успехот на националните стратегии за сајбер криминал. Сепак, на Косово му недостасува правна и регулаторна рамка што овозможува структурирани ЈПП. Поголемиот дел од соработката е неформална, со ограничена размена на податоци и без обврзувачки безбедносни протоколи.

Покрај тоа, исклучувањето на Косово од полноправно членство во клучните меѓународни организации за сајбер безбедност ја ограничува неговата способност да учествува во координирани одговори на прекугранични закани. Платформи за регионална соработка и билатерални договори со земјите-членки на ЕУ постојат, но се недоволно искористени поради ограничувања на капацитетите и политички размислувања. Литературата се залага за зголемено учество на Косово во европските механизми како што се ENISA, сајбер единиците на ИНТЕРПОЛ и мрежата G7 24/7 за да се обезбедат капацитети за брз одговор.

2.6. Идентификувани празнини и придонес во истражувањето

Литературата за сајбер измамите во Косово открива три меѓусебно поврзани празнини кои сè уште не се доволно адресирани од постојната научна и институционална пракса:

1. **Нормативна неусогласеност:** Иако Косово делумно ги интегрираше принципите на Будимпештанската конвенција во својот Кривичен законик (2019 година), законските одредби остануваат генерализирани и фрагментирани, без детални процедурални стандарди за зачувување на докази, јасност на јурисдикцијата и типологии на финансиски измами.
2. **Слабости во институционалното спроведување:** Студиите од Косовскиот правен институт (2022) и извештаите за напредокот на ЕУ (2023) нагласуваат

ограничена судска специјализација, недоволни технички ресурси и отсуство на специјализирани единици за сајбер криминал. Овие недостатоци создаваат системски одложувања и ја поткопуваат ефикасноста на обвинителството.

3. **Недоволно развиени механизми за соработка:** И покрај меѓународното признавање на важноста на јавно-приватните партнерства и прекуграничната соработка, рамките на Косово за структурирана соработка со банки, телекомуникациски даватели на услуги и регионални агенции за спроведување на законите остануваат неформални и ad hoc.

2.7. Истражувачки придонес

Ова докторско истражување ги опфаќа горенаведените празнини нудејќи анализа заснована на докази и мултидимензионална анализа за управувањето со сајбер измами во Косово. Нејзините придонеси се тројни:

- Доктринарен/правен придонес: Студијата обезбедува систематско мапирање на косовското законодавство за сајбер криминал во однос на меѓународните стандарди, идентификувајќи ги областите каде што се итно потребни законски усогласувања и процедурална јасност.
- Емпириски придонес: Со интегрирање на секундарни податоци од отворен извор (на пр., полициска статистика, жалби за заштита на податоци, случаи на измами во државната каса) со претстојните официјални збирки податоци од Централната банка на Косово (ЦБК) и Општинските судови, истражувањето создава единствена сеопфатна слика за инциденцата на сајбер измами, моделите на гонење и ефикасноста на судството.
- Политички/практичен придонес: Проектот формулира конкретни препораки за реформи за законодавците, агенциите за спроведување на законите и креаторите на политики, вклучувајќи ја институционализацијата на јавно-приватни партнерства, воспоставувањето специјализирани единици за сајбер криминал и зајакнувањето на прекуграничната соработка.

3. Проблем на истражување

Сајбер измамите во Косово претставуваат брзорастечка закана за дигиталната доверба, правниот интегритет и економската безбедност. Иако постојат законски одредби во Кривичниот законик и во придружното законодавство, капацитетот на државата да истражува и гони сајбер измами е ограничен. Постои јаз помеѓу формалната законска рамка и нејзината оперативна ефикасност. Судските процеси

остануваат бавни, собирањето докази е технички ограничено, а меѓуагенциската координација е фрагментирана. Дополнително, ограничената интеграција на Косово во меѓународните рамки за спроведување на сајбер криминалот ги поткопува напорите за борба против прекуграничните закани. Недостатокот на јавна свест и недоволното пријавување дополнително го замаглуваат вистинскиот обем на проблемот.

Ова докторско истражување е дизајнирано критички да ги испита правните и институционалните недостатоци во тековните механизми за одговор на Косово и да ја процени нивната компатибилност со меѓународните стандарди, особено оние што произлегуваат од Советот на Европа и Европската Унија. Проектот има за цел да утврди кои реформи, и нормативни и процедурални, се потребни за да се подобри отпорноста на Косово на сајбер измами.

