ЗАШТИТА НА ДИГИТАЛНАТА ПРИВАТНОСТ

АНАЛИЗА НА ЛЕГИСЛАТИВАТА И ПРАКТИКАТА
ВО РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА И ПОШИРОКО

СКОПЈЕ 2024

Издавач
Македонско здружение на млади правници (МЗМП)
ул. Донбас бр. 14/1-6 1000 Скопје
www.myla.org.mk | contact@myla.org. mk
тел. 02/ 3220 870

Автори
Љубица (Пендароска) Крстевска
Методи Хаџи-Јанев

Уредник
Мартина Дранговска Мартинова

Лектура
Елеонора Попетревска

Дизајн
Харис Мурић

Место на издавање
Скопје

Место за ЦИП

Содржина

Преглед на листата на позначајни кратенки

АЗЛП	Агенција за заштита на личните податоци
VoIP	Voice over IP
ЕКС	Електронски комуникациски услуги
ЕМБГ	Единствен матичен број на граѓанинот
ENISA	Европска агенција за безбедност на мрежи и информации
ЕУ	Европска Унија
MKD - CIRT	Национален центар за одговор на компјутерски инциденти
ООН	Организација на обединетите нации
ОЕЦД	Организација за економска соработка и развој
ПВВЗП	Проценка на влијанието врз заштитата на податоците
РСМ	Република Северна Македонија
СЕ	Совет на Европа
ФЗО	Фонд за здравствено осигурување

Извршно резиме

Конвергенцијата на виртуелниот и физичкиот свет нуди голем број поволности, но носи и ризици. Покрај другото, овие ризици се манифестираат преку различни и зголемени можности во волумен и фреквенција за нарушување на приватноста на граѓаните. Иако на меѓународен план свеста за потребата од поефективна заштита на приватноста преку интернет е препознаена широко, пролиферацијата на модерните технологии и нивната меѓусебна поврзаност и зависност ја зголемува ранливоста на ова човеково право. Во таа насока, сајбер-нападите претставуваат сериозна и континуирана закана за приватноста на македонските граѓани во интернет-просторот.

Користејќи ги современите технологии и ниското ниво на свесност кај македонските граѓани, малициозни актери лесно може да воспостават контрола врз информациите што граѓаните ги споделиле или складирале на интернет. На тој начин, овие актери или, пак, тие што се заинтересирани за тоа, може да дојдат до чувствителни лични податоци, финансиски податоци, историја на прелистување, информации за локацијата на престојување и онлајн-однесување. Дигиталниот пејзаж во таа смисла нуди комплексен екосистем, каде што информациите течат беспрекорно, честопати замаглувајќи ги границите помеѓу јавните и приватните домени. Ако во овој контекст се стават зачестените сајбер-напади врз македонските институции за кои јавноста знае, опасноста за приватноста на граѓаните преку македонскиот интернет-простор расте катадневно.

Политиките за заштита на приватноста се камен-темелник на транспарентноста и довербата помеѓу онлајн-платформите и давателите на услуги и нивните корисници. Тие овозможуваат насоки за тоа како се собираат, складираат, обработуваат и споделуваат личните податоци. Сепак, ефективноста и сеопфатноста на овие политики е различна за различни платформи. Нивната доследна имплементација е императив за намалување на ризиците за загрозување на приватноста на граѓаните преку интернет-просторот. Овие политики треба да воспостават баланс помеѓу потребата од законски уредено собирање, чување и обработка на податоците и да ги намалат ризиците од злоупотреба на податоците на граѓаните преку интернет.

Усогласеноста на законската регулатива за заштита на приватноста на македонските граѓани преку интернет, сепак, не е гаранција за ефикасноста на заштитата на приватноста во пракса. Во таа насока, покрај општите предизвици карактеристични за сите земји во светот, постојат низа предизвици што се специфични за безбедноста на приватноста преку интернет на македонските граѓани.

Предизвиците што влијаат врз намалување на ефективната заштита на приватноста преку интернет и се специфични за Република Северна Македонија може да се класифицираат во две групи. Прво, политизација и партизација на јавниот сектор и за сметка на тоа непрофесионален пристап кон прашањата и делокругот на области поврзани со приватноста. Второ, поврзано со претходното, ниското ниво на свест за важноста на заштитата на приватноста преку интернет и во склад со тоа низа други недостатоци што влијаат на намалување на ефективната и ефикасна заштита на приватноста преку интернет.

Вовед

Потребата од заштита на приватноста преку интернет е резултат на напорите за дигитализација и предизвиците што се јавуваат од овие напори. Зголемената потреба за користење на информациско-комуникациските технологии во секојдневниот живот отвора низа можности за злоупотреба на приватноста на македонските граѓани преку интернет-просторот. Од тоа како и колку добро ќе бидат создадени политиките, законските решенија и организациската поставеност на органите во однос на почитувањето на приватноста, но и нивната доследна примена преку почитувањето на демократските принципи за добро, транспарентно и одговорно владеење ќе зависи и ефикасноста и ефективноста на заштитата на приватноста преку интернет. Оваа анализа има цел да утврди како и во која мерка правото на приватност преку интернет на македонските граѓани е заштитено.

За да ја постигне таа цел, анализата прави компаративни согледувања на политиките за заштита на приватноста преку интернет и меѓународните и европските стандарди со политиките и правната рамка за заштита на приватноста преку интернет во Северна Македонија. На тој начин се идентификуваат празнините, слабостите и областите за подобрување. Анализата започнува со опис на користената методологија и ја обработува содржината преку четири глави.

Во првата глава се дава општ преглед на заштитата на приватноста во дигиталниот свет. Во таа насока, анализата прави осврт на ризиците што влијаат на загрозувањето на приватноста преку интернет со посебен осврт на ризикот за македонскиот граѓанин и на тоа што треба да опфати проценката на политиките за заштита на приватноста преку онлајн-платформи и услуги во Северна Македонија.

Во втората глава анализата се фокусира на правната рамка на правото на приватност во Северна Македонија. Оваа глава прво ја скицира законската основа што ја уредува приватноста општо и преку интернет посебно, а потоа ги разработува релевантните законски решенија за тоа. Анализата во овој дел детално го разработува Законот за заштита на личните податоци. Понатаму, ги посочува и другите законски решенија, како Законот за електронските комуникации, Законот за електронската трговија, Законот за кривичната постапка, Кривичниот законик, Законот за следењето на комуникациите и сл., со што прави сумарен преглед на речиси сите законски решенија што ја регулираат заштитата на приватноста на македонските граѓани директно или, пак, имаат улога во спречувањето на нејзиното нарушување преку интернет-просторот.

Третата глава ги користи заклучоците од претходната анализа за споредба на усогласеноста на македонската регулатива со законските решенија на Европската Унија и меѓународните стандарди и принципи за заштита на приватноста преку интернет. Општата регулатива за заштита на податоците на ЕУ е главен извор во однос на кој се мери усогласеноста на македонската законска рамка во предметната анализа (заштита на приватноста преку интернет) со таа на Европската Унија. Земајќи предвид дека приватноста преку интернет има свои специфичности, анализата во овој дел се осврнува и на Директивата на ЕУ за е-приватност, но и на идејното решение што набргу ќе стане реалност – Нацрт-регулативата на ЕУ за е-приватност. Анализата врши споредба и со другите меѓународни принципи и стандарди што имаат релевантност во воспоставувањето правна рамка за поефикасно уредување на

заштитата на приватноста преку интернет-просторот. Тука посебно се обработени темелните документи што ги генерираат општите принципи и стандарди за заштита на правото на човекот, како рамка за воспоставување ефикасна регулатива за заштита на приватноста преку интернет. Покрај општите начела на меѓународното право за правата на човекот, посебно внимание во оваа глава се посветува на проценатa на усогласеноста на македонската регулатива за заштита на приватноста преку интернет со специфичните упатства, насоки и инструменти на меѓународен и регионален план. Така, покрај насоките на релевантните тела на ООН, се обработени и насоките и инструментите на регионалните организации што имаат голема важност за Северна Македонија. Во последниот дел оваа глава нуди краток преглед на добрите практики за примена на правото на приватност во дел од земјите членки на Европската Унија со посебен осврт на заштитата на приватноста преку интернет.

Врз основа на претходните заклучоци, во четвртата глава анализата ги утврдува празнините во тековниот пристап кон заштита на приватноста преку интернет во Северна Македонија. Заради поголема прегледност, анализата најпрвин ги идентификува генералните предизвици за заштита на приватноста преку интернет што се релевантни и за Северна Македонија. Потоа, прави осврт на специфичните предизвици што произлегуваат од примената на законските решенија и добрите практики од ЕУ vis-a vis заканите, инцидентите и примената на политиките за заштита на приватноста преку интернет во македонската пракса. На крај се дадени првични наоди и препораки за подобрување.

Методологија за сеопфатна анализа на политиките за приватност на интернет во Северна Македонија

Оваа методологија обезбедува структуриран пристап за спроведување сеопфатна анализа на политиките и регулативите за приватност на интернет во Северна Македонија. Методологијата овозможува темелно испитување, утврдување на релевантните актери со цел давање соодветни препораки за подобрување на политиките, законските решенија, но и нивна примена во пракса за заштита на приватноста на македонските граѓани преку интернетот.

За да ја постигне саканата цел, оваа методологија ќе се фокусира на дефинирање на предметот и рамката на анализата преку идентификација на ризиците за приватноста преку интернет и утврдување на потребните политики за нејзина заштита. Потоа ќе изврши преглед на правната регулатива, компаративна анализа на македонската регулатива со европските и меѓународните стандарди и утврдување на празнините и идентификација на слабостите. Резултатите се добиени со вкрстена анализа на постојните законски решенија, заклучоците од досегашните истражувања и работилници на оваа тема, упатствата и добрите практики на ЕУ, добрите практики од светски и реномирани автори во областа и долгогодишната работа на експертите на повеќе проекти (прегледот на литературата што е користена е дадена на крајот од оваа анализа).

Благодарение на заклучоците на ваквата вкрстена анализа ќе биде подготовен документ за јавни политики во кој ќе бидат наведени неопходните реформи со цел да се даде приоритет и да се зајакне заштитата на приватноста на интернет во Северна Македонија. Единствено ограничување е немањето можност за организирање структурирани интервјуа (беа користени резултатите од досегашните анализи) и анкетни прашалници или примена на системската анализа за евалуација за која авторите се сертифицирани евалуатори.

Глава - I

Заштита на приватноста во дигиталниот свет

1.1 Ризикот за приватноста на македонските граѓани во дигитални средини

Приватноста како основен дел од човековата безбедност (доаѓа од human security) е под силен притисок. Можноста што современите технологии ја даваат во смисла на собирање, размена, складирање и обработка на голем број податоци во единица време станува сериозен предизвик за заштита на личните податоци, а со тоа и за човековите права општо и приватноста посебно на граѓаните ширум светот.

Во таа смисла, релевантноста на загриженоста за македонските граѓани доаѓа од глобалниот досег штп интернетот и современите дигитални технологии го овозможуваат. Меѓусебната зависност и поврзаност на овие технологии за добро, е предуслов со кој голем број актери од различни побуди имаат директен пристап до интимата-приватноста на македонскиот граѓанин. На тој начин, за релативно кратко време под прагот на воспоставените процедури во физичкиот свет (изградени врз база на претпоставката за физичката дистанца, безбедносните и гранични протоколи, царински процедури, цената на услугата за патување, сместување и времето за сето тоа), индивидуалци со различен профил и интерес може лесно преку виртуелниот свет да ја загрозат приватноста на речиси секој граѓанин што користи некакви уреди за комуникација преку интернет-просторот. Анонимноста што овие заинтересирани страни може да си ја дозволат, како и можноста за глобален досег со многу мала можност за одвраќање (во смисла на комплицираност за процесирање или прогон во случај на прекршување на приватноста на домот или личните податоци на граѓанинот) ја прави можноста за интрузивност мошне привлечна.

Приватноста во дигиталните средини ја опфаќа заштитата на личните податоци, а преку тоа и нашите навики, движења, размислувања и вредности.[1] Со обезбедување контрола врз нечии информации споделени или складирани на интернет, покрај другото, може да се дојде до чувствителни лични податоци, финансиски податоци, историја на прелистување, информации за локација и онлајн-однесување. Иако честопати обичниот граѓанин е воден од помислата дека неговите лични податоци и навики, на пример, не се од јавен или општ интерес, голем број специјализирани компании имаат различни причини да собираат податоци за населението.

Компаниите што имаат комерцијален интерес, како огласувачите, на пример, имаат потреба од податоци за населението и поради тоа имаат посебни алгоритми со кои нé таргетираат преку персонализирани реклами.[2] Компаниите што ги управуваат или поседуваат социјалните медиуми за комуникација ги користат податоците за да го анализираат нашето однесување и да ни покажат попривлечна содржина. Иако во голема мерка граѓаните поради ниското ниво на свесност или, пак, поради желбата за услуги доброволно ги тргуваат своите податоци, проблемот се јавува, кога истите тие лични податоци ќе паднат во погрешни раце. Листата со потенцијални злонамерни корисници на податоците на македонскиот граѓанин во таа смисла се протега од обични криминалци што имаат економски интерес, преку лица со душевни или други социјални проблеми, па се до индивидуалци или групи што имаат екстремистичка и насилна идеологија или владини агенти (односно лица најмени од субјекти што имаат политички мотив). Хакерите можат да ги користат личните податоци за да извршат кражба на идентитет, да пристапат до банкарски сметки на граѓаните, па дури и да вршат уцени, да дезинформираат, манипулираат, а со тоа и радикализираат, односно да побудат политички активизам против системот и интересите на државата.[3]

1 Повеќе за ова може да се види во: The UNOHCR, (2022), "OHCHR And Privacy In The Digital Age", A/HRC/51/17, https://www.ohchr.org/en/privacy-in-the-digital-age

2 За начините на кои компаниите собираат податоци преку интернет пошироко може да се види на пример во: Max Freedman, (Oct 20, 2023), How Businesses Are Collecting Data (And What They're Doing With It), Business News Daily, https://www.businessnewsdaily.com/10625-businesses-collecting-data.html

3 Пошироко за злоупотребата на овие практики може да се види во последниот извештај на ООН, UN General Assembly, (2022), The right to privacy in the digital age - Surveillance of personal devices and communications, Hacking, достапно на: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement

Покрај сите овие ризици, постојат и етички причини за тоа како компаниите ги користат нашите лични податоци. Условно многу луѓе се чувствуваат непријатно од идејата да бидат под постојан мониторинг на интернет. Скандалите од типот на „Кембриџ аналитика“, каде што политичка консултантска фирма ги собрала податоците на милиони корисници на „Фејсбук“ без нивна согласност, најдобро го отсликува овој проблем.[4]

Неколку предизвици ја загрозуваат приватноста во дигиталната област. Првиот е сеприсутноста на механизмите за собирање податоци. Компаниите и онлајн-платформите користат софистицирани алгоритми за собирање информации за корисниците, честопати без експлицитна согласност. Дополнително, ризикот од злоупотреба на податоци и сајбер-напади е голем, потенцијално изложувајќи ги поединците на кражба на идентитет, финансиска загуба или нанесување штета на репутацијата и угледот. Понатаму, со сé поголемата присутност на меѓусебно поврзани уреди преку интернет или т.н. ефект на „интернет на нештата“ (доаѓа од Internet of Things-IoT)[5] предизвикува загриженост за безбедноста на личните информации што се пренесуваат преку различни уреди (паметни часовници, паметни телевизори, паметни клима-уреди, правосмукалки и други апарати за домаќинството, па дури и паметни системи во автомобилите, беспилотните летала и други помагала за социјално дејствување и општење кои се со дигитални платформи за комуникација преку интернет).

1.2. Преглед на вообичаените трендови на сајбер-напади за прекршување на приватноста преку интернет во Северна Македонија

„Фишинг“ напади: Фишингот продолжува да биде значајна закана, за нарушување на приватноста преку интернет. Овој вид сајбер-напади се шири и еволуира, како што се засилуваат кампањите за подигање на свеста кај граѓаните за опасностите и методите на фишинг што се користат за злоупотреба на податоците и приватноста преку интернетот за различна корист - од економска, преку социјална до политичка. Во основа, фишинг-нападите вклучуваат измамничка е-пошта или пораки преку апликациите за комуникација на социјалните медиуми (вклучително и СМС-пораки) дизајнирани да ги измамат граѓаните и да создадат поволни услови за креаторите на овие пораки полесно да дојдат до чувствителни информации за жртвата. Овие напади често се насочени кон вработените во организациите, или, пак, се применуваат масовно и по случаен избор со цел на илегален начин да се дојде до податоци со кои се загрозува приватноста преку интернет-просторот.