4. Хипотеза и цели

Овој дел ја дефинира водечката хипотеза и основните цели на докторскиот истражувачки проект. Врз основа на поширокаата цел за придонес на оригинално знаење во правната регулатива на сајбер криминалот, студијата е структурирана околу централен истражувачки предлог во врска со адекватноста на правниот и институционалниот одговор на Косово на сајбер измамите. Хипотезата е формулирана преку критичко испитување на постојното законодавство, практиките за спроведување и меѓународните стандарди. Целите дефинирани овде го воспоставуваат аналитичкиот опсег на проектот и ја одразуваат неговата посветеност на доктринарна анализа, институционална евалуација и компаративно правно истражување. Овие компоненти заедно ја формираат концептуалната рамка преку која докторскиот проект се стреми да го унапреди научното разбирање и да предложи нормативни и процедурални реформи.

4.1. Хипотеза

Правната и институционалната рамка во Република Косово не е соодветно опремена за ефикасно спречување, откривање и гонење на сајбер измами и бара суштински реформи во согласност со меѓународните правни и политички рамки.

4.2. Цели на истражувањето:

Да се анализира нормативната рамка што ги регулира сајбер измамите во Косово.

Да се идентификуваат празнините во спроведувањето, институционалната координација и процедуралната правда.

Да се споредат правните практики на Косово со оние на избрани земји-членки на ЕУ.

Да се оцени ангажманот на Косово со меѓународните конвенции и работните групи за сајбер криминал.

Да се предложат правни и институционални реформи врз основа на идентификуваните најдобри практики.

5. Научен придонес на истражувањето

Ова докторско истражување придонесува за правната наука преку решавање на недоволно истражената врска помеѓу дигиталниот криминал и институционалната подготвеност во постконфликтен и транзициски контекст. Неговиот примарен научен придонес лежи во понудата на сеопфатна правна и политичка анализа на управувањето со сајбер измамите во Косово, позиционирана во рамките на поширокаta европска правна средина. Студијата генерира нови знаења за ефикасноста на правните норми, процедуралните заштитни мерки и практиките за спроведување во еден дигитален правен систем во развој. Исто така, дава практични придонеси преку формулирање на практични препораки за политики и законодавни измени, со што се премостува јазот помеѓу академските истражувања и правната реформа.

Нудејќи правна анализа заснована на докази и чувствителна на контекстот, истражувањето го подобрува академското разбирање на регулирањето на сајбер криминалот и го поддржува развојот на посилни правни и институционални одговори. Неговите наоди можат да послужат како основа за законодавна реформа, програми за обука на судии и стратешко планирање за регионална соработка во областа на сајбер криминалот.

6. Методи и материјали

Ова докторско истражување користи мешана правна методологија, комбинирајќи доктринарна анализа со емпириско истражување и компаративна проценка. За да се обезбеди концептуална јасност, методите се разликуваат помеѓу канцелариско истражување (анализа на текстови и секундарни материјали) и примарни емпириски извори (податоци собрани директно од институции и засегнати страни).

6.1. Деск истражување (доктринална и анализа на содржина)

Деск истражувањето ја сочинува основата на студијата. Тоа вклучува:

- Доктринарна/правна анализа на домашните закони (Кривичен законик на Косово, закон за заштита на податоци, закон за електронски комуникации), стратегии и подзаконски акти.
- Меѓународни и регионални инструменти, како што се Конвенцијата од Будимпешта, релевантните директиви на ЕУ (2013/40/EU, GDPR, NIS/NIS2, PSD2) и претстојната Конвенција на ОН против сајбер криминалот.
- Анализа на содржината на институционалните извештаи (на пр., слики на закани на ENISA, Европол IOCTA, извештаи за напредокот на Европската комисија, студии за следење на Косовскиот правен институт).
- Академска литература за сајбер криминалот, типологии на измами и практики на управување. Оваа фаза ја утврдува нормативната и концептуалната основа според која се оценува рамката на Косово.

6.2. Примарни правни извори

- Домашно право и политика: Кривичен законик на Република Косово, секторско законодавство (на пр., електронски комуникации, заштита на податоци), национални стратегии за сајбер безбедност и подзаконски акти за имплементација.
- Меѓународни инструменти: Конвенција од Будимпешта на Советот на Европа (ETS бр. 185) и поврзани директиви и рамки на политики на ЕУ (кои се користат како нормативни репери).