Успешноста на фишинг-нападите се должи на масовноста на користењето на интернетот и на ниското ниво на свест за опасностите во комбинација со медиумската и информациската (не)писменост на корисниците. Ова го прави фишингот една од најраспространетите закани за сајбер-безбедноста наоколу, особено кога станува збор за загрозување на приватноста преку интернет.

4 Rosalie Chan, (October 9, 2019), "The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections", Business Insider, достапно на: https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10

5 Alexander S. Gillis, (2021), "DEFINITION internet of things (IoT)", TechTarget достапно на: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

Дел од варијантите што се идентификувани како такви опфаќаат т.н. сајбер-напад на **„Фишинг со копје“ (Spear Phishing).** Овој вид сајбер-напади вклучува таргетирање поединец во рамките на институцијата (јавен или приватен сектор). Целта на овој вид фишинг-напади е да се украдат нивните ингеренции за најавување (лични податоци лозинка и корисничко име). Напаѓачот често прво собира информации за личноста пред да започне нападот, како што се неговото име, позиција и детали за контакт.

Вишинг (Vishing - кратенка за „гласовен фишинг“) е сајбер-напад кога некој ги користи телефонот и апликациите за комуникација преку социјалните медиуми на телефонот за да се обиде да украде информации. Напаѓачот може да се преправа дека е доверлив пријател или роднина или дека ги застапува или, пак, да биде некоја друга личност што ѝ е позната на жртвата со цел да извлече податоци со кои би се загрозила приватноста, па дури и јавната чест. Иако вишинг-нападот може да изгледа како старомодна измама, користењето на автоматската технологија за симулација на глас или апликации на вештачка интелигенција може да го направат мошне софистициран. Јавување за лажни телемаркетинг понуди, измами за техничка поддршка за кабелските оператори, измама за компромитирање на банкарската сметка, претставување во име на владин претставник и сл. се формите преку кои оваа форма на напад најчесто се манифестира за да ја злоупотреби приватноста преку интернет.

Фишинг по е-пошта. Во измама за фишинг преку е-пошта напаѓачот испраќа е-пошта што изгледа легитимна, дизајнирана да го измами примачот да внесе информации како одговор или на страница што хакерот може да ја користи за да ги украде или продаде нивните податоци.

HTTPS фишинг. Нападот за фишинг на HTTPS се врши со испраќање е-пошта на жртвата со линк до лажна веб-локација. Веб-страницата потоа може да се користи за да се измами жртвата да ги внесе своите приватни информации.

Фарминг. Во сајбер-напад на фарминг, жртвата добива инсталиран злонамерен код на својот компјутер. Овој код потоа ја испраќа жртвата на лажна веб-локација дизајнирана да ги собере нивните ингеренции за најава.

Поп-ап фишинг (Pop-up Phishing). Ваквиот фишинг-напад често користи „скокачки“ (pop-up) прозорец за проблем со безбедноста на компјутерот на жртвата или некој друг проблем за да ја измами жртвата да кликне на малициозниот линк. Потоа жртвата се упатува да преземе датотека, која завршува како малициозен софтвер, или да повика центар за поддршка.

Злонамерен-близнак фишинг (Evil Twin Phishing). Во ваквиот вид сајбер-напад, хакерот поставува лажна Wi-Fi мрежа, која изгледа реално. Ако некој се најави на неа и внесе чувствителни детали, хакерот ги „фаќа“ неговите информации.

Сајбер-напад од типот „дупка за наводнување“ како облик на фишинг. Во овој вид напад на фишинг, хакерот открива локација што група корисници имаат тенденција да ја посетат. Тој потоа го користи за да ги инфицира компјутерите на корисниците во обид да навлезе во мрежата.

Сајбер-напад познат како Whaling (Китови). Ова е напад на фишинг кој цели на висок извршен директор. Овие лица често имаат длабок пристап до чувствителните области на мрежата, така што успешен напад може да резултира со пристап до вредни информации.

Покрај фишинг-нападите, постојат и друг вид напади со кои се загрозува приватноста на интернет.

Ransomware сајбер-напади: Нападите што се класифицираат како Ransomware сајбер-напади вклучуваат шифрирање на податоците на жртвата и барање откуп за нивното ослободување. Овие напади вообичаено се изведуваат во комбинација со други сајбер- напади преку кои жртвата се намамува да сподели дел од своите податоци или, пак, преку кои се дозволува пристап до податоците што се приватни. Потоа хакерите – сајбер-криминалците ги користат овие податоци за илегално навлегување во одредена база на податоци (вообичаено кај правните лица-организации, компании или јавниот сектор). Северна Македонија во изминатиот период се соочи со ваков вид напад, за што ќе стане збор подолу.

Сајбер-напади врз синџирот на снабдување: Хакерите во овие напади се насочени кон ранливости во синџирот на снабдување за да го компромитираат софтверот или хардверот што го користат организациите. Ова може да доведе до широко распространети прекршувања на податоците, како што се гледа во различни сектори.

Инсајдерски закани: Злонамерните или небрежни дејствија од страна на вработените или изведувачите – давателите на услуги може да претставуваат значителен ризик. Ова може да вклучи намерна кражба на податоци, ненамерно изложување на чувствителни информации или несоодветни безбедносни практики и потценување на протоколите за безбедно чување и управување со личните податоци преку интернет.

Сајбер-напади што се резултат на слабо управување со автентикација и акредитиви. Слабите лозинки, несоодветното чување и нивното несмасно споделување, несоодветните механизми за автентикација и лошите практики за управување со ингеренциите може да доведат до неовластен пристап. Повеќефакторската автентикација е клучна за ублажување на овој ризик.

Напади што ги искористуваат застарените софтвери и системи: Неуспехот навремено да се применат безбедносни ажурирања (update) на софтверите и системите може да ги изложи системите во кои се чуваат податоците или што се користат за комуникација и пренос на лични податоци на пропусти. Редовното ажурирање на софтверот и системите е од суштинско значење за намалувањето на ризиците од ваков вид напади.

Ранливост на Интернет на нештата (IoT): Зголеменото усвојување на IoT уреди воведе нови вектори на напади. Небезбедните IoT уреди или оние што имаат слаба заштита може да се искористат за да се добие неовластен пристап до мрежи и до чувствителни податоци.

Несоодветно шифрирање на податоците: Потценувањето на потребата за тоа да се шифрираат чувствителни податоци и во транзит и во мирување може да резултира со лесно пробивање или прекршување на безбедноста на податоците. Спроведувањето робусни протоколи за шифрирање помага да се заштитат информациите од неовластен пристап.

Сајбер-напади што ги искористуваат предизвиците за усогласеност со регулативата: Придржувањето кон прописите за заштита на податоците, како што е, на пример, Општата регулатива за заштита на податоците во ЕУ или, пак, насоките од Директивата на е-приватност на ЕУ е од клучно значење. Непочитувањето може да доведе до правни последици и оштетување на угледот.

Загриженост за безбедноста на виртуелните облаци (Cloud): Како што организациите сè повеќе мигрираат кон чување на податоците во виртуелни облаци, осигурувањето на безбедноста на услугите и податоците базирани на чување на податоците во облак станува критично. Погрешно конфигурираните поставки за облак може да изложат чувствителни информации.

1.3. Преглед на некои случаи на злоупотреба на приватноста на граѓаните преку интернет во Северна Македонија

Напад врз Државната изборна комисија.[6]

Хакерскиот напад врз веб-страницата на Државната изборна комисија (ДИК) на самиот изборен ден во 2020 година, како и обвинувањата за технички слабости на апликацијата отворија прашања за начинот на којшто институциите го штитат изборниот процес. По сајбер-нападот врз ДИК, следуваа директни напади на серверите на Министерството за здравство и Министерството за образование и наука. Резултатот од ова беше преземање податоци од мејл-серверот на Министерството за здравство. Во случајот со МОН, институциите не посочија каква штета е предизвикана.[7]

Напад врз Министерството за образование и наука

Нападот врз Министерството за образование и наука што се случи на 10 септември 2022 година е еден од посериозните напади во кои постои сомневање дека приватноста преку собирање на личните податоци на голем број граѓани е загрозена. Ова е напад во кој веб-страницата на Министерството за образование и наука (МОН) беше хакирана. На сајтот на МОН тогаш пишуваше дека страната е хакирана од грчки хакерски тим „Netwatchers“.[8] Тогаш од МОН информираа дека се во комуникација со Националниот ЦИРТ центар за компјутерски инциденти при Агенцијата за електронски комуникации, каде што е пријавен случајот и од каде што се очекува, со поддршка на МВР, да се преземат конкретни активности за пронаоѓање на локацијата и изворот на нападите. Од Министерството посочија дека нема потреба од грижи за наводно преземање на некакви бази на податоци на граѓаните, затоа што на веб-страницата не постојат такви позадински бази и таа има информативен карактер.

Vlada.mk „препродава“ патики, дресови, ташни и чевли по поволни цени[9]

Ова беше саркастичниот наслов во кој еден од информациските портали ја сподели веста за хакираната владина интернет-страница. Информацијата навлезе подлабоко во

6 Истражувачка репортерска лабораторија Македонија, (28 јули, 2020), „Агенцијата за заштита на лични податоци ќе проверува дали ДИК безбедно ги чува податоците по сајбер-нападот на изборниот ден“, достапно на: https://irl.mk/agentsiata-za-zashtita-na-lichni-podatotsi-e-proveruva-dali-dik-bezbedno-gi-chuva-podatotsite-po-saber-napadot-na-izborniot-den/

7 Истражувачка репортерска лабораторија Македонија, (28 јули, 2020), „Агенцијата за заштита на лични податоци ќе проверува дали ДИК безбедно ги чува податоците по сајбер-нападот на изборниот ден“, достапно на: https://irl.mk/agentsiata-za-zashtita-na-lichni-podatotsi-e-proveruva-dali-dik-bezbedno-gi-chuva-podatotsite-po-saber-napadot-na-izborniot-den/

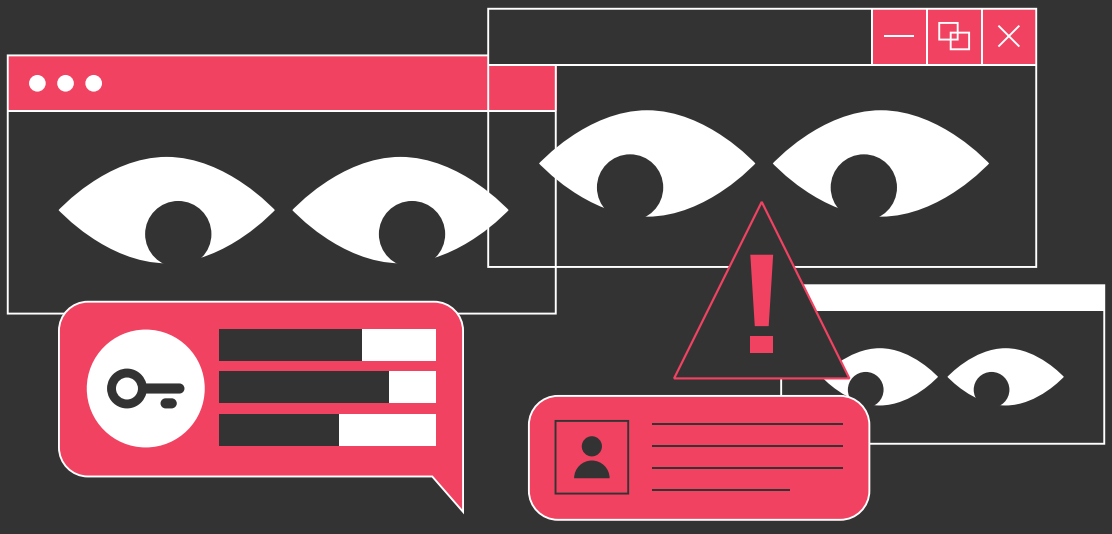
8 „360 степени“, (12 септември, 2022), „По хакерскиот напад на сајтот на МОН ќе се проверува дали имало нарушување на безбедноста на личните податоци“, достапно на: https://360stepeni.mk/po-hakerski-ot-napad-na-sajtot-na-mon-ke-se-proveruva-dali-imalo-narushuvane-na-bezbednosta-na-lichnite-podatotsi/

9 IT MK, (септември 2022), „Vlada.mk 'препродава' патики, дресови, ташни и чевли по поволни цени“, достапно на: https://it.mk/vlada-mk-preprodava-patiki-dresovi-tashni-i-chevli-po-povolni-tseni/

нападот и во истата сторија беше објавено дека тоа не е сé. Имено, во „топ-шоп“ фазон, Vlada.mk не „препродава“ само патики и чевли, сајтот Vlada.mk има индексирано и повеќе од 1.590.000 резултати за ташни и аксесоари за патување.[10] Сепак, и покрај сарказмот, сериозноста на нападот беше евидентна бидејќи, според надворешните анализи, се работи за сериозен ИТ безбедносен пропуст. Хакирањата на сајтови кои најчесто се автоматизирани со скрипти и служат за градење репутација на т.н. backlinks на сајтови што се занимаваат со е-трговија, препродажба и affiliate е можно во два случаја. Во првиот случај се работи за SPAM линкови изгенерирани најчесто преку искористување на интерниот систем за пребарување на сајтовите, при што со внесување на клучен збор или термин, самиот интерен пребарувач на сајтот гради и страна со URL за дадениот линк. Второто сценарио е дека некој на некој начин добил пристап до серверите каде што е хостиран сајтот Vlada.mk и креирал инстанци на сајтови за е-трговија наполнети со еден куп продукти, кои потоа се поврзуваат до други сајтови. Во вториот случај тоа значи и пристап до сериозни податоци од серверите.

Напад врз Министерството за земјоделство, шумарство и водостопанство

Министерството за земјоделство, шумарство и водостопанство ги информира граѓаните дека електронскиот систем на министерството беше цел на хакерски напад кој предизвика блокирање на редовниот работен процес и оневозможување на исполнувањето на тековните процеси во надлежност на министерството – беше дел од соопштението што Министерството го објави на една од социјалните мрежи.[11] Нападот беше пријавен во Министерството за внатрешни работи за понатамошно истражување и постапување, а поради сериозноста на проблемот, системите во министерството моментално се ставени вон функција. Во моментот на нападот вработените во Секторот за информатички технологии при Министерството работеа на отстранување на проблемот и повторно подигнување на системот. Сепак, подоцна беше известено дека напаѓачите успеаја да дешифрираат податоци од документи и за нив бараа откуп.[12]



10 IT MK, (септември 2022), „Vlada.mk 'препродава' патики, дресови, ташни и чевли по поволни цени“, достапно на: https://it.mk/vlada-mk-preprodava-patiki-dresovi-tashni-i-chevli-po-povolni-tseni/

11 https://www.facebook.com/mzsv.gov.mk/posts/460581649442322

12 Владимир Калински, (21 октомври, 2022), https://www.slobodnaevropa.mk/a/%D0%B7%D0%B0%D1%87%D0%B5%D1%81%D1%82%D0%B5%D0%BD%D0%B8%D1%82%D0%B5-%D1%81%D0%B0%D1%98%D0%B1%D0%B5%D1%80-%D0%BD%D0%B0%D0%BF%D0%B0%D0%B4%D0%B8-%D0%BD%D0%B0-%D0%B4%D1%80%D0%B6%D0%B0%D0%B2%D0%BD%D0%B8-%D1%81%D0%B0%D1%98%D1%82%D0%BE%D0%B2%D0%B8-%D0%B3%D0%BE-%D0%B2%D0%BA%D0%BB%D1%83%D1%87%D1%83%D0%B2%D0%B0%D0%B0%D1%82-%D1%86%D1%80%D0%B2%D0%B5%D0%B8%D0%BE%D1%82-%D0%B0%D0%BB%D0%B0%D1%80%D0%BC-/32093026.html

Напад врз Фондот за здравствено осигурување

Еден од најсериозните напади во кои е можно да дојде до масовна злоупотреба на податоците преку интернет е нападот што се случи врз Фондот за здравствено осигурување.[13] Во овој напад на податоци на корисниците, вклучително и личните податоци на граѓаните, беа украдени сите податоци од Фондот за здравствено осигурување. Изјавите на премиерот и министерот за внатрешни работи дека информатичкиот систем на ФЗО е хакиран со напад од типот „ransomware", со кој ги криптирале податоците во кои, покрај другото, има лични податоци на сите осигуреници во Фондот. Логично, како и при секој ваков напад хакерите барале откуп за да го ослободат системот.[14] Надминувањето на предизвикот беше со рачно внесување на дел од податоците, а на оперативните тимови од Министерството за здравство и ФЗО им помогнаа експерти од Германија и други меѓународни партнери.[15]

Бројот на напади врз јавните сервери е зголемен

Иако бројот на сајбер-напади не е ограничен на наведените, евидентно е дека фреквенцијата на напади врз јавните сервери на кои се чуваат и обработуваат лични податоци на граѓаните е зголемен. Според информациите на МКД-ЦИРТ, напади што вклучуваат т.н. метода на фишинг-напад во просек се случуваат и до два-пати неделно. Овие напади се користат за испраќање лажни пораки со кои напаѓачите добиваат чувствителни информации или распоредуваат малициозен софтвер во инфраструктурата на жртвата, а потоа бараат откуп. Покрај финансиските или економските ефекти, во голема мерка овие напади се порта за загрозување на приватноста преку интернет.