6.3. Секундарни институционални податоци

За да ги поткрепи тврдењата со квантитативни докази, проектот се потпира на секундарни податоци што веќе се собрани и објавени од надлежни институции. Клучните извори вклучуваат:

- Годишни извештаи и статистика на Косовската полиција за сајбер криминал (на пр., во 2023 година, полицијата евидентираше 40 случаи на сајбер криминал, уапси 29 осомничени и поднесе 37 кривични пријави против 68 осомничени).
- Метрики на Агенцијата за информации и приватност (AIP) за жалби за заштита на податоци (на пр., околу 400 жалби во последните три години, што укажува на системска изложеност на дигитални права и прекршувања на приватноста).
- Секторски/сајбер безбедносни проценки од реномирани организации (ENISA, Европол, документација за напредокот на ЕУ, национални стратешки документи) за контекстуализирање на институционалниот капацитет и трендови.

- Комуникации од финансискиот сектор од Централната банка на Република Косово (CBK) - вообичаено позната како „Косовска национална банка“ - за сајбер инциденти, координација на секторот и градење на надзорни капацитети.

Посветеност на официјални бази на податоци: Емпириското јадро на ова истражување систематски ќе добие и анализира (а) агрегатна статистика за измами/сајбер инциденти од ЦБК (платежни измами, неовластени трансакции, извештаи за инциденти) и (б) административни евиденции за случаи од општинските судови на Косово (поднесоци, правни класификации, исходи, траење) за да се потврдат и прошират наодите од отворен код.

6.4. Материјали за студијата на случај

Фокусирана студија на случај ќе ја испита кражбата од ~2 милиони евра од државната каса на Косово во 2020 година, инцидент кој е широко цитиран како разоткривање на акутни слабости во управувањето и контролата во дигиталните финансиски процеси. Студијата ќе ги триангуларизира медиумските истраги, институционалните изјави и (под услов да има пристап) обвинителските/судските досиеја. Забележете дека прецизната класификација на инцидентот (сајбер напад наспроти измама/социјален инженеринг/злоупотреба од внатре) е оспорена; самата оваа двосмисленост е аналитички вредна за проценка на законските дефиниции, стандардите за докази и меѓуагенциската координација.

6.5. План за собирање (примарни податоци)

- ЦБК (Народна банка на Косово): Барање податоци од временски серии за обиди и успешни инциденти со измами во плаќањата, вредност под ризик, стапки на наплата и типологии на инциденти пријавени од страна на надгледуваните субјекти; дополнување со надзорни циркулари и известувања за сајбер инциденти.
- Општински судови: Барање регистри за сајбер измами и сродни прекршоци (на пр., неовластен пристап, кражба на идентитет, фишинг, електронска измама), вклучувајќи поднесоци, обвинења, осуди, казни и времетраење на случаите.

Доколку е потребно, барањата ќе се потпираат на важечките одредби за пристап до информации и јавните збирки на податоци на судските статистички служби. Ќе се применува агрегација и анонимизација за да се обезбеди усогласеност со законот за заштита на податоците.

6.6. Техники на анализа

- Доктринарно мапирање на законските одредби во однос на Будимпештанската конвенција и законодавството на ЕУ.
- Описна и трендовска анализа на секундарните статистики (на пр., годишен обем на работа, сооднос на обвинителство/осудување).
- Следење на содржината и процесот во студијата на случај за да се идентификуваат процедуралните тесни грла и проблемите со ракувањето со докази.
- Споредбено споредување со избрани јурисдикции на ЕУ за да се откријат изводливи реформи.

6.7. Етика, валидност и ограничувања

Проектот се придржува до нормите за истражувачка етика, вклучувајќи доверливост и одговорно ракување со административни податоци. Триангулацијата, низ правни текстови, институционална статистика и студија на случај, ќе ја ублажи пристрасноста од еден извор. Ограничувањата вклучуваат потенцијални празнини во стандардизираното известување низ институциите и еволуирачките класификации на сајбер измами, кои ќе бидат експлицитно документирани и адресирани во анализи на чувствителност.

7. Методологија на истражување

Ова истражување користи избалансиран пристап со мешани методи, комбинирајќи една квалитативна и една квантитативна техника. Ова обезбедува методолошка кохерентност и избегнува дисперзија низ премногу алатки. Квалитативната димензија (полуструктурирани интервјуа со експерти) обезбедува контекст и длабочина, додека квантитативната димензија (анализа на официјалните збирки податоци на ЦБК и Општинските судови) дава статистички докази. Квалитативните наоди ќе послужат за пополнување на интерпретативните празнини што се јавуваат кога секундарните статистики се нецелосни или кога официјалните податоци не ја доловуваат целосно динамиката на сајбер измамите.

7.1. Квалитативна компонента

Квалитативната компонента се базира на полуструктурирани интервјуа со одбрани правни експерти, креатори на политики, службеници за спроведување на законот и претставници на финансиски институции. Целното земање примероци обезбедува учество на лица со специјализирано знаење. Овие интервјуа ќе генерираат увид во тоа како функционираат законските рамки во пракса, институционалните

предизвици во гонењето на сајбер измамите и перспективите за усогласувањето на Косово со нормите на ЕУ и меѓународните норми. Овие квалитативни докази ќе ја надополнат статистичката анализа со решавање на прашањата што се недоволно пријавени или не се опфатени во официјалните збирки податоци.

7.2. Квантитативна компонента

Квантитативната компонента се потпира на официјални збирки податоци добиени од Централната банка на Косово (ЦБК) и Општинските судови. Клучните индикатори вклучуваат број и вид на случаи на сајбер измами, исходи од гонење, стапки на осудување, времетраење на случаите и вклучени финансиски вредности. За да се процени институционалниот капацитет и ефикасноста на постапките, ќе се примени описна статистика и анализа на трендови. Овие квантитативни наоди ја обезбедуваат емпириската основа на студијата.

7.3. Вклучување на засегнатите страни и студии на случај

Студиите на случај и консултациите со засегнатите страни се користат во поддршка, збогатувајќи ја анализата со илустративни детали и потврдувајќи ги шемите идентификувани преку главните методи. Истражувањето ќе вклучува избрани студии на случај на инциденти на сајбер измами во Косово, избрани да претставуваат и типични и исклучителни сценарија за спроведување. Тие ќе дадат увид во судското расудување, обвинителските стратегии и институционалната соработка. Анализата на студиите на случај ќе ги истакне повторливите правни и процедурални пречки, како и примерните практики што можат да ги информираат идните реформи.

Вклучувањето на засегнатите страни ќе биде олеснето и преку експертски консултации и анализа на иницијативите за јавно-приватно партнерство (ЈПП) насочени кон спречување и ублажување на сајбер измамите. Студијата ќе ја истражи улогата на финансиските институции, телекомуникациските фирми и давателите на услуги за сајбер безбедност во поддршката на националните напори за борба против дигиталниот криминал.

7.4. Меѓународна соработка и проценка на усогласеноста

Со оглед на инхерентно транснационалниот карактер на сајбер измамите, оваа студија ќе го оцени учеството на Косово во меѓународните мрежи за спроведување на законот, како што се ИНТЕРПОЛ, ЕВРОПОЛ и платформата SIRIUS. Ќе се процени ефикасноста на процедурите за екстрадиција, заедничките истраги и размената на информации во реално време.

Покрај тоа, истражувањето ќе ја испита усогласеноста на Косово со меѓународните стандарди за сајбер безбедност, вклучувајќи ја Општата регулатива за заштита на податоци (GDPR) на Европската Унија и Директивата за напади врз информациски системи (2013/40/EU). Ќе се идентификуваат правни празнини и недостатоци во усогласеноста за да се формулираат препораки за подобрување на меѓународниот кредибилитет и функционалниот капацитет на Косово во спречувањето на дигиталниот криминал.

Со примена на оваа сеопфатна методолошка рамка, спојувајќи квалитативно правно истражување, квантитативна анализа, вклучување на засегнатите страни и компаративни студии на случаи, истражувањето има за цел да генерира увиди засновани на докази што придонесуваат за развој на политики, институционално зајакнување и законска реформа во борбата против сајбер измамите во Косово.

Позиционирање vis-à-vis Конвенцијата на ОН. Покрај споредувањето со Конвенцијата од Будимпешта, GDPR и сајбер инструментите на ЕУ, студијата ќе го разгледа потенцијалното усогласување на Косово со претстојната Конвенција на ООН против сајбер криминалот (отворена за потпишување 25-26 октомври 2025 година). Проценката на усогласеност ќе ги идентификува областите каде што Косово може проактивно да ги хармонизира домашните процедури и алатките за соработка со оваа рамка на ООН за да се олесни споделувањето докази, заедничките истраги и градењето капацитети со поширок круг меѓународни партнери.