Во интервју за Радио „Слободна Европа" од МКД-ЦИРТ потенцираат дека во државата сè уште нема законска обврска за задолжително пријавување на инцидентите. Некои од пријавите доаѓаат од трети лица, некои од самата организација што е цел на сајбер-нападот, а и самите детектираат „проблеми" за кои потоа бараат потврда од организацијата дали се резултат од напад.[16]

13 „eMагазин": Од Фондот за здравство тврдат дека податоците на граѓаните се безбедни и дека не се украдени, објавено на 17.2.2023, достапно на: https://emagazin.mk/od-fondot-za-zdravstvo-tvrdat-deka-podatocite-na-graanite-se-bezbedni-i-deka-ne-se-ukradeni/

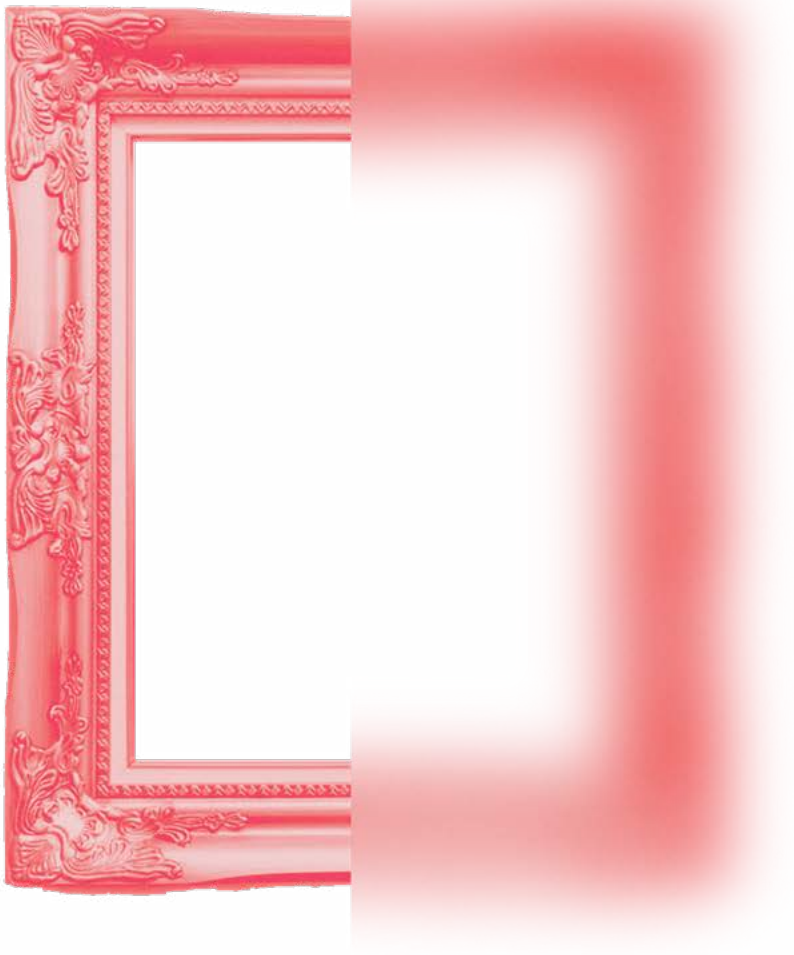
14 „eMагазин": Од Фондот за здравство тврдат дека податоците на граѓаните се безбедни и дека не се украдени, објавено на 17.2.2023, достапно на: https://emagazin.mk/od-fondot-za-zdravstvo-tvrdat-deka-podatocite-na-graanite-se-bezbedni-i-deka-ne-se-ukradeni/

15 „eMагазин": Од Фондот за здравство тврдат дека податоците на граѓаните се безбедни и дека не се украдени, објавено на 17.2.2023, достапно на: https://emagazin.mk/od-fondot-za-zdravstvo-tvrdat-deka-podatocite-na-graanite-se-bezbedni-i-deka-ne-se-ukradeni/

16 Владимир Калински, (21 октомври, 2022), цитирано

Глава - II

Преглед на правната рамка на правото на приватност во Република Северна Македонија



2.1 Анализа на заштитата на приватноста во дел од позначајните македонски законски решенија

2.1.1. Законот за заштита на личните податоци

Законот за заштита на личните податоци ја уредува заштитата на личните податоци и правото на приватност во врска со обработката на личните податоци, а особено: начелата поврзани со обработката на личните податоци, правата на субјектот на личните податоци, положбата на контролорот и обработувачот, преносот на личните податоци во други држави, основањето, статусот и надлежностите на Агенцијата за заштита на личните податоци, посебните операции на обработка на личните податоци, правните средства и одговорноста при обработката на личните податоците, супервизијата над заштита на личните податоци, како и прекршоците и прекршочната постапка во оваа област. Овие теми се обработени во единаесет поглавја.

Законот се применува на целосно или делумно автоматизирана обработка на личните податоци и на друга обработка на личните податоци коишто се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци. Законот не се применува врз обработката на личните податоци што се врши од страна на физички лица, исклучиво заради лични активности или активности во домот. Законот се применува и ако контролорот или обработувачот на личните податоци е основан на територијата на Република Северна Македонија, без разлика дали обработката на личните податоци се врши на територијата на Република Северна Македонија или надвор од нејзините граници.

Во понатамошниот дел новиот закон, за разлика од првичниот донесен во 2005 година дава преглед на нови дефиниции и поими. Во таа смисла во членот 4 од Законот се дефинираат нови поими и термини што се одраз на еволуцијата и осовременувањето на технологијата што се користи при обработката на личните податоци или со кои е можно нарушувањето на приватноста.

Законот исто така предвидува дека изразите што се употребуваат, а не се дефинирани во ставот имаат значење утврдено со друг закон. Во оваа глава се и начелото на забрана за дискриминација, одредбите за примена на Законот за општа управна постапка, како и одредби со кои се дефинираат давањето податоци и пружањето помош.

Во однос на преносот на лични податоци, Законот предвидува дека секој пренос на лични податоци што е подложен на обработка или е наменет за обработка по преносот во трета земја или во меѓународна организација, може да се изврши само доколку условите се утврдени според законот. Притоа, не се бара овие одредби да се применуваат само од контролорот и обработувачот, туку да се осигури примена на одредбите и во понатамошниот пренос на личните податоци од третата земја или меѓународна организација во друга трета земја или меѓународна организација. Целта на овие одредби е да се обезбеди заштита на физичките лица. Ако податоците се пренесуваат во рамките на ЕУ (земја членка) или во земја членка на Европскиот економски простор, тогаш овие одредби не се применуваат, контролорот или обработувачот е должен да ја извести Агенцијата.

Новиот Закон за заштита на личните податоци воведува како новина низа технички и организациски мерки. Новина е тоа што овие мерки се дизајнираат и имплементираат

според повеќе критериуми. Таквите критериуми, покрај другото, се однесуваат на природата, обемот, контекстот и целите на обработката, како и на ризиците со различна веројатност и на сериозноста за правата и слободите на физичките лица. Дополнително, мерките се дизајнираат и имплементираат согласно најновите технолошки достигнувања (a state-of-the-art technology), што како обврска бара техничките и организациските мерки секогаш да се преиспитуваат и ажурираат, на начин што ќе биде соодветен на времето во кое се дизајнираат и имплементираат. Такви мерки што законот експлицитно ги наведува се псевдонимизацијата и криптирањето на личните податоци, способноста за обезбедување континуирана доверливост, интегритет, достапност и отпорност на системите и услугите за обработка на личните податоци или, пак, на пример способноста за навремено, повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на физички или технички инцидент.

Дополнителна новина претставува и делот од законот што се однесува на техничката и интегрирана заштита на личните податоци (data protection by design and by design). Согласно овие новини, контролорот (како што е дефиниран погоре) во моментот на дефинирање на средствата за обработка, како и во моментот на самата обработка, е должен да примени соодветни технички и организациски мерки со кои ќе се обезбеди ефикасно спроведување на начелата за заштита на личните податоци, како што се, на пример, псевдонимизацијата и сведувањето на минимален обем на податоците (data minimization). Контролорот исто така е должен да ги примени сите потребни заштитни мерки во процесот на обработката, со цел да се исполнат условите за законита обработка на личните податоци, а воедно да се обезбеди заштита на правата на субјектите на личните податоци.

Согласно оваа мерка, контролорот треба да ги примени сите технички и организациски мерки со кои се обезбедува интегрирано (by default), односно на ниво на целиот информациски систем на контролорот, дека се обработуваат само оние лични податоци што се неопходни за секоја посебна цел на обработката. Оваа обврска се однесува на количеството собрани лични податоци, опсегот на нивната обработка, рокот на чување и нивната достапност. Воедно, оваа мерка треба да обезбеди дека интегрираните лични податоци без индивидуална интервенција нема да можат да бидат автоматски достапни за неограничен број на физички лица.

Следна новина со законот е проценката на влијанието на заштитата на личните податоци (или т.н. Data Protection Impact Assessment-ДПИА). Во овој контекст, Законот бара секогаш кога ќе се користи некоја нова технологија за кој било вид обработка на личните податоци, да се провери дали постои веројатност таа да предизвика висок ризик за правата и слободите на физичките лица. Затоа, пред да биде извршена обработката, контролорот треба да изврши проценка на влијанието на предвидените операции на обработката во однос на заштитата на личните податоци.

Законот во оваа насока предвидува обврски и кон надзорниот орган. Конкретно, Агенцијата за заштита на личните податоци има обврска да воспостави и јавно да објави листа на оние видови операции на обработка на податоците, за кои се бара контролорите задолжително да извршат проценка на влијанието на заштитата на личните податоци. Законодавецот обезбедува контрола на почитувањето на обврските за утврдување висок ризик при евентуална злоупотреба или повреда на приватноста преку ефект врз заштита на личните податоци, со тоа што контролорот секогаш ќе треба да се консултира со Агенцијата, пред обработката, ако резултатите од проценката на влијанието на заштитата на личните податоци покажат ризик. Исто така, како висок ризик се смета доколку контролорот не преземе мерки за ублажување на ризикот. Притоа, кога Агенцијата смета дека планираната обработка го прекршува Законот

за заштита на личните податоци, особено кога контролорот не го идентификувал или намалил ризикот во доволна мера, му дава мислење на контролорот или обработувачот или, пак, може да искористи друго овластување утврдено со закон.

Новина во Закон за заштита на личните податоци е и дополнителното зајакнување на улогата на офицерот за заштита на лични податоци – обврска што беше воведена со измените на претходните законски решенија во оваа област. Имено, контролорот и обработувачот треба секогаш да определат офицер за заштита на личните податоци. Законот дава можност група правни лица да можат да определат еден офицер за заштита на личните податоци, под услов офицерот да биде лесно достапен за секое правно лице. Дополнителна новина е должноста контролорот или обработувачот или здруженија и други тела што ги претставуваат категориите на контролори или обработувачи, исто така да определат офицер за заштита на личните податоци, кој може да ги извршува задачите за тоа здружение или друго тело што ги претставува контролорите и обработувачите. Новина е и можноста за тоа офицерот за заштита на личните податоци да ги извршува работите врз основа на договор за услуги без притоа да има заснован постојан работен однос кај контролорот или обработувачот.

Согласно законот, секоја организација во која има процес на обработка на податоци мора да ги почитува следните начела на обработка на податоци: законитост, правичност и транспарентност, ограничување на целите, минимален обем на податоци, точност, ограничување на рокот на чување, интегритет и доверливост и отчетност. Новиот закон исто така ја дефинира категоријата-поимот обработка на податоци во „голема мера“. Во таа насока утврдувањето на тоа дали обработката на личните податоци вклучува обработка што потпаѓа под категоријата што се класифицира како обработка на податоци од голема мера.

Следна новина во законот претставува поимот „редовно и систематско следење на субјектите на личните податоци“. Овој термин не е дефиниран во Законот, но ги вклучува сите форми на следење и профилирање на интернет, вклучувајќи ги и целите на рекламирањето базирано на однесувањето на корисникот (профилирање).

2.2.2. Заштита на приватноста преку интернет преку Законот за електронски комуникации

Во заштитата на приватноста преку интернет голема улога има Законот за електронски комуникации. Со оглед на тоа дека во претходната глава констатиравме оти загрозувањето на приватноста преку интернет во голема мерка зависи од безбедноста на информациско-комуникациските системи, на деловите што се однесуваат за безбедноста на комуникациите ќе им се посветиме подетално.

Во почетните одредби се наведува дека целта на овој закон, меѓу другото, е и заштита на правата на корисниците, вклучувајќи ги крајните корисници со инвалидитет и крајните корисници со посебни социјални потреби, односно обезбедување доверливост на комуникациите.[17] Од позначајните дефиниции и утврдување на поими поврзани со заштита на приватноста би ги издвоиле поимите „Услуги на информатичко општество“, „На далечина“, „Преку електронски средства“ и „На лично барање на примателот на услугата“. Поимот „Услуги на информатичко општество“ се дефинира или се однесува на услуги што се обезбедуваат за надоместок на далечина преку електронски средства и на лично барање на примателот на услугата. „На далечина“ означува дека услугата се обезбедува без истовремено присуство на две страни. „Преку електронски средства“ значи дека услугата се испраќа од почетната/изворната точка

17 Член 2 од Законот став 3 и 8.

и се добива на крајната дестинација преку електронска опрема за процесирање (вклучително и дигитална компресија) и чување податоци и се испраќа, пренесува и добива во целост преку кабел, радиобранови, оптички средства или други електромагнетни средства. „На лично барање на примателот на услугата" значи дека услугите се обезбедуваат преку пренос на податоци на лично барање.

Како надлежни органи во спроведувањето на одредбите од законот и со тоа обезбедување на комуникациите се Министерството за информатичко општество и администрација и Агенцијата за електронски комуникации. Со член 26-а од Законот за електронските комуникации, во состав на Агенцијата за електронски комуникации се формира посебна организациона единица – Национален центар за одговор на компјутерски инциденти (MKD-CIRT), која ќе претставува официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај мрежите и информациските системи и кој ќе идентификува и ќе обезбедува одговор на безбедносни инциденти и ризици.

Значаен сегмент во поглед на осигурување на приватноста преку интернет е содржан во поглавјето што се однесува на „Безбедност и интегритет на јавните електронски комуникациски мрежи и услуги и заштита на личните податоци".