8. Резултати и дискусија

Овој дел ги синтетизира достапните наоди од отворен код за сајбер измами во Косово, идентификува шеми и институционални одговори и интегрира студија на случај на инцидент со висок профил. Служи како привремена база на докази, додека целосната валидација ќе се постигне преку статистички податоци од Централната банка на Косово (ЦБК) и Општинските судови.

8.1. Трендови и модели на сајбер измами во Косово

Секундарните податоци укажуваат на постојан пораст на инцидентите со сајбер измами во текот на изминатата деценија. Според Годишниот извештај на косовската полиција (2023), органите за спроведување на законот регистрирале 40 случаи на сајбер криминал во текот на годината, поднеле 37 кривични пријави против 68 осомничени и обезбедиле 29 апсења. Иако сајбер криминалот останува недоволно пријавен, овие

бројки ја илустрираат и растечката распространетост на сајбер измамите и растечкиот одговор на обвинителството.

Дополнителните докази од Косовската агенција за информации и приватност (AIP) ги потврдуваат системските ранливости во дигиталните права и заштитата на податоците. Помеѓу 2021 и 2023 година, AIP регистрираше приближно 400 жалби за прекршување на податоците и приватноста. Ова ниво на изложеност ја истакнува нејасната линија помеѓу сајбер измамите, злоупотребата на идентитетот и пошироките неуспеси во безбедноста на податоците.

Регионалните и проценките на ЕУ ги потврдуваат овие наоди. Извештајот за напредокот на Европската комисија за Косово за 2023 година ги нагласи постојаните слабости во капацитетот за спроведување на сајбер криминалот, меѓуагенциската координација и обуката на судството. Слично на тоа, Извештајот за состојбата на заканите на ENISA за 2023 година предупредува на зголемена софистицираност во механизмите за измама, особено фишингот и шемите за рансомвер.

8.2. Правни и институционални празнини

И покрај постоењето на одредби за сајбер криминал во Кривичниот законик од 2019 година, институционалното спроведување останува фрагментирано. Косовскиот правен институт (2022) го истакна отсуството на специјализирани единици за сајбер криминал, ограничената судска експертиза во ракувањето со дигитални докази и процедуралните одложувања што го попречуваат ефикасното гонење.

Споредбеното споредување открива дека одговорот на Косово е послаб од колегите од ЕУ. На пример, додека земјите-членки на ЕУ имаат корист од размена на разузнавачки информации во реално време преку Европол и платформата SIRIUS, делумната интеграција на Косово го спречува целосното учество во прекугранични истраги.

8.3. Предизвици во спроведувањето и судска неефикасност

Интервјуата и отворените извештаи се спојуваат околу постојаните предизвици за спроведување:

- Ниската јавна доверба во институциите ги обесхрабрува жртвите да пријавуваат измама.
- Ракувањето со дигитални докази останува недоволно развиено, со чести процедурални грешки што доведуваат до отфрлање на случаите.
- Заостанатите случаи во општинските судови ги одложуваат постапките, ослабувајќи го одвраќањето.

Овие предизвици придонесуваат за циклус каде што сајбер измамите честопати остануваат неказнети, зајакнувајќи ја неказнивоста.

8.4. Студија на случај: Измамата со Министерството за финансии во 2020 година

Еден истакнат случај ја илустрира ранливоста на Косово на сајбер измами. Во 2020 година, хакерите се инфилтрираа во системите на државната каса на Косово и извршија лажни трансфери во износ од приближно 2 милиони евра.

Истражувачкото новинарство и анализите на меѓународната политика идентификуваа неколку системски слабости:

- Слаби внатрешни контроли во дигиталните системи за плаќање.
- Доцнење во откривањето, при што сомнителните трансфери првично ги заобиколуваат системите за рано предупредување.
- Нејасна правна класификација, бидејќи властите дебатираа дали инцидентот претставува сајбер напад, внатрешна измама или хибриден криминал.

Случајот со измама во Министерството за финансии останува пресвртница во наративот за дигитална безбедност на Косово. Тој откри не само технички слабости, туку и потреба од прецизни законски дефиниции, подобро обучени истражители и посилна меѓуагенциска координација. Исто така, ја откри важноста на соработката со банкарскиот сектор, зајакнувајќи ја релевантноста на надзорот на ЦБК во спречувањето на измами.

8.5. Улогата на јавно-приватните партнерства

Новите докази покажуваат ограничени, но позитивни ефекти од ad hoc соработката помеѓу органите за спроведување на законот и финансиските институции. Изолираните партнерства го подобрија откривањето на измами и ги зајакнаа механизмите за рано предупредување. Сепак, во отсуство на формална правна рамка за структурирана размена на информации, овие иницијативи остануваат фрагментирани.