Во делот што се однесува на безбедноста и интегритетот на јавните електронски комуникациски мрежи и услуги[18] се наведува дека операторите се должни да преземаат соодветни технички и организациони мерки со цел соодветно да управуваат со ризиците за безбедноста на мрежите и услугите. Имајќи го предвид техничкиот напредок, овие мерки треба да обезбедат ниво на безбедност соодветно на настанатиот ризик. Мерките, според законодавецот, особено треба да се преземаат за да се спречи и минимизира влијанието на безбедносните инциденти врз корисниците и меѓусебно поврзаните мрежи. Законодавецот лоцира обврски и за операторите на јавни електронски комуникациски мрежи. Во таа насока операторите на јавни електронски комуникациски мрежи треба да ги преземаат сите соодветни чекори за да го обезбедат интегритетот на нивните мрежи и истовремено, континуитетот на услугите што ги обезбедуваат со тие мрежи. Понатаму операторите на јавни електронски комуникациски мрежи или јавни електронски комуникациски услуги, согласно тоа што беше посочено во анализата во Глава – I, треба да усвојат и имплементираат политика за безбедност со која ќе се утврди ранливоста на системот, надзорот и спроведување превентивни и корективни мерки, како и мерки за ублажување на инциденти за безбедноста и интегритетот на мрежите.

Она што е особено значајно за загрозувањето на приватноста преку интернет е дека во случај на значителен ризик од повреда на безбедноста на мрежата, операторот на јавни електронски комуникациски услуги е должен да ги информира претплатниците за таквиот ризик и доколку е надвор од опсегот на мерки што ги презема операторот, да ги информира и за можните решенија за отстранување на ризикот, како и за можните трошоци за таквите решенија.

Агенцијата за електронски комуникации има значителна улога во заштитата на приватноста преку односот кон операторите и надлежностите што ги има во однос на нив. Агенцијата исто така има право да ги испита случаите на неусогласеност и нивните ефекти врз безбедноста и интегритетот на мрежите. Во овој контекст, особено е значаен делот за нарушување на безбедноста на личните податоци. Во случај на нарушување на безбедноста на личните податоци, операторот на јавни електронски комуникациски услуги, е должен веднаш, но не подоцна од 24 часа од моментот на утврдување на нарушувањето на безбедноста на личните податоци, да достави до Агенцијата за електронски комуникации и Дирекцијата за заштита на личните податоци (значи АЗЛП) известување за нарушување на безбедноста на личните податоци.

18 Членот 166 од Законот за електронски комуникации

Особено интересна сфера што се однесува на заштита на приватноста преку интернет претставува и регулирањето и постапувањето при „Небарани комуникации".[19] Во таа смисла законодавецот регулира дека користењето автоматско повикување и комуникациски системи за повикување на претплатнички телефонски броеви без човечка интервенција (автоматски машини за повикување, СМС, ММС), факс-апарати или електронска пошта, заради вршење директен маркетинг, може да биде дозволено само доколку претплатниците претходно се согласиле. Физички и правни лица може да ги користат електронските контакт-податоци за електронска пошта добиени од потрошувачите на нивните производи или услуги, за директен маркетинг и продажба само на нивни слични производи или услуги, под услов на тие потрошувачи да им обезбедат јасна и недвосмислена можност на бесплатен и едноставен начин да приговораат за таквото користење на електронските контакт-податоци при нивното добивање и при добивање на секоја порака, во случај кога потрошувачот однапред не го одбил таквото користење на електронски контакт-податоци.

2.2.3. Осврт на заштитата на приватноста преку интернет во Законот за кривична постапка, Кривичниот законик и Законот за следење на комуникациите

Иако за анализата и ризиците за приватноста веќе стана збор детално во Глава I, овде само би дополниле дека посебните истражни мерки-ПИМ, по својата природа, претставуваат смислено нарушување, покрај другото, и на приватноста како загарантирано право со Уставот и со меѓународните документи, која државните органи ја оправдуваат со потребата за остварување повисоки цели – заштита на општеството и граѓаните од тешки форми на криминал и ефикасна и успешна борба против него, односно заштита на националната безбедност. Напредокот на дигитализацијата и пролиферацијата на технологии за електронска комуникација најчесто преку интернет-просторот ја наметнува потребата од наоѓање баланс помеѓу заштитата на јавното добро и приватноста.

Во Кривичниот закон во кривичните дела против слободите и правата на човекот и граѓанинот е уредено кривичното дело: „Злоупотреба на лични податоци":

„Тој што спротивно на условите утврдени со закон без согласност на граѓанинот прибира, обработува или користи негови лични податоци, ќе се казни со парична казна или со затвор до една година. Со казна од став 1 се казнува тој што ќе навлезе во компјутерски информатички систем на лични податоци со намера користејќи ги за себе или за друг да оствари некаква корист или на друг да му нанесе некаква штета".

Со оглед на тоа што демнењето и следењето, но и облиците на психичко насилство кои се инкриминирани како кривично дело според Кривичниот законик вклучуваат значителни форми на нарушување на приватноста, во овој контекст е вредно да се спомене и уредувањето на оваа материја. Според Кривичниот законик, меѓу другото, „под насилство врз дете" се подразбира: и „психичко насилство, насилство преку интернет, врсничко насилство, како и демнење и следење на детето". Законодавецот притоа предвидел дека „тој што ќе изврши физичко, психичко или друг вид насилство спрема дете, ќе се казни со парична казна или со затвор од шест месеци до три години".

Имајќи го предвид погоре наведеното, како и можноста за врсничко насилство помеѓу деца под 14-годишна возраст, како дополнителни два закона кои треба да се земат предвид во контекст на предметната анализа се и Законот за правда на децата[20] и Законот за заштита на детето.[21]

19 Член 174 од Законот

20 Закон за правда на децата („Службен весник на Република Македонија" бр.148/2013 и „Службен весник на Република Северна Македонија" бр. 152/2019 и 275/2019)

21 Закон за заштита на децата („Службен весник на Република Македонија" бр. 23/2013, 12/2014, 44/2014, 144/2014, 10/2015, 25/2015, 150/2015, 192/2015, 27/2016, 163/2017, 21/2018 и 198/2018 и „Службен весник на Република Северна Македонија" бр. 104/2019, 146/2019, 275/2019, 311/2020 и 294/2021)

Достапноста на современите технологии (поради цената и пролиферацијата) во оваа смисла, со кои и други актери-не државни (приватни компании и лица) може да применат интрузивни методи за нарушување на приватноста, ги усложнува напорите за детално регулирање на приватноста преку интернет и ја наметнува потребата од вклучување други законски решенија и регулативи и нивно усогласување според начелото на уставност[22] и принципот lex specialis derogat legi generali.[23] На пример, производство, нудење на продажба, продажба, увоз, извоз, реекспорт или држење средства за следење на комуникациите не може да се врши без одобрение што го издава Министерството за внатрешни работи врз основа на поднесено писмено барање од правно лице, во прилог на кое е доставена техничка спецификација на видот и карактеристиките на средствата што можат да бидат наменети за следење на комуникациите.[24] Оттука, подзаконските акти и правилниците што ја регулираат работата на овие контролни органи, но и на регистрацијата на трговски друштва, на пример, исто така влегува во збирката на законски и подзаконски акти со кои се уредува приватноста општо, но и преку интернет посебно.

Законот за следење на комуникациите е новина што беше воведена по скандалот што ја стресе земјата со незаконско прислушкување. Значењето на овој закон за заштита на приватноста во ек на пролиферација на современи технологии со кои се нарушува приватноста преку интернет е голема. Во таа смисла, како основни начела на кои се градат законските решенија со овој закон се наведуваат: почитување на човековите слободи и права утврдени со Устав, закон и меѓународни договори ратификувани во согласност со Уставот на Република Северна Македонија и забрана за следење на комуникациите согласно со овој закон без судска наредба.[25]

Со законот детално се предвидува примена на „постапка за спроведување посебна истражна мерка“, преку следење на комуникациите, односно условите и постапката за спроведување мерки за следење на комуникациите заради заштита на интересите на безбедноста и одбраната на државата. Покрај другото, а во интерес на заштитата на приватноста преку интернет, законодавецот детално ги регулира постапките поврзани со следењето на комуникациите кога за тоа постои законска основа. Со законот исто така се регулираат и обврските и пристапот кон мета-податоците, но и спроведувањето на мерките за следење на комуникациите со посебни технички уреди и опрема. АЗЛП е надзорен орган за заштита на личните податоци.

22 Член 51 од Уставот на Република Северна Македонија со кој се предвидува супрематија на Уставот над другите законски решенија - закони и подзаконски акти.

23 Види повеќе во Trans-Lex „lex specialis derogat legi generali“, достапно на: https://www.trans-lex.org/910000/_/lex-specialis-principle/

24 Член 2 од Законот за следење на комуникациите

25 Член 3 од Законот за следење на комуникациите

Глава - III

Компаративна анализа на усогласеноста на заштитата на правото на приватноста преку интернет во Република Северна Македонија со европските и меѓународните стандарди

Деталната анализа на новиот Закон за заштита на личните податоци, споредено со Општата регулатива за заштита на податоците на Европската Унија – (понатаму ЕУ-регулатива) покажува дека Законот за заштита на личните податоци е адаптација на ЕУ-регулативата. Во овој дел анализата ќе се фокусира на компарација на европската регулатива и дел од меѓународната регулатива со постојната законска регулатива. Целта на ваквиот пристап е да се изврши споредба на усогласеноста на законските решенија за заштита на приватноста на интернет во Република Северна Македонија со Општата регулатива за заштита на податоците на Европската Унија, но и со Директивата за е-приватност на Унијата[26], односно идната Регулатива за е-приватност на ЕУ, која е пред усвојување. Најпрвин ќе биде посочена компаративна анализа помеѓу ЕУ-регулативата и македонските законски решенија. Потоа, за целосна анализа ќе биде направен краток преглед на заштитата на приватноста во дел од земјите членки на ЕУ. На крај во оваа глава анализата ќе направи краток преглед на заштитата на правото на приватност преку интернет со земјите од регионот.

3.1 Усогласеноста на македонското законодавство за заштита на приватноста преку интернет со Општата регулатива за заштита на податоците на ЕУ

На 27 април 2016 година Европскиот парламент и Советот на Европската Унија ја донесоа Регулативата (ЕУ) 2016/679 за заштита на физичките лица во однос на обработката на личните податоци и движењето на таквите податоци. Со носењето на оваа регулатива се укина Директивата 95/46/ЕК (Директивата 95/46/ЕК).[27] Споменувањето на оваа директива е битно во конкретниот контекст на анализата, бидејќи Законот за заштита на личните податоци од 2005[28] година беше продукт пресликан од оваа директива.

Носењето на новата регулатива, всушност, значеше отпочнување реформски процес во рамките на самата Унија. Со донесувањето на Регулативата се предвиде транзициски период од две години. Тоа значеше дека имплементацијата на Регулативата во Европската Унија ќе започне две години по донесувањето или попрецизно од 25 мај 2018 година.

Законот наложи контролорите и обработувачите на податоци да се усогласат со Законот до 24 август 2021 година. Дополнително, оваа обврска важеше и за компаниите и претпријатијата во која општат и дејствуваат контролорите и обработувачите. Во февруари 2022 година, Агенцијата за заштита на лични податоци (АЗЛП) ја усвои и методологијата за усогласување на ресорното законодавство со Законот за заштита на личните податоци.[29] Во методологијата се дадени насоки со кои се регулира постапувањето на министерствата во процесите на усогласување на ресорното законодавство. Овој процес, покрај другото, го опфаќа и ревидирањето на постојните законски решенија со цел ускладување со регулативата на ЕУ. Методологијата е подготвена во согласност со добрите практики и законодавството на Европската Унија и нејзините земји членки. Во таа насока, паралелно со донесувањето на законот, е воспоставен и процесот на вршење процена на влијанието на законите во однос на заштитата на личните податоци. Методологијата исто така содржи информации за процесите на претходна консултација со националниот орган за заштита на податоците, односно АЗЛП при подготовката на предлог-законите или соодветните подзаконски акти поврзани со обработка на лични податоци.

Компаративната анализа со претходниот Закон од 2005 година покажува дека новиот Закон од 2020 година има низа новини што се однесуваат на: нови дефиниции, нови дополнителни начела и принципи и нови обврски за контролорите и обработувачите.

26 EUR Lex, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Document 32002L0058, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

27 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Date of end of validity: 24/05/2018; Repealed by 32016R0679, достапно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

28 Законот за заштита на личните податоци („Службен весник на Република Македонија" број 7/2005 и 103/2008)

29 Методологија - цитирано

Во делот што следува компаративната анализа ќе се фокусира на техничките и организациските мерки што се новина, а со кои, всушност, Законот за заштита на личните податоци е целосно усогласен со Регулативата на ЕУ.

Во однос на примената на техничките и организациските мерки воведни се низа новини. Една од тие новини е техничката и интегрирана заштита на личните податоци, односно (data protection by design and by default). Оваа мерка се воведува како задолжителна за контролорите и обработувачите на личните податоци, согласно најновите технолошки достигнувања (a state-of-the-art technology), што како обврска бара техничките и организациските мерки секогаш да се преиспитуваат и ажурираат, на начин што ќе биде соодветен на времето во кое се дизајнираат и имплементираат. Со тоа, специфично за оваа мерка е што таа зема во предвид повеќе критериуми, како што се природата, обемот, контекстот и целите на обработката, но и ризиците со различна веројатност и сериозноста со која овие ризици вршат влијание или загрозување на правата и слободите на физичките лица.

„Приватноста по дифолт“ и „приватноста по дизајн“ се основни принципи наведени во Општата регулатива за заштита на податоците на Европската Унија (GDPR), а кои се имплементирани целосно и во Законот за заштита на личните податоци. Овие принципи имаат цел да ја подобрат заштитата на приватноста и личните податоци на поединците во дигиталната ера. Усогласеноста со овие принципи, според GDPR, е задолжителна за организациите што постапуваат со лични податоци на граѓани на ЕУ. Тоа бара од нив да ја земат предвид приватноста како основен аспект во текот на нивните операции и циклус на развој на производи.

Со имплементирање на овие принципи се влијае корективно врз работодавците да поттикнат култура што дава поголема заштита на приватноста, да дадат приоритет на приватноста на корисниците и да ги намалат ризиците од прекршување на податоците или злоупотреба, на крајот зголемувајќи ја довербата помеѓу поединците и организациите што ракуваат со нивните податоци.

Проценката на влијанието врз заштитата на податоците (ПВВЗП, доаѓа од Data Protection Impact Assessment-DPIA) е уште една клучна алатка наложена со Општата регулатива за заштита на податоците (GDPR) на Европската Унија, која е целосно имплементирана со законот. Овој принцип е дизајниран да им помогне на организациите/работодавачите да ги идентификуваат и минимизираат ризиците за приватноста на поединците преку проценка на потенцијалното влијание на операциите за обработка на личните податоци.

ПВВЗП вклучува систематска проценк, која се однесува на неопходноста, пропорционалноста и ризиците поврзани со обработката на личните податоци. Примената на овој принцип, како и во претходниот случај, е од особено значење кога постои голема веројатност дека од активноста на обработка на податоците ќе има висок ризик за правата и слободите на поединците.

Во склад со насоките на ЕУ-регулативата, и во нашето законодавство се воведени соодветни контролни механизми. Супервизијата над заштитата на личните податоци во таа смисла е креирана врз база на системски и независен пристап кон контрола над законитоста. Овој пристап притоа согласно законските решенија во Република Северна Македонија се однесува на преземените активности при обработката на личните податоци и нивната заштита во спроведувањето на Законот за заштита на личните податоци, но и прописите донесени врз основа на овој закон, што особено опфаќа истражување, проверка, давање насоки и превенција на контролорите и обработувачите.

Како орган задолжен за системската контрола е одредена АЗЛП. Во однос на традициите, би требало да се констатира и дека Агенцијата не е сосема ново тело. Имено, таа е наследник на поранешната Дирекција за заштита на личните податоци, која беше формирана како посебно правно лице уште со Законот од 2005 година. Уште тогаш Дирекцијата имаше за задача да врши надзор над законитоста на преземените активности при обработување лични податоци и на нивната заштита.

Со Законот за заштита на личните податоци од 2020 година Дирекцијата за заштита на лични податоци се трансформира во АЗЛП. Како и дирекцијата, и Агенцијата продолжи да дејствува како самостоен и независен државен орган, надлежен да врши надзор над законитоста на преземените активности при обработката на личните податоци на територијата на Република Северна Македонија, како и заштита на темелните права и слободи на физичките лица во однос на обработката на нивните лични податоци. Сходно со тоа, а во склад со насоките на ЕУ-регулативата, АЗЛП има надзорни, советодавни и корективни овластувања.

Покрај овластувањата и надлежностите на АЗЛП, македонскиот законодавец ги пропишал и задачите што овој државен орган треба да ги извршува. Една од тие законски обврски е и „да ја промовира јавната свест и согледувањето на ризиците, правилата, заштитните мерки и правата во однос на обработката на личните податоци, а особено на активностите што се насочени кон децата“.

Во пракса корективната и контролната функција на АЗЛП, на пример, може да ја погледнеме во однос на обработката на податоци. Во случај кога АЗЛП смета дека планираната обработка на податоци го прекршува Законот за заштита на личните податоци, особено кога контролорот не го идентификувал или намалил ризикот во доволна мера, му дава мислење на контролорот или обработувачот, при што може да користи и кое било од своите овластувања утврдени со закон.

Друг пример за улогата на АЗЛП во пракса претставува должноста за известување за нарушувањето на безбедноста на личните податоци. Согласно ЕУ-регулативата, а и Законот за заштита на лични податоци, известувањето или т.н. „Data breach notification“се доставува до АЗЛП и до субјектите на личните податоци.

Сумарно, би рекле дека усогласеноста на Законот со ЕУ-регулативата може да се демонстрира преку:

- Прописите за примената на технички и организациски мерки со кои се обезбедува ниво на безбедност соодветно на ризикот, вклучувајќи ги тука и техничката и интегрирана заштита на личните податоци;

  - ↘ Соодветни политики за заштита на личните податоци;
  - ↘ Развој и почитување на одобрените кодекси на однесување;
  - ↘ Почитување на одобрените механизми за сертификација;
  - ↘ Документирање на сите нарушувања на безбедноста на личните податоци;
  - ↘ Проценка на влијанието на заштитата на личните податоци;
  - ↘ Определувањето и положбата на офицерот за заштита на личните податоци.

Покрај усогласеноста со општата ЕУ-регулатива, друг значаен сегмент за проценка на заштита на приватноста преку интернет во споредба со законодавството на Унијата е и директивата на ЕУ за е-приватност.[30]

30 EUR-Lex Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Document 52017PC0010 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017PC0010

Сепак, во последниот извештај на ЕУ од 2023 година се наведува дека во однос на заштитата на личните податоци, потребно е целосно усогласување со Општата регулатива за заштита на податоците. Области што бараат усогласување се: пренос на лични податоци; независноста на Агенцијата за заштита на личните податоци (АЗЛП); застарени делови од старите национални закони, кои треба да се укинат. Дополнително, согласно Извештајот, постои потреба и од усогласување на законодавството со ЕУ-директивата за примена на правото, која се однесува на полициската работа и заштита на личните податоци. Оваа директива опфаќа области што не се опфатени со Општата регулатива на ЕУ за заштита на податоците. Режимот за ЕУ-директивата за извршување на законот се применува само во случаи кога контролорот на податоците е „надлежен орган“, а обработката се врши за „цели за спроведување на законот“. Извештајот, сепак, ја нотира посветеноста на АЗЛП за поднесените измени на Законот за заштита на личните податоци. Но, во Извештајот се наведува и дека Земјата треба да усвои национално законодавство во согласност со Директивата на ЕУ за спроведување на законот.

3.2 Осврт на ЕУ-директивата за е-приватност и усогласеноста на македонското законодавство за заштита на приватноста преку интернет

Директивата за е-приватност во смисла на оваа анализа се однесува на ЕУ-директивата 2002/58/ЕЗ за приватност и електронски комуникации, изменета со ЕУ-директивата 2009/136/ЕЗ.

Директивата за е-приватност ја дополнува ЕУ-регулативата и поставува конкретни правила во врска со директните маркетинг-комуникации и поставувањето колачиња и слични идентификатори во опремата на корисниците (компјутери, лаптопи, паметни телефони и други уреди). Дополнително, Директивата за е-приватност поставува конкретни правила за давателите на електронски комуникациски услуги кога обезбедуваат електронски комуникациски услуги (ЕКС). Од влегувањето во сила на Европскиот кодекс за електронски комуникации на крајот на 2021 година, ЕКС ги вклучува не само традиционалните комуникациски услуги, како што се мобилната телефонија и пристапот до интернет, туку и:

- апликациите за инстант-пораки,
- Voice over IP (VoIP),
- веб-услуги за е-пошта базирани на е-пошта
- видеоконференции (често во буквален превод се нарекуваат комуникациски услуги преку врвот или скратено се користи OTT).

Со оглед на тоа што ЕУ-директивата за е-приватност не е регулатива на ЕУ, таа не е директно применлива. Ова значи дека земјите членки мора да ги транспонираат правилата на ЕУ за е-приватност во националното законодавство. Тоа само по себе резултира со некои варијации помеѓу законите за е-приватност на земјите членки на ЕУ.

Главните обврски што ЕУ-директивата за е-приватност ги генерира се однесуваат на директен маркетинг, користење и примена на е-колачиња (понатаму: колачиња) и на електронски комуникациски услуги-ЕКС.

Во однос на директниот маркетинг, Директивата за е-приватност ги поставува правилата за испраќање директни маркетинг комуникации (е-пошта, СМС, маркетинг-повици). Директивата генерално забранува употреба на автоматски системи за повици и комуникации (без човечка интервенција) и е-пошта за директен маркетинг, освен ако корисникот (или претплатникот) дал согласност. Согласноста на корисникот во пракса има тенденција да се добива преку одјавување. „Одлучете“ значи дека лицето треба да преземе специфичен позитивен чекор. Во

пракса, на пример, тоа би значело „штиклирајте поле“, „испратете е-пошта“ или „кликнете на копче“ за корисникот да изрази согласност дека сака да добива информации поврзани со маркетинг. Паралелно на тоа има опција „да се откаже“, што би значело дека лицето мора да преземе позитивен чекор за да одбие или да се откаже од маркетингот.

Како исклучок од правилото да се одлучат, Директивата им дозволува на компаниите и организациите да испраќаат директни маркетинг-мејлови до постојните клиенти без нивна согласност, под услов таквата е-пошта да продава слични производи или услуги на таа компанија или организација и на клиентот да му е понуден избор да се откаже од таквите комуникации. Тоа што, сепак, треба да се има на ум е дека, иако Општата регулатива за заштита на податоците на ЕУ наведува дека „обработката на лични податоци за цели на директен маркетинг може да се смета за легитимен интерес“, Регулативата за е-приватност, како „lex specialis“ на Општата регулатива, ќе ја отфрли оваа можност, па ако конечната верзија бара согласност, легитимните интереси нема да важат за директен маркетинг, иако во Општата регулатива (која е во сила) се вели дека се дозволени.

Крајните корисници исто така ќе имаат апсолутно право на приговор, во тој случај мора да престанете да им продавате што е можно поскоро, но секако во рок од еден месец. Исто така, мора да ги информирате за тоа право и за фактот дека имате намера да ги користите нивните податоци за цели на директен маркетинг.

Кога станува збор за користење на т.н. колачиња, Директивата за е-приватност бара од земјите на ЕУ да се погрижат корисниците да ја дадат својата согласност пред какви било информации, како што се колачиња и слични технологии, да бидат складирани или пристапени во нивните компјутери, паметни телефони или други уреди поврзани на интернет. Во однос на оваа насока, постојат одредени ситуации кога се можни исклучоци, но само ако се законски регулирани.

Во однос на електронските комуникациски услуги-ЕКС, Директивата за е-приватност, исто така, воспоставува правила за доверливост на електронските комуникации и дозволената употреба на сообраќајни податоци, рутирачки податоци и податоци за локација (метаподатоци за електронски комуникации) од давателите на електронски комуникациски услуги.

ЕУ-директивата, покрај другото, содржи упатства и за утврдување на надлежните национални органи на ЕУ и санкции. Во однос на утврдувањето на надлежни национални органи, Директивата за е-приватност им остави на земјите-членки на ЕУ да го назначат органот задолжен за спроведувањето на правилата за е-приватност на национално ниво. Со оглед на правната рамка што ја воспоставува директивата (значи не е регулатива), ваквата насока во пракса резултира со недостаток на усогласеност на ова упатство/насока низ Унијата.

Во некои земји на ЕУ, како и кај нас на пример, постојат неколку надлежни органи што покриваат различни области поврзани со заштитата на приватноста. Тоа во пракса значи, дека дел од органите се надлежни за спроведување на различен дел од правилата за е-приватност (на пр. орган за заштита на податоци надлежен за спроведување на правилата за колачиња, но национален телеком регулатор надлежен за спроведување на правилата во врска со услугите за електронска комуникација). Оваа разновидност на надлежни органи на национално ниво е илустрирана со списокот објавен од Комисијата на ЕУ.

Во однос на примената на санкциите, спротивно на Општата регулатива за заштита на личните податоци, Директивата за е-приватност не предвидува никаков степен или износ на

казни или санкции. Во неа само се укажува дека тие мора да бидат ефективни, пропорционални и разубедувачки. Како резултат на тоа, износот на максималните казни варира од една земја членка на ЕУ до друга.

Македонската законска реалност е усогласена со оваа директива. Иако терминот колачиња директно не се спомнува во Законот за електронски комуникации, во однос на политиката за користење на колачиња законодавецот предвидел законска основа за користење на колачињата - како опција за собирање и обработка на податоците. Изразувањето согласност е единствената можна правна основа за обработка на лични податоци во контекст на колачиња. Тоа, како што и претходно објаснивме во Главата II, е уредено во делот „Безбедност и интегритет на јавните електронски комуникациски мрежи и услуги и заштита на личните податоци“ (конкретно членот 168) од Законот за електронски комуникации.

Сепак, мора да се укаже дека постои и исклучок за колачиња што не се опфатени со оваа мерка, а кои се технички неопходни. Техничките (задолжителните) колачиња се секогаш активни. Тие се неопходни за функционирањето на интернет-страницата и не смеат да бидат исклучени во системите. Субјектите на лични податоци може да бидат информирани за обработката на лични податоци преку колачиња како дел од политиката/изјавата за приватност на контролорот. Покрај согласноста, македонскиот законодавец регулирал и дека контролорот мора претходно да обезбеди јасни информации за субјектот на лични податоци согласно членовите 17 и 18 од Законот за заштита на личните податоци.

Потребата за унапредување на заштитата на приватноста преку интерет во рамките на ЕУ беше согледана паралелено со потребата за донесување на општата ЕУ-регулатива за заштита на личните податоци. Во 2017 година, Комисијата на ЕУ предложи нови правила за е-приватност преку нацрт-предлог за Регулатива за приватност и електронски комуникации (понатаму: Регулатива за е-приватност). Откако ќе се усвои, Регулативата за е-приватност ќе ги замени сегашните правила за е-приватност.

Со тоа, несомнено е дека во рамките на Унијата постои свест за потребата од подетално, но и посериозно регулирање на заштитата на приватноста преку интернет vis-a- vis современите текови и можности за нарушување на приватноста преку интернет, на што конкретно ќе се посветиме во следната, глава IV. Иако текстот на Регулативата сè уште не е конечен, подолу накратко е даден главен преглед на тоа што е суштински новитет со нацрт-содржината, која е пред усвојување.

3.3 Краток осврт на Нацрт-регулативата за е-приватност на ЕУ

Европската регулатива за е-приватност ќе претставува важен, условно кажано, амандман - унапредување на постојната директива за е-приватност од 2002 година. Ова надградување е потребно со цел да се следи текот на унапредувањето на новите технологии и нивната примена во пазарни достигања. Тоа во пракса ги вклучува сегашната широка употреба на Voice over IP, услуги за е-пошта и пораки базирани на веб, и појавата на нови техники за следење на онлајн-однесувањето на корисниците.

Европската регулатива за е-приватност во таа смисла е замислена да биде *lex specialis* на Општата регулатива за заштита на податоци на ЕУ.[31]

На 10 февруари 2021 година, Советот на Унијата го усогласи својот став за правилата за е-приватност. Во таа смисла, земјите членки на ЕУ се согласија за преговарачки мандат за ревидирани правила за заштита на приватноста и доверливоста при користењето на

31 ЕУ ја прифаќа правната доктрина „lex specialis derogat legi generali“ (посебен закон ги надминува законите што ги регулираат општите работи). Како што претходно објаснивме Lex specialis е латинска фраза што значи „закон што регулира одредена специфична материја во однос на некоја поопшта материја“. Во таа смисла ако заштитата на личните податоци е општа материја, заштитата на приватноста преку интернет или во онлајн-просторот е конкретна/специфична материја.

електронските комуникациски услуги. Овие ажурирани правила за „ePrivacy“ ќе дефинираат случаи во кои на давателите на услуги им е дозволено да обработуваат податоци за електронски комуникации или да имаат пристап до податоците складирани на уредите на крајните корисници. Следниот чекор, согласно ЕУ процедуралните правила, се разговорите со Европскиот парламент за усогласување на финалниот текст.

Според мандатот на Советот, регулативата ќе ги опфати електронските комуникациски содржини што се пренесуваат со користење на јавно достапни услуги и мрежи, како и метаподатоци поврзани со комуникацијата. Метаподатоците вклучуваат, на пример, информации за локацијата, времето и примачот на комуникацијата. Се смета за потенцијално исто толку чувствителен колку и содржината.

Разбирањето на Европската регулатива за е-приватност е од особена важност за примената на приватноста преку интернет во Република Северна Македонија. Содржината на електронските комуникации може да открие многу чувствителни информации за физичките лица вклучени во комуникацијата, од лични искуства и емоции до медицински состојби, сексуални преференции и политички ставови, чиешто откривање може да резултира со лична и социјална штета, економска загуба или непријатност.

Слично на тоа, метаподатоците добиени од електронските комуникации може исто така да откријат многу чувствителни и лични информации. Овие метаподатоци ги вклучуваат повиканите броеви, посетените веб-локации, географската локација, времето, датумот и времетраењето кога поединецот се јавил итн., што овозможува да се извлечат прецизни заклучоци во врска со приватниот живот на лицата вклучени во електронската комуникација. На пример, тоа се однесува на социјалните односи на корисниците, нивните навики и активности во секојдневниот живот, нивните интереси, вкусови итн.

Комплементарноста на текстот на Предлог-регулативата за е-приватност на ЕУ со Општата регулатива за заштитата на податоците е голема. Во таа смисла, доколку со нацрт-предлогот на регулативата за е-приватност на ЕУ не се воспоставени конкретни правила, Општата регулатива за заштитата на податоците треба да се применува на секоја обработка на податоци што се квалификуваат како лични податоци. Од друга страна, одредбите на Нацрт-регулативата за е-приватност ја дополнуваат Општата регулатива за заштитата на податоците со тоа што поставуваат правила во врска со теми што не се во нејзиниот опсег, како што е заштитата на правата на крајните корисници кои се правни лица.

Се очекува Регулативата за е-приватност да воспостави идентичен режим на казни како Општата регулатива на ЕУ, што во пракса би значело максимални казни од 20 милиони евра (околу 17,5 милиони евра) или 4% од глобалниот годишен обрт на организацијата. Во тој контекст, крајните корисници што трпат „материјална или нематеријална штета“ поради прекршување на Регулативата за е-приватност, исто така, имаат право да добијат компензација од прекршителот.

3.4 Преглед на усогласеноста на заштитата на приватноста преку интернет во Република Северна Македонија со меѓународните стандарди и упатства од релевантни меѓународни организации кои се однесуваат на заштита на приватноста и човековите права

Меѓународните стандарди и принципи што се поврзани со заштита на приватноста својата правна заснованост ја имаат во универзалните документи за заштита на човековите права, кои имаат статус на *ius coegens* норми или општи принципи на правото со општа примена. Тоа во пракса, наједноставно кажано, значи дека без разлика дали некоја држава или организирана форма на власт ги потпишала овие принципи или не, тие имаат примена на територијата на државите, а органите се должни да ги почитуваат.