8.6. Меѓународна соработка и усогласеност

Ограниченото членство на Косово во глобалните организации за сајбер безбедност го ограничува неговиот капацитет за соработка во реално време. Иако делумно се усогласи со принципите на Будимпештанската конвенција, на Косово му недостасува меѓународно признание потребно за целосно пристапување. Ова го ограничува пристапот до специјализираните канали за сајбер криминал на ИНТЕРПОЛ и заедничките операции на ЕВРОПОЛ.

Сепак, билатералните партнерства и регионалните иницијативи (на пр., со Северна Македонија и Албанија) покажуваат растечки потенцијал за прекугранична координација. Идните реформи мора да ги искористат овие можности.

9. Очекувани резултати и заклучок

9.1. Очекувани резултати

Се очекува ова докторско истражување да генерира сеопфатно разбирање на правните и институционалните одговори на Косово на сајбер измамите преку комбинирање на доктринарна анализа, секундарни податоци и истражување на студии на случај. Очекуваните резултати вклучуваат:

- Идентификација на правни празнини: Студијата ќе потврди дека законодавната рамка на Косово, иако формално е усогласена со аспектите на Конвенцијата од Будимпешта, нема детални одредби за сајбер овозможени финансиски измами, безбедно ракување со докази и структурирана јавно-приватна соработка.
- Проценка на институционалниот капацитет: Врз основа на докази од отворен извор и претстојни збирки податоци од Централната банка на Косово (ЦБК) и Општинските судови, истражувањето предвидува откривање на критични слабости во меѓуагенциската координација, судската специјализација и техничката подготвеност.
- Емпириски придонес: Секундарните податоци веќе укажуваат на зголемување на трендовите на сајбер криминал - 40 случаи регистрирани во полицијата во 2023 година, околу 400 жалби за приватност помеѓу 2021-2023 година и случајот со измама во државната каса од 2 милиони евра. Понатамошни емпириски сознанија од ЦБК и судските евиденции ќе обезбедат авторитативна база на докази за моделите на гонење, стапките на осудување и системските тесни грла.
- Споредбено споредување: Истражувањето ќе ја истакне дивергенцијата помеѓу практиките за спроведување на законите на Косово и моделите на ЕУ за управување со сајбер криминалот. Лекциите од EUROPOL, ENISA и одбрани земји-членки ќе послужат како планови за правните и институционалните реформи на Косово.
- Препораки за политиката: Ќе се развијат предлози за акција за:

  - Усогласување на законодавството со Конвенцијата од Будимпешта и директивите на ЕУ.

- Воспоставување на специјализирани единици за сајбер криминал во спроведувањето на законот и судството.
- Институционализирани јавно-приватни партнерства за спречување на измами.
- Зајакнување на учеството на Косово во регионалните и меѓународните работни групи за сајбер криминал.

- Подготвеност за Конвенцијата на ОН: Мапирање на приоритетни измени и институционални практики што би го позиционирале Косово за брзо усогласување со претстојната Конвенција на ОН против сајбер криминал (отворена за потпишување 25-26 октомври 2025 година), обезбедувајќи кохерентност со практиките со седиште во Будимпешта и законодавството на ЕУ.

9.2. Заклучок

Наодите од ова докторско истражување покажуваат дека сегашната законска и институционална рамка на Косово останува недоволна за справување со сложеноста и обемот на сајбер измамите. Иако постојат нормативни одредби, нивната ефикасност е поткопана од слабата имплементација, фрагментираниот институционален капацитет и нецелосната интеграција во меѓународните мрежи за соработка.

Студијата на случајот за измамата со Министерството за финансии во 2020 година ги нагласува и материјалните ризици што ги претставуваат финансиските злосторства овозможени преку сајбер технологија и итна потреба од робусни законски дефиниции, посилни превентивни механизми и подобрени практики за ракување со докази.

Со интегрирање на доктринарна анализа со секундарни податоци и емпириска валидација преку евиденцијата на ЦБК и Општинските судови, ова истражување ќе го обезбеди првиот сеопфатен приказ за управувањето со сајбер измамите во Косово, базиран на докази. Ќе обезбеди и теоретски придонеси за правни стипендии и практични препораки за креаторите на политики и практичарите.