Правото на приватност е регулирано и во Универзалната декларација за човекови права (во член 12)[32], како и во Меѓународниот пакт за граѓански и политички слободи и права (член 17)[33]. И во двата члена се наведува дека „*никој нема да биде изложен на произволно вмешување во приватниот живот, семејството, домот и никој не смее да биде изложен на произволно мешање во приватниот живот, семејството, домот или преписката, ниту на напади врз честа и угледот. Секој има право на заштита од законот против вакво мешање или напад*“.

Од доменот на глобалните меѓународни документи што се однесуваат на заштита на приватноста би требало да се спомене и Резолуцијата 68/167 на Генералното собрание на ОН.[34] Правото на приватност, според некои видувања, е значајно за реализацијата на правото на слобода на изразувањето, соопштување на сопственото мислење без мешање, што претставува едно од начелата на кои се темели демократското општество.[35] Иако обезбедува ограничени нормативни насоки, оваа понова резолуција на Генералното собрание на ООН сигнализира и обновен меѓународен интерес за човековото право на приватност, како и посветеност на институциите на Обединетите нации (ОН) да го истражат значењето на ова право во дигиталната ера.

Значаен меѓународен документ кој е имплементиран во македонското законодавство, а генерира обврски за заштита на приватноста на интернет, е и Конвенцијата за правото на детето од 1989 г.[36] Конвенцијата за правата на детето е најуниверзално прифатениот инструмент за човекови права. Тој е ратификуван од секоја земја во светот освен две. Конвенцијата го вклучува целиот опсег на човекови права - граѓански, политички, економски, социјални и културни права - на децата во еден единствен документ. Конвенцијата во 41 член ги наведува човековите права што треба да се почитуваат и штитат за секое дете на возраст под осумнаесет години. Покрај другото, оваа конвенција во членот 16 предвидува дека „ниту едно дете нема да биде подложено на произволно или незаконско мешање во неговата/нејзината приватност, семејство, дом или кореспонденција; детето треба да биде заштитено од незаконски напади на неговата чест и углед”.

32 United Nations, “Universal Declaration of Human Rights” proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A), член 12, достапно на: https://www.un.org/en/about-us/universal-declaration-of-human-rights

33 United Nations, “International Covenant on Civil and Political Rights”, 16 December 1966, General Assembly resolution 2200A (XXI), Entry into force: 23 March 1976, in accordance with Article 49, достапно на: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

34 UN, General Assembly. Resolution 68/167. The right to privacy in the digital age. A/RES/68/167. 18 December 2013. https://undocs.org/en/A/RES/68/167

35 UN, General Ass Anupam Chander and Molly Land, (January 20, 2017), United Nations General Assembly Resolution on the Right to Privacy in the Digital Age, Cambridge University Press, https://www.cambridge.org/core/journals/international-legal-materials/article/abs/united-nations-general-assembly-resolution-on-the-right-to-privacy-in-the-digital-age/136942F57940B12E0733852518E4B68C embly. Resolution 68/167. The right to privacy in the digital age. A/RES/68/167. 18 December 2013. https://undocs.org/en/A/RES/68/167

36 Конвенцијата беше усвоена од Генералното собрание на ОН на 20 ноември 1989 година и стапи во сила во септември 1990 година. Види повеќе на: Convention on the Rights of the Child, достапно на: https://www.coe.int/en/web/compass/convention-on-the-rights-of-the-child#:~:text=The%20Convention%20was%20adopted%20by,the%20age%20of%20eighteen%20years.

Од универзалните документи што имаат релевантност за македонското законодавство се и Упатствата (насоките) на Генералното собрание на ООН за регулирање на компјутеризираните датотеки со лични податоци од 1990 г.[37] Овие упатства ја одразуваат посветеноста на заштитата на приватноста и личните податоци во контекст на новите технологии, особено компјутеризираната обработка на податоци. Тие обезбедуваат рамка за националните законодавства и меѓународната соработка во справувањето со предизвиците што ги носи собирањето и обработката на личните податоци во компјутеризираните системи. Принципите што се дадени во овие упатства се целосно прифатени од страна на ЕУ, а со тоа се имплементирани и во македонското законодавство.

Следна инстанција во однос на релевантноста на македонската регулатива кои имаат примена во заштитата на приватноста преку интернет и се во склад со законската, и уставна обврска (во корелација со членот 118 од Уставот),[38] се документите на Советот на Европа како регионални инструменти. Како и ООН, 47-те земји членки на Советот на Европа имаат пропишано меѓународно правни инструменти што имаат цел да ја унапредат заштитата на приватноста како дел од поширокаta посветеност за соработка и заштита на основните слободи и човекови права.

Европска конвенција за човекови права[39] во член 8 налага дека секој човек има право на почитување на неговиот приватен и семеен живот, домот и преписката. Никој, дури ниту државните органи притоа, не смее да се меша во остварувањето на ова право. Дерогација на ова право, сепак, постои, како во однос на правото на другите така и во однос на јавното добро. Во таа смисла, прекршувањето на ова право е можно ако потребата од мешање (нарушување) на приватноста е предвидена со закон и ако претставува мерка што е во интерес на државната и јавната безбедност, економската благосостојба на земјата, заштитата на поредокот и спречувањето на кривични дела, заштитата на здравјето и моралот или заштитата на правата и слободите на другите, во едно демократско општество.

Паралелно на ова, напорите на Советот на Европа се значајни и затоа што првиот правно обврзувачки меѓународен инструмент во областа на заштитата на податоците е донесен токму од оваа институција. Конвенцијата за заштита на поединци од аспект на автоматските обработки на личните податоци (позната како Конвенција бр. 108, или CETS бр.108) на Советот на Европа беше отворена за потпишување на 28 јануари 1981 година. Визионерството на оваа конвенција се огледува во фактот што основните принципи содржани во Конвенцијата 108 успеаја да одолеат на тестот на времето поради својот неутрално технолошки пристап.

Сепак, во 2018 година, Советот на Европа сметаше дека е неопходно дел од овие принципи да бидат модернизирани и адаптирани на новата дигитална реалност, но и да бидат регулирани делови што бараат поспецифично дообјаснување или прецизирање заради поголема заштита. Во таа насока беше донесен Протоколот за измените и дополнувањата на Конвенцијата 108 (CETS бр. 223), кој е отворен за потпишување на 10 октомври 2018 година. Намерата за донесување на Протоколот 223 е да ги реафирмира основните принципи на Конвенцијата 108, да зајакне дел од нив, но и да утврди нови заштитни мерки. Овие мерки, според креаторите, треба да се применуваат во новата реалност на онлајн-светот, како и да ја зајакнат потребата од промоција на добро владеење во услови на дигитализација. Како резултат на овие заложби беа донесени нови принципи во областа, како што се принципите на транспарентност, пропорционалност, одговорност, минимизирање на податоците, приватност по дизајн итн. Овие принципи со Протоколот сега се признати како клучни елементи на механизмот за заштита на приватноста преку интернет.

37 Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990, достапно на: https://www.refworld.org/pdfid/3ddcafaac.pdf

38 Според членот 118 од македонскиот Устав - Меѓународните договори што се ратификувани во согласност со Уставот се дел од внатрешниот правен поредок и не можат да се менуваат со закон.

39 Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, широко позната и како European Convention on Human Rights, Rome, 4.XI.1950 достапно на: https://www.echr.coe.int/documents/d/echr/convention_eng

Имајќи ги предвид новите предизвици за заштита на лицата во однос на обработката на личните податоци, како и фактот дека целта на модернизацијата што се врши со Протоколот е што подобро да се реагира на предизвиците во областа на приватноста што произлегуваат од зголемената употреба на новите информациско/информатички технологии и глобализацијата во однос на обработката на личните податоци, Министерството за правда во 2019 година оцени дека е целисходно и од интерес за Република Северна Македонија да се пристапи кон потпишувањето на Протоколот за измена на Конвенцијата за заштита на лица во однос на автоматска обработка на лични податоци (CETS 223).[40]

Со тоа, Република Северна Македонија стана 37 земја потписничка на протоколот со кој се врши модернизација на Конвенцијата за заштита на лица во однос на автоматска обработка на лични податоци (ETS 108) и на Дополнителниот протокол кон Конвенцијата за заштита на поединците во поглед на автоматска обработка на лични податоци, во врска со надзорните тела и прекуграничниот пренос на податоци (ETS No.181), како и зајакнување на нивната примена. Сепак, треба да се напомене дека до моментот на пишувањето на оваа анализа протоколот не е ратификуван.[41]

3.5 Краток преглед на некои добри практики за примена на правото на приватност во дел од земјите членки на Европската Унија со посебен осврт на заштитата на приватноста преку интернет

Примената на правото на приватност генерално и преку интернет зазема централно место во заштитата на индивидуалните права на граѓаните на земјите членки на Унијата. Иако главната цел на ЕУ-регулативата е да го усогласи законот за заштита на податоците низ ЕУ, дел од земјите членки на ЕУ имаат воведено дополнителни или поспецификни правила во одредени области. Преку тоа овие земји демонстрираат широка посветеност на заштита на индивидуалните права преку промоција, почитување и заштита на индивидуалните права, а со тоа и правото на приватност преку интернет, како дел од корпусот на човекови права.

Зголемена заштита, поголема од таа што се предвидува со ЕУ-регулативата, на пример, кај дел од земјите членки на Унијата, е евидентна во неколку области. Тоа, меѓу другото вклучува ситуации кога обработката вклучува здравствени податоци, генетски податоци, биометриски податоци, податоци за вработени или национални идентификациски броеви, или ако обработката на лични податоци служи за архивирање, научни, историски истражувања или статистички цели.

Германскиот сојузен закон за заштита на податоците (како што е ревидиран во 2019 година), на пример, бара од бизнисите да назначат ДПО доколку трајно ангажираат најмалку 20 лица во обработката на податоците, ако вршат активности за обработка на податоци што се предмет на проценка на импактот на ПВВЗП или ако комерцијално обработуваат лични податоци за цели на истражување на пазарот. Земјите членки на ЕУ може да предвидат и правила за обработка на лични податоци на починати лица. Францускиот Закон за заштита на податоците, ажуриран на 21 јуни 2018 година, на пример, вклучува такви правила, со тоа што на поединците им дава право да го дефинираат начинот на кој нивните лични податоци ќе се обработуваат по нивната смрт, покрај правата предвидени со ЕУ-регулативата. Во контекст на онлајн-услугите наменети за деца, ЕУ-регулативата бара родителска согласност за деца под 16-годишна возраст, но законот на земјите членки на ЕУ може да пропише пониска старосна граница, под услов таа да не е пониска од возраста 13. Оваа граница е намалена до 13-годишна возраст, на пример, во белгискиот Закон за заштита на податоците и до 14-годишна возраст во австрискиот закон

40 Министерство за правда, 6.12.2019, „Дескоска на средба со генералниот секретар на Советот на Европа: Потпишан Протокол за Конвенцијата за заштита на лица во однос на автоматска обработка на лични податоци"

41 Збирка на меѓународни договори, (ажурирано во август 2023), достапно и пристапено на 14 јануари, 2023) на https://www.caa.gov.mk/wp-content/uploads/2023/08/%25D0%25A1%25D0%25BE%25D0%25B4%25D1%2580%25D0%25B6%25D0%25B8%25D0%25BD%25D0%25B0-%25D0%25BD%25D0%25B0-%25D0%2597%25D0%25B1%25D0%25B8%25D1%2580%25D0%25BA%25D0%25B0-%25D0%25BD%25D0%25B0-%25D0%25BC%25D0%25B5%25D1%2593%25D1%2583%25D0%25BD%25D0%25B0%25D1%2580%25D0%25BE%25D0%25B4%25D0%25BD%25D0%25B8-%25D0%25B4%25D0%25BE%25D0%25B3%25D0%25BE%25D0%25B2%25D0%25BE%25D1%2580%25D0%25B8_2.pdf

за дополнување за заштита на податоците од 2018 година. Во Словенија Законот за заштита на податоците, кој стапи во сила на 26 јануари 2023 година, предвидува слични законски решенија со кои се даваат построги критериуми за заштита на личните податоци, вклучително и правото на приватност преку интернет. Ова создава дополнителни слоеви на сложеност за бизнисите, кои треба внимателно да ги следат овие случувања во релевантните земји членки и да го проценат територијалниот опсег на специфичните национални правила таму каде што е применливо.

3.5.1. Краток преглед на заштитата на правото на приватност преку интернет во Германија

Германија, според многу анализи, е лидер во регулативите за заштита на податоците и приватноста, особено со спроведувањето на Општата регулатива за заштита на податоците на ниво на Европската Унија. Во овој краток приказ ќе се осврнеме на правната рамка за заштита на приватноста, генерално и преку интернет посебно, органите за заштита на приватноста, почитувањето на клучните принципи (на кои се осврнавме во различните меѓународни документи), правата на германските граѓани како субјекти на податоци, регулирањето на согласноста за обработка на податоци, безбедноста на податоците, прекуграничниот пренос на податоци и на проценката на влијанието врз заштитата на податоците (ПВВЗП).

Германија се придржува до Општата регулатива на ЕУ за заштита на податоците. Сходно со тоа германскиот законодавец поставува правила за обработка на лични податоци и им дава на поединците поголема контрола врз нивните лични информации. Сепак, во однос на дигиталната приватност има и одредени други специфични закони кои се lex specialis на општата законска рамка за заштита на податоците.

Во Германија функцијата на орган за заштита на личните податоци ја остварува Сојузен комесар за заштита на податоци и слобода на информации (BfDI). Овој орган е одговорен за обезбедување усогласеност со законите за заштита на податоците на сојузно ниво. Дополнително, секоја германска покраина има свој орган за заштита на податоците.

Законодавецот предвидел дека податоците може да се собираат за одредени, експлицитни и легитимни цели и да не се обработуваат понатаму на начин што не е во согласност со тие цели. Во таа насока во Германија законодавецот наложува минимизирање на собирањето на податоците. Тоа во пракса значи дека собирањето податоци кога тоа е возможно мора да биде фокусирано само на потребните податоци. Понатаму собраните податоци може да се користат исклучиво за наменетата цел.

Согласно важечките прописи во Германија, граѓаните имаат право на пристап до нивните податоци, отстранување на неточните податоци, бришење на податоците под одредени услови, ограничување на обработката на нивните податоци и право што строго ја регулира преносливоста на податоците. Согласноста е клучен аспект на обработката на податоците. Компаниите мора да добијат јасна и експлицитна согласност од поединци пред да ги собираат и обработуваат нивните лични податоци.

Од компаниите се бара да спроведат соодветни технички и организациски мерки за да обезбедат ниво на безбедност соодветно на ризикот од обработка на податоците. Овие насоки, покрај со Општата регулатива за заштита на податоците на ЕУ, се прецизирани и со Директивата за е-приватност, но и насоките на ОЕЦД прифатени од ЕНИСА.

Германскиот законодавец наложува пријавување на одредени видови прекршувања на податоците до релевантниот орган за заштита на податоците во рок од 72 часа откако ќе се дознае за прекршувањето, освен ако не е веројатно дека прекршувањето ќе резултира со ризик за поединци. Компаниите треба да се погрижат кога пренесуваат податоци преку границите, да се усогласат со одредбите на GDPR поврзани со меѓународниот пренос на податоци, како што е употребата на стандардни договорни клаузули.

Законодавецот во Германија налага организациите да мора да спроведат ПВВЗП за активности за обработка што би можеле да резултираат со висок ризик за правата и слободите на германските граѓани. Во оваа насока германските закони налагаат одговорност и добро управување со податоците. Организациите имаат обврска да водат евиденција за активностите за обработка и, во предвидените случаи, да вршат ревизии за заштита на податоците.

Неусогласеноста со законските решенија, тоа значи и со Општата регулатива за заштита на податоците на ЕУ, може да резултира со значителни казни. Согласно Регулативата на ЕУ, и германското законодавство дозволува казни до 4% од годишниот глобален промет на една компанија или 20 милиони евра, кое и да е повисоко.

Службеници за заштита на корпоративни податоци (DPO): од одредени организации се бара да назначат службеник за заштита на податоци за да го надгледува усогласувањето со прописите за заштита на податоците.

3.5.2. Краток преглед на заштитата на правото на приватност преку интернет во Хрватска[42]

Од 25 мај 2018 година, главниот концепт на заштита на приватноста во Република Хрватска е регулиран со Општата регулатива за заштита на податоците на ЕУ и Акт за спроведување на Општата регулатива за заштита на податоците од 2018 година.[43] Врз основа на тоа е донесен и Законот за заштита на личните податоци (Zakon o zaštiti osobnih podataka)[44], кој, всушност, претставува нов и посилен механизам за заштита на личните податоци. Иако повеќето одредби и правила за заштита на податоците се наоѓаат во општата регулатива на ЕУ и Законот, постојат и други национални статути и подзаконски акти што пропишуваат специфични правила за обработка и употреба на податоците.

Уставот во Хрватска ја утврдува заштитата на личните податоци како основно право. Сепак, имплементацијата и понатамошниот развој на законодавството за заштита на личните податоци недостасувале сè до 2003 година, кога хрватскиот парламент, под влијание на Директивата 95/46/ЕЗ и Договорот 108 на Советот на Европа (двата документа обработени погоре), го усвои Законот за заштита на личните податоци, со кој се воспостави Хрватската агенција за заштита на податоците и до 2018 година го претставуваше општиот фундаментален рамковен закон со кој се регулира областа на заштитата на податоците во земјата.

Откако Хрватска стана членка на ЕУ, на 1 јули 2013 година, acquis communautaire на ЕУ, исто така, стана дел од хрватскиот правен систем. Во контекст на заштитата на правото на приватност генерално и преку интернет посебно, особено важна е Повелбата за фундаменталните права на Европската Унија (Повелбата), која ја предвидува заштитата на личните податоци како основно право, затоа пропишува дека личните податоци може да се обработуваат само ако „правично се обработуваат за одредени цели и врз основа на согласност на засегнатото лице или некоја друга легитимна основа утврдена со закон“. Покрај тоа, како основни права

42 Придонес кон овој дел има правната компанија „Лукина и партнерите од Хрватска“, добар дел од нивните трудови може да се најдат на https://www.lexology.com/firms/24422

43 Hrvatski Sabor, 2018, „Odluku O Proglašenju Zakona O Provedbi Opće Uredbe O Zaštiti Podataka“, достапна на: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html

44 Hrvatski Sabor, 2018, „Odluku O Proglašenju Zakona O Provedbi Opće Uredbe O Zaštiti Podataka“, достапно на: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html

Повелбата ги предвидува правото на пристап и правото на исправка на сопствените лични податоци, како дополнение на обврската независен орган да го надгледува почитувањето на правилата за заштита на податоците. Во мај 2016 година, она што е познато како пакет за заштита на податоците на ЕУ, односно Регулатива (ЕУ) 2016/679 (GDPR) и Директива (ЕУ) 2016/680 (DPLED), беше усвоен и заедно со Директивата 2002/58/Е3 (Директивата за е-приватност), која воспостави хармонизирана рамка во ЕУ за заштита на приватноста на интернет, претставува основна правна рамка за заштита на податоците. Регулативата за е-приватност, како што претходно напоменавме, сè уште не е усвоена. Одредбите од Директивата за е-приватност беа транспонирани во хрватскиот правен систем преку хрватскиот ЗЏакон за електронски комуникации (ЕСА). И покрај општата рамка во врска со заштитата на личните податоци утврдена со GDPR, заедно со Законот за имплементација, актите специфични за секторите (на пр., Законот за труд, ЕСА, Законот за податоци и информации во здравствената заштита, Законот за осигурување) исто така обезбедуваат правна рамка за заштита на податоците генерално во однос на средствата за обработка или целта на обработката на податоците.

Со оглед на тоа што, како и во случајот со Германија, и во Хрватска законот е целосно усогласен со Општата регулатива, во делот што следува ќе дадеме осврт само на некои аспекти од заштитата на приватноста преку интернет. Во однос на тоа дел од другите законски решенија во Хрватска беа подложени на смени со цел да се постигне целосна усогласеност со насоките за ефективна заштита на приватноста општо и преку интернет посебно.

Со измените на Законот за трговски друштва се имплементира Директивата на ЕУ (ЕУ) 2017/1132 и се додадоа одредби во врска со обработката на личните податоци на акционерите на акционерските друштва, кои стапија во сила на 1 јануари 2021 година. Соодветната одредба пропишува дека компанијата, а и посредниците имаат право да ги обработуваат личните податоци на акционерите за целите на идентификување, комуникација, остварување на правата на акционерите и соработка со акционерите. Дополнително, со измените на Законот за трговски друштва не е предвидена слична одредба во однос на обработката на личните податоци на акционерите на други видови компании; затоа, компаниите мора да најдат соодветна правна основа за обработка на личните податоци на нивните акционери и соодветно да ги информираат своите акционери.

Во однос на заштитата на личните податоци во контекст на потрошувачите, Законот за имплементација не пропишува никакви дополнителни барања, сепак, хрватскиот Закон за заштита на потрошувачите содржи одредба во која се наведува дека „на трговецот на мало ќе му се забрани да дава лични податоци на трета страна без претходна согласност од потрошувачот, во согласност со законот со кој се уредува заштитата на личните податоци“. Во однос на горенаведеното и бидејќи Општата регулатива на ЕУ изречно пропишува дека „слободното движење на личните податоци во Унијата нема да биде ниту ограничено ниту забрането од причини поврзани со заштитата на физичките лица во однос на обработката на личните податоци“, применливоста и степенот на гореспоменатата одредба од Законот за заштита на потрошувачите во моментов не се јасни.

Измените на Законот за хрватските кредитни институции, кои стапија во сила на 25 април 2020 година, дозволија и регулираа пренос на лични податоци помеѓу кредитните институции и Хрватскиот регистар на кредитни обврски со цел да се процени кредитната способност на потрошувачите. Имено, согласно Законот за потрошувачки станбени кредити и Законот за потрошувачки кредити, кредитните институции се обврзани да ја проценат кредитната способност на потрошувачите пред да склучат договор за кредит, меѓу другото, со увид во

расположливите кредитни регистри. Бидејќи хрватскиот регистар на кредитни обврски ја суспендира размената на податоци за кредитните обврски за граѓаните на 21 мај 2018 година, горенаведените измени обезбедуваат правна сигурност во размената на информации што кредитните институции ги разменуваат директно или преку посебно правно лице со цел да се оцени кредитната способност на потрошувачите. Тој, исто така, предвидува обврска на кредитната институција да размени, по барање, со други кредитни институции минимална покриеност на информации поврзани со обврските на клиентите, вклучувајќи ги и личните податоци на клиентот, заради проценка на кредитната способност и управување со кредитниот ризик. Сепак, кредитните институции сè уште имаат должност да ги информираат потрошувачите за обработката на нивните лични податоци преку пренесување на нивните лични податоци во Хрватскиот регистар на кредитни обврски и други кредитни институции во согласност со GDPR.

Правото на приватност преку интернет во Хрватска е регулирано и преку регулативите за електронски маркетинг. Употребата на систем за автоматско повикување или комуникација без човечко посредување, уреди за телефакс или е-пошта, вклучувајќи СМС и ММС пораки, е дозволена за целите на директен маркетинг и продажба само со претходна согласност на претплатниците или корисниците, освен кога претплатникот или корисникот е правно лице. Меѓутоа, деловните субјекти, и физички и правни лица, во случај потрошувачот претходно да не ја отфрлил таквата употреба на лични податоци, може да ги користат адресите на е-пошта собрани од потрошувачите кога продаваат производи и услуги само за директен маркетинг и продажба на слични производи и услуги, под услов таквите потрошувачи да имаат јасна и недвосмислена можност за бесплатен и едноставен приговор за таквата употреба на адресата на е-пошта во време на собирање на нивната е-пошта и секое наредно примање на таква е-пошта. Според важечкото решение во Република Хрватска, забрането е упатување повици и пораки преку телефон на потрошувачи што се запишани во регистарот на потрошувачи што не сакаат да примаат повици и пораки во врска со рекламирање и продажба преку телефон. Регистарот се води во Хрватската регулаторна агенција за мрежни активности (НАКОМ). Уписот во регистарот на „Не повикувај“ (NE ZOVI) е преку поднесување барање на посебен образец. И во случај на промена на операторот, конкретниот телефонски број на потрошувачот е евидентиран и нема потреба од нов упис. Секое прекршување е казниво.

Во споредба со Хрватска, (како и во Република Северна Македонија) во Германија „Do Not Call“ листа не постои од причина што телемаркетингот може да се практикува само врз основа на претходна изречна согласност (не согласност дадена во текот на разговорот), што претставува најсилна заштита на потрошувачите.

На 19 април 2019 година, Хрватската агенција за заштита на личните податоци даде свое мислење во врска со обработката на личните податоци за целите на маркетингот во кое наведе дека според Европскиот суд на кредитори-ЕСК, релевантните деловни субјекти можат да обработуваат лични податоци врз основа на согласност и легитимен интерес во согласност со горенаведените правила предвидени во ЕСК. Понатаму, Хрватската агенција подвлекува дека не е дозволено последователно користење на основата на легитимен интерес за обработка доколку има проблеми со валидноста на согласноста.

3.5.3. Краток преглед на заштитата на правото на приватност преку интернет со земјите од регионот

Овој дел од анализата ќе се фокусира на земјите што вообичаено се означуваат како земји од Западен Балкан, а покрај Република Северна Македонија се однесува на Албанија, Босна и Херцеговина, Косово, Србија и Црна Гора. Краткиот преглед укажува дека македонската регулатива во однос на заштитата на приватноста преку интернет е меѓу најнапредните во смисла на пружање ефективна заштита и на усогласеност со регулативите на ЕУ, но и другите меѓународни стандарди.

Сите земји во регионот во своите устави имаат предвидено заштита на приватноста. Во однос на Конвенцијата 108 на Советот на Европа (СЕ), само Косово (кое поради тоа што Србија се противи на неговото зачленување во СЕ) ја нема потпишано и ратификувано оваа конвенција. Кога станува збор за Протоколот 223, треба да се напомене дека само Република Северна Македонија, БиХ и Србија го имаат потпишано овој протокол, а само Србија го има ратификувано.

Според анализата што ја направила фондацијата Share за USAID,[45] во однос на усогласеноста на законските регулативи со Општата регулатива за заштита на податоците на ЕУ, покрај македонската регулатива, целосна усогласеност има и кај српската и косовската регулатива. За разлика од нив, регулативите на Албанија и БиХ се делумно усогласени. Во однос на органите што се грижат за заштита на податоците, истата студија утврдува дека сите земји имаат свои органи за заштита на податоците, кои се формирани како независни тела одговорни пред Народното собрание, а често се задолжени и за заштитата на личните податоци и за слободата за пристап до информации. Во Албанија, Косово, Црна Гора и Србија надлежностите на органите се за заштита на податоци и слободен пристап до информации, додека во македонската и босанската агенција има надлежност единствено за заштита на личните податоци.

Во сите земји од регионот, провајдерите на телекомуникациски услуги задржуваат метаподатоци за комуникациите (евиденција на повиците, IP-адреси, локација итн.) и ги чуваат до две години. До овие податоци подоцна можат да пристапат агенциите за спроведување на законите за разни цели поврзани со криминални истраги. За разлика од македонското законодавство, кое предвидува дека податоците може да се задржат најмногу 12 месеци (а податоци за географска локација 72 саати), во Албанија е регулирано дека податоците може да се задржат до 24 месеци, во БиХ и Косово - е регулирано дека задржувањето е можно најмалку 12 месеци (максималното ограничување не е дефинирано), во Црна Гора максимално дозволено време е 24 месеци и во Србија, како и кај нас, до 12 месеци.

45 Share Fondacia, (December 2021), Регулатива во областа на дигиталните права, компаративна анализа: Албанија, Босна и Херцеговина, Косово, Црна Гора, Северна Македонија, Србија, USAID

Глава - IV

Утврдување на празнините во тековниот пристап кон заштитата на приватноста преку интернет во Република Северна Македонија

4.1 Генерални предизвици за заштитата на приватноста преку интернет релевантни и за Република Северна Македонија

Заштитата на приватноста преку интернет во ера на глобален технолошки бум носи низа предизвици. Напорите во оваа насока во генерална смисла за речиси сите земји и власти во светот е сложена задача поради различни предизвици. Дел од тие причини накратко гравитираат околу: зголемувањето на потребата, но и техничките можности за собирање податоци; нивото на свесност и разбирање на корисниците за предизвикот и можноста нивните податоци да бидат собрани и злоупотребени; комплексноста на политиките за приватност; можноста за следење на „колачиња и профилирање преку интернет"; можноста за споделување на податоците на корисниците од трета страна; безбедносните ризици што влијаат на прекршувања на приватноста; несоодветното регулаторно спроведување на мерките за заштита на приватноста, влијание на напредокот на технологијата и можноста за квалитетен надзор, ограничената контрола над личните податоци во ек на современ технолошки развој; безбедноста на Интернет на нештата (IoT) и динамичната природа на онлајн заканите. Во делот што следува накратко ќе се осврнеме на сите од нив.

Решавањето на овие предизвици бара повеќеслоен пристап, вклучувајќи робусни регулаторни рамки, едукација на корисниците, транспарентни практики за приватност и развој на технологии што ѝ даваат приоритет на приватноста на корисниците. Тековните напори за балансирање на иновациите со заштитата на приватноста се од суштинско значење за да се создаде безбедна и доверлива онлајн-средина.

Глобалната природа на интернетот. Еден од генералните предизвици за приватноста преку интернет лежи во природата на интернетот. Интернетот ги надминува географските граници, со што е релативно тешко да се спроведат конзистентни стандарди за приватност во различни земји поради различните јурисдикции. Ваквиот предизвик влијае со тоа што различните прописи за приватност и законски рамки создаваат сложеност за бизнисите и корисниците, што доведува до недоследности во заштитата на приватноста.

Зголемувањето на потребата, но и техничките можности за собирање податоци. За разлика од порано технолошкиот напредок овозможува олеснето собирање и обработка на податоците. Интернетот и можноста за глобален досег го олеснува обемното собирање податоци од различни субјекти, вклучувајќи веб-локации, апликации, огласувачи и платформи за социјални медиуми. Сето тоа влијае на можноста за изобилството од собрани податоци што, пак, само по себе го зголемува ризикот од нарушување на приватноста (бидејќи повеќе лични информации се подложни на неовластен пристап или злоупотреба).

Нивото на свесност и разбирање на корисниците за предизвикот и можноста нивните податоци да бидат собрани и злоупотребени. Голем број корисници имаат мала или слаба информациска и медиумска писменост. Тоа, меѓу другото, се однесува и на сеопфатното разбирање на поставките за приватност, импликациите од споделувањето податоци и ризиците поврзани со онлајн-активностите. Голем дел од граѓаните на Република Северна Македонија приватноста и нејзината безбедност ја земаат здраво за готово. Тоа влијае голем дел од нив наивно да наседнат на се поголемиот број манипулации и измами преку интернет со што преземаат дејствија со кои ја загрозуваат и личната приватност, но и на другите корисници преку интернет.

Комплексноста на политиките за приватност. Политиките за приватност на онлајн-платформите често се долги, сложени и напишани на тешко разбирлив јазик, кој изобилува со правни термини. Тоа, а и големиот број странцизми и технички изрази им отежнуваат на корисниците да ги разберат условите за заштита. Често во пракса, вклучително и поради ниското ниво на свест, тоа влијае корисниците да го прескокнат читањето на политиките за приватност. Како резултат на тоа, се намалува транспарентноста за тоа како податоците на граѓаните се користат и обработуваат.

Следењето од страна на колачиња и профилирање преку интернет: Следењето од страна на колачиња и онлајн-профилирањето се вообичаени практики за насочено рекламирање. Поради неразбирањето за тоа каква улога може да имаат овие колачиња како технички решенија што имаат и комерцијална цел, голем дел од корисниците имаат тешкотија да ги контролираат поради што често се откажуваат од можноста да влијаат на редуцирање на таквите механизми за следење. Ова, за жал, има сериозно негативно влијание поради фактот што постојаното следење може да резултира со креирање детални кориснички профили за македонските граѓани, што само по себе претставува ризик за приватноста и потенцијално придонесува за манипулативни маркетинг-практики и практики на монетизација - силно и зачестено изразена кај децата преку играњето игри на интернет.

Споделувањето податоци од трета страна. Техничките карактеристики на веб-страниците и нивните локации често споделуваат кориснички податоци со трети лица за различни цели, што доведува до недостаток на контрола врз начинот на постапување со личните информации. Тоа влијае врз приватноста преку фактот што често корисниците не се свесни за обемот на споделување податоци, зголемувајќи ја веројатноста за неовластен пристап или употреба на нивните информации.

Безбедносни ризици што влијаат на прекршувањата на приватноста. Заканите од сајбер-безбедноста за кои стана збор претходно претставуваат значителен ризик за приватноста на корисниците на интернет. Несовесноста, слабата ефикасност и другите предизвици во овој домен за кои станува збор конкретно во македонската интернет-реалност носи низа ризици за приватноста преку интернет за граѓаните на Република Северна Македонија. Ова влијае на тој начин што успешните сајбер-напади може да доведат до неовластен пристап и откривање на чувствителни кориснички информации, загрозувајќи ја приватноста и потенцијално предизвикувајќи финансиска, емотивна/психичка штета или штета на репутацијата и угледот на граѓаните.

Несоодветно регулаторно спроведување. Спроведувањето на прописите за приватност на интернет варира и зависи од повеќе фактори, како политички или геополитички така и од културните перспективи на одредени нации. Поради тоа во пракса некои региони или држави може да немаат цврсти механизми за да се обезбеди усогласеност со стандардите за приватност. Потребата од патување, желбата за освојување на пазарот и сл. може да влијае негативно граѓаните или претпријатијата да станат жртва или да бидат извор за повреда на приватноста преку интернет како резултат на лошите или слабите регулативи.

Технолошките достигнувања и можноста за надзор. Современите технологии, како што се вештачката интелигенција и можноста за дигитално профилирање, на пример, преку препознавање на лицето, претставуваат нови предизвици за приватноста на интернет. Дополнително, владините програми за надзор во одделни држави, може да ја загрозат анонимноста на македонските граѓани без тие да бидат свесни за тоа. Тоа влијае корисниците да

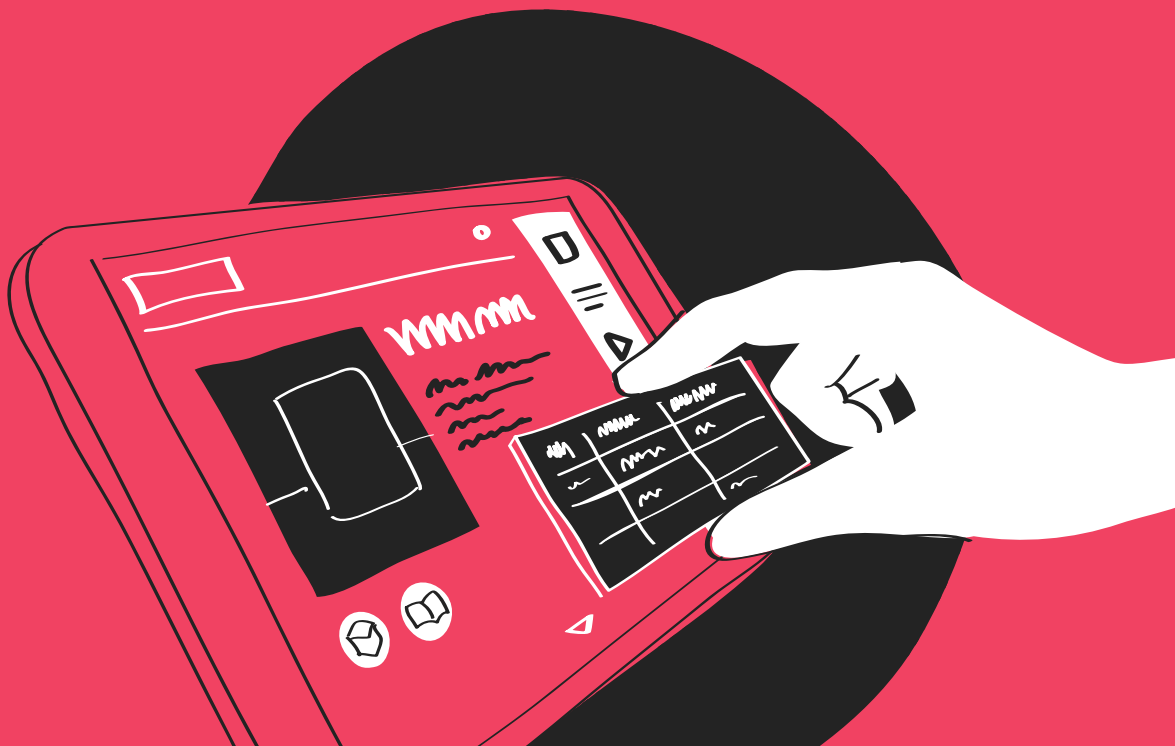
се чувствуваат сé повеќе надгледувани, ограничувајќи ја нивната способност да ја одржуваат приватноста и да се вклучат во анонимни онлајн-активности.

Ограничена контрола над личните податоци. Како резултат на претходно изнесеното, македонските граѓани често имаат ограничена контрола врз тоа како нивните лични податоци се складираат, обработуваат и споделуваат преку онлајн-платформите. Недостатокот на контрола може да влијае на начин што ќе ја наруши довербата, а корисниците може да се колебаат да споделуваат информации онлајн, што го попречува растот и развојот на дигиталните услуги.

Безбедност на Интернет на нештата (IoT). Покрај класичните предизвици за безбедноста на интернетот од т.н. фишинг-напади и другите хакерски напади за кои стана збор претходно, сè поголемата распространетост на уредите познати како интернет на нештата-IoT отвора голем простор за загриженост за безбедноста на поврзаните уреди и потенцијалот за упади во приватноста. Големата популарност и желбата да се имаат овие уреди, заедно со несоодветно обезбедените уреди или политики за приватност при користењето на овие уреди може да се експлоатираат без дозвола на македонските граѓани од злонамерни корисници, што доведува до неовластен пристап до лични податоци, простории и активности на граѓаните - на тој начин загрозувајќи ја нивната приватност, но и приватноста на нивните најблиски и пријателите со кои комуницираат.

Динамичната природа на онлајн-заканите. Онлајн-заканите и ризиците за приватност постојано се развиваат, што само по себе претставува предизвик за организациите, но и за регулаторите во трката да го задржат чекорот со намалувањето на слабостите и пропустите поради кои се нарушува безбедноста, но и приватноста преку интернет. Ваквата динамика често влијае на тоа институциите да доцнат во приспособувањето на новите закани што често влијае да се применуваат застарени мерки за заштита на приватноста, оставајќи ги корисниците изложени на нови ризици за приватноста.

Дел од предизвиците што имаат глобална примена се резултат на современите трендови за поефикасна заштита на приватноста. Овие предизвици се релевантни и за македонските граѓани, бидејќи, како што видовме претходно, законските решенија во голема мерка ги следат современите текови за заштита на приватноста. Во таа насока во делот што следува накратко ќе се осврнеме на предизвиците што се јавуваат како резултат на современите напори да се заштитат личните податоци, а се релевантни за македонските граѓани во контекст на новиот закон за заштита на личните податоци.



4.1.1. Специфични предизвици за безбедноста на приватноста преку интернет кои се јавуваат со примената на дел од новитетите во напорите за заштита на личните податоци релевантни и за Република Северна Македонија

а) Предизвици што се јавуваат по ефективна заштита на приватноста на интернет со заложбите за техничката и интегрирана заштита на личните податоци по дифолт и дизајн, согласно новиот Закон за заштита на личните податоци

Покрај општите предизвици што имаат примена и во напорите за заштита на личните податоци преку принципите по дифолт и дизајн (како на пример комплексната правна терминологија и сл.) примената на овие принципи генерира низа предизвици што имаат влијание во ефективната заштита на приватноста преку интернет.

Разбирање на заштитата на податоците по дизајн и по дифолт претставува сериозен предизвик за голем број помали компании од причина што многу од нив можеби не ги разбираат целосно овие принципи. Честопати програмерите и носителите на одлуки може да немаат потребно ниво на свест за специфичните барања и импликации на овие принципи.

Ограничените ресурси се следниот предизвик што е релевантен за македонските институции. Анализата на причините на дел од сајбер-нападите врз македонските институции за кои стана збор погоре, недвосмислено укажува на недостаток од вложување во градење на капацитетите за заштита од векторите на закана од сајбер-просторот.[46] Ова е особено специфично за помалите организации и компании, на кои им недостасуваат ресурси за да се посветат на сеопфатни иницијативи за усогласување со приватноста. Ова може да резултира со фокусирање на најнепосредните и најочигледните барања, при што принципите по дифолт и дизајн да бидат занемарени.

Недостаток од домашна експертиза во имплементирањето на принципите по дифолт и дизајн за заштита на личните податоци е следен предизвик за нивното почитување и ефективна примена. Згора на тоа, разбирањето и спроведувањето на овие принципи бара мултидисциплинарен пристап, кој вклучува правна, техничка и организациска експертиза. Голем број организации во Република Северна Македонија немаат можност или потреба од ваква експертиза.[47] Од друга страна, законските олеснувања што дозволуваат користење експерти од надвор, делумно поради недостаток од претприемачка култура, а делумно и поради страв од непознато, одбиваат да користат надворешна експертиза.

Поврзано со претходниот предизвик, погрешното толкување на барањата за усогласеност може да предизвика дополнителна тешкотија во примената на принципите по дифолт и дизајн. Поради немањето искуство, а и поради новитетот, контролорите во македонскиот јавен и приватен сектор може погрешно да ги разберат специфичните барања на заштита на личните податоци на граѓаните по дифолт и дизајн. Тоа по автоматизам може да доведе до погрешни толкувања или нецелосни имплементации.

Како следен предизвик специфичен за примената на принципите по дифолт и дизајн во заштита на податоците што може да се одрази на ефикасната заштита на приватноста преку интернет е и честото ставање на функционалноста пред заштитата на приватноста. Во некои случаи, контролорите може да им дадат приоритет на функционалноста и карактеристиките

46 На пример, во анализата за еден од низата сајбер-напади еден од експертите што бил интервјуиран забележува дека „Опасноста е преголема, бидејќи продолжува неинвестирањето и невложувањето во развој на ресурси и технологии, за прво да го заштитиме периметарот, а потоа и внатрешната инфраструктура. Сметам дека сме во многу опасна ситуација со оглед на случувањата во нашата блиска околина". За ова може да се види на: Владимир Калински, (21 октомври, 2022), цитирано

47 Марина Митревска и Тони Милески, (2022) „Кон отпорност и заштита на критичната инфраструктура: студија на случај на Република Северна Македонија", Фондација „Фридрих Еберт" Канцеларија Скопје, достапно на: https://library.fes.de/pdf-files/bueros/skopje/19769.pdf

на нивните производи или услуги во однос на инкорпорирање силни мерки за заштита на податоците.

Културен отпор кон промените кај вработените во рамките на контролорите е честа причина зошто принципите за заштита на податоците по дифолт и дизајн нема да се применуваат. Спроведувањето на новите принципи често бара културна промена во самата организација. Отпорот кон промените, особено кога станува збор за воспоставени процеси и работни текови, може да го попречи усвојувањето на овие принципи.

Како следен предивик од примената на овие принципи што е релвантен за македонското поднебје е и навиката за задоволување на формата - во смисла на ставањето акцент единствено на прописите и нивната усогласеност со тие на ЕУ, односно законските во случај на контролорите. Кај поголем дел од македонските субјекти што се инволвирани во обезбедувањето заштита на податоците евидентен е менталитетот на заштитата на податоците (со тоа и приватноста) да гледаат како на еднократна задача, а не како на постојана обврска. Овој пристап ставен во контекст на технолошкиот развој и еволуцијата на заканите може да доведе до површно или несоодветно спроведување на принципите за заштита на податоците по дифолт или дизајн.

Ниското ниво на свест за заштита од сајбер-просторот генерално и на приватноста специфично е евидентно меѓу македонските граѓани и институции. Ограниченото разбирање на ризиците за приватноста во таа смисла влијае на тоа да не се преземаат релевантни мерки и проактивно да се влијае на заштита на личните податоци, односно приватноста преку интернет. Оттука, недоволниот број на програми за обука за подигање на свеста за потребата од заштита на приватноста и за сајбер-безбедноста генерално негативно се одразуваат во случаите кога треба да се применат некои поспецифични мерки како што се принципите за заштита на податоците по дизајн и дифолт.[48]

б) Предизвици што се јавуваат за ефективна заштита на приватноста на интернет од примената на обврската за проценка на влијанието на заштитата на личните податоци со новиот Закон за заштита на личните податоци

Како што веќе посочивме, со цел да ги усогласи законските решенија со регулативите на ЕУ, а и да обезбеди поефективна заштита на личните податоци, законодавецот во новиот Закон за заштита на личните податоци, покрај другото, во случај на примена на нови технологии наложува контролорите да вршат проценка на влијанието на заштитата на личните податоци (или позната како Data Protection Impact Assessment-DPIA). Сепак, иако идејата за ова е добронамерна, во пракса, генерално оваа мерка може да наиде на низа предизвици, а дел од нив се веќе евидентни и во Република Северна Македонија.

Проценката на влијанието врз заштитата на податоците (DPIA) е клучна компонента на заштитата на дигиталната приватност, која им помага на организациите да ги идентификуваат и ублажат ризиците поврзани со активностите за обработка на податоци.

Една од причините што предизвикув предизвик за имплементација на оваа мерка потекнува од комплексноста и опсегот на дигиталните екосистеми. Овие ситеми во праксата се често сложени и меѓусебно поврзани, вклучувајќи различни технологии, платформи и текови на податоци. Разбирањето на целосниот опсег на активностите за обработка на податоци станува предизвик, особено во големите и сложени организации. Тоа влијае на нецелосното или неточното идентификување на активностите за обработка на податоци што во пракса може

48 Ниското ниво на свесност кај македонските институции за заштита на приватноста и за сајбер-безбедноста е евидентирано преку повеќе случаи. За тоа повеќе може да се види на: „Фактор", (18 октомври, 2022), „Сајбер-напади ја 'дрмаат' Македонија и регионот - Кој стои зад нив?", достапно на: https://faktor.mk/sajber-napadi-ja-drmaat-makedonija-i-regionot---koj-stoi-zad-niv

да резултира со ситуација во која голем дел од потенцијалните ризици за приватноста преку интернет нема да бидат земени предвид. Причините за овој предизвик, генерално, се поврзани со брзиот технолошки напредок. Денес, нашироко е прифатено дека дигиталните технологии се развиваат со брзо темпо и поради поголемата побарувачка, но и поради потребата да се понудат целосни решенија, се воведуваат нови алатки и техники. Да се биде во тек со овие достигнувања е сериозен предизвик, особено кога ресурсите се мали, а културата за следење на промени е инертна. Тоа влијае на фактот проценките што се направени да може бзо да застарат, со што се зголемува ризикот од несоодветни проценки и превидувања на потенцијалните закани за приватноста.

Ревизорскиот извештај на Фондот за здравство, на пример, констатира дека во 2021 година биле платени скоро 282.000 евра за превентивно и адаптивно одржување на информатичкиот систем на Фондот, додека во 2020 - над 300.000 евра.[49] И покрај тоа, во 2023 година Фондот беше цел на сериозен напад, кој побуди голем број сомнежи околу можноста за нарушување на приватноста на граѓаните.

Дополнителен предизвик е тоа што, иако се упатува на проценка, ако државата нема воспоставен критериум за безбедносни стандарди, не е јасно како и со колкава ефикасност ќе може да се примени проценката на влијанието врз заштитата на податоците. Без стандардизирана рамка, не е јасно како може да се бара од организациите доследно да применат проценка. Дополнително, отсуството на заедничка методологија за проценка може да резултира со варијации во квалитетот и ефективноста на проценката за влијанието врз заштитата на податоците. Тоа секако ќе предизвика низа недоследности кои може да доведат до нерамномерно ниво на заштита на приватноста во различни проекти и сектори. Случајот со македонската компанија „Сајтрокс“, која со три други поврзани компании од Грција, Унгарија и од Ирска беше ставена на црната листа на САД поради злоупотреба на комерцијален софтвер за шпионажа