Конечно, со поставување на реформскиот пат на Косово во рамките на воспоставената рамка од Будимпешта и претстојната Конвенција на ОН против сајбер криминал (25-26 октомври 2025 година), проектот нагласува практичен пат за осовременување на домашното право и модалитетите за соработка. Раното усогласување со инструментот на ОН би го зголемило кредибилитетот на Косово, би ги проширило каналите за меѓусебна правна помош и би ја зајакнало отпорноста на истрагите за сајбер измами.

На крајот, студијата има за цел да го позиционира правниот систем на Косово на траекторија кон поголема отпорност, транспарентност и усогласеност со европските и меѓународните стандарди, со што ќе се зајакне јавната доверба во дигиталното управување и ќе се зајакнат аспирациите на Косово за европска интеграција.

10. Признанија

Ова докторско истражување не би било можно без непроценливата поддршка и водство од бројни поединци и институции. Прво и најважно, изразувам најдлабока благодарност до мојот ментор, проф. д-р Ице Илијевски, за неговото непоколебливо охрабрување, неговиот проникliв фидбек и континуираното менторство во текот на ова истражувачко патување. Неговата експертиза во областа на сајбер правото беше инструментална во обликувањето на насоката и длабочината на оваа студија.

Изразувам искрена благодарност до наставниот кадар и персоналот на Универзитетот „Св. Климент Охридски“ – Битола, Правен факултет – Кичево, чија посветеност на академската извонредност обезбеди поволна средина за моето истражување. Посебна благодарност до членовите на правната и истражувачката заедница за сајбер безбедност кои го споделија своето знаење и дадоа непроценливи увиди што го збогатија обемот на овој проект.

Исто така, сум благодарен на професионалците, креаторите на политики и службениците за спроведување на законот во Косово кои учествуваа во интервјуа и дискусии, нудејќи перспективи од прва рака за правните предизвици и механизмите за спроведување поврзани со сајбер измамите. Нивните придонеси значително ги подобрија практичните импликации на оваа студија.

Искрена благодарност до моето семејство и пријателите за нивната постојана поддршка, трпение и мотивација во текот на ова патување. Нивното охрабрување ме одржа фокусиран и решен да го постигнам овој успех.

Оваа работа е посветена на сите оние кои се стремат да ги зајакнат законските рамки и механизмите за спроведување против сајбер измамите, обезбедувајќи побезбедна дигитална средина за сите.

11. Литература

11.1. Странска литература

1. Aleksandrovich, L. A. *Cyber Law: Addressing Legal Challenges in the Digital Age*. *Uzbek Journal of Law and Digital Policy* 1, no. 3 (2023): 1–9.

2. AllahRakha, N. “Cybercrime and the Legal and Ethical Challenges of Emerging Technologies.” *International Journal of Law and Policy* 2, no. 5 (2024): 28–35.
3. Brenner, Susan W. *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara: Praeger, 2012.
4. Brenner, Susan. *Cybercrime and Legal Challenges: International Perspectives*. Oxford: Oxford University Press, 2019.
5. Broadhurst, Roderic, and Julie Ayling. “The Suppression of Organized Crime: New Approaches and Problems.” In *Policing and Security in Practice: Challenges and Achievements*, edited by Tim Prenzler, 37–55. Basingstoke: Palgrave Macmillan, 2012.
6. Goodman, Marc. *Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It*. New York: Anchor Books, 2018.
7. Holt, Thomas J., and Adam M. Bossler. *Cybercrime and Digital Forensics: An Introduction*. London: Routledge, 2016.
8. Hoxha, Arben. “Cybersecurity Challenges in Kosovo: Legal and Institutional Perspectives.” *Journal of Digital Law* 8, no. 2 (2021): 55–72.
9. Hoxha, Arben. “Cybersecurity Challenges in Kosovo’s Public Administration.” *Journal of Cybersecurity and Law* 4, no. 1 (2021): 22–37.
10. Hoxha, Elira. “Challenges in Prosecuting Cybercrime in Kosovo.” *Journal of Legal Studies* 12, no. 2 (2020): 87–105.
11. Kaska, Kadri, and Rain Ottis. “Cybersecurity in Estonia: A Model for Small States?” *European Cybersecurity Review* 5, no. 1 (2021): 45–60.
12. Kelmendi, Fisnik. “Challenges in the Legal Treatment of Cybercrime in Kosovo.” *Legal Studies Journal* 12, no. 2 (2020): 45–59.
13. Kelmendi, Fisnik. “Cyber Fraud and Legal Challenges in Kosovo: A Critical Assessment.” *Balkan Legal Review* 15, no. 1 (2020): 34–49.
14. Mustafa, Ardian, and Rilind Halili. “Legal Responses to Cyber Fraud in Kosovo: An EU Approximation Perspective.” *Pristina Legal Journal* 9, no. 1 (2021): 33–50.
15. Peci, Liridon. “Institutional Responses to Cybercrime in Kosovo: Strengths and Weaknesses.” *European Cybersecurity Journal* 4, no. 3 (2018): 102–115.
16. Rexhepi, Lulzim. “Institutional Capacity in Cybercrime Prevention: The Case of Kosovo.” *South Eastern European Law Journal* 14, no. 3 (2022): 21–40.
17. Smith, R. G., Peter N. Grabosky, and Gregor Urbas. *Cyber Criminals on Trial*. Cambridge: Cambridge University Press, 2019.
18. Smith, J., et al. *Cyber Fraud: A Global Analysis*. Cambridge: Cambridge University Press, 2020.
19. Wall, David S. *Cybercrime: The Transformation of Crime in the Information Age*. 2nd ed. Cambridge: Polity Press, 2017.

11.2. Интернет извор и слично

1. Balkan Insight. “Hackers Steal €2 Million from Kosovo’s Treasury.” September 2020. https://balkaninsight.com.
2. Council of Europe. *Convention on Cybercrime – Budapest Convention (ETS No. 185)*. Strasbourg: Council of Europe, 2001. https://www.coe.int/en/web/cybercrime/convention.

3. DCAF – Geneva Centre for Security Sector Governance. Asllani, Mentor. *Cybersecurity Challenges in Kosovo's Financial Sector*. Policy Brief, 2022. https://www.dcaf.ch.
4. ENISA – European Union Agency for Cybersecurity. *Threat Landscape 2023: Cybercrime and Critical Sectors*. Athens: ENISA, 2023. https://www.enisa.europa.eu.
5. European Commission. *Kosovo 2023 Report*. Brussels: European Commission, 2023. https://neighbourhood-enlargement.ec.europa.eu.
6. Europol. *Internet Organised Crime Threat Assessment (IOCTA) 2021*. The Hague: Europol, 2021. https://www.europol.europa.eu.
7. Europol. *Europol Programming Document 2021–2023*. The Hague: Europol, 2021. https://www.europol.europa.eu.
8. Global Initiative Against Transnational Organized Crime (GITOC). *The Future of International Cooperation Against Transnational Organized Crime*. Geneva: GITOC, 2021. https://globalinitiative.net.
9. Information and Privacy Agency (AIP). *Annual Report 2023*. Pristina: Republic of Kosovo, 2023. https://aip.rks-gov.net.
10. Kosovo Law Institute (KLI). *Monitoring the Implementation of the Law on Cybersecurity in Kosovo*. Pristina: KLI, 2022. https://kli-ks.org.
11. Kosovo Police. *Annual Report 2023*. Pristina: Kosovo Police, 2024. https://kosovopolice.com.
12. Kosovo 2.0. "How Strong Are Kosovo's Cyber Defenses?" October 2020. https://kosovotwopointzero.com.
13. Republic of Kosovo. *Criminal Code of the Republic of Kosovo (Law No. 06/L-074)*. Official Gazette of the Republic of Kosovo, 2019. https://gzk.rks-gov.net.
14. Republic of Kosovo. *National Cybersecurity Strategy 2019–2023*. Government of Kosovo, 2019. https://gzk.rks-gov.net.
15. Republic of Kosovo. *Law on Electronic Communications (Amendments)*. Official Gazette of the Republic of Kosovo, 2023. https://gzk.rks-gov.net.
16. United Nations. *United Nations Convention Against Cybercrime* (to be opened for signature, 25–26 October 2025). United Nations Office on Drugs and Crime (UNODC). [link will be available on UNODC's cybercrime page once formally published].
17. European Union. *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.* Official Journal of the European Union, L 218/8, 14.8.2013.
18. European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).* Official Journal of the European Union, L 119/1, 4.5.2016.
19. European Union. *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).* Official Journal of the European Union, L 194/1, 19.7.2016.
20. European Union. *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).* Official Journal of the European Union, L 333/1, 27.12.2022.
21. European Union. *Directive (EU) 2015/2366 on payment services in the internal market (PSD2).* Official Journal of the European Union, L 337/35, 23.12.2015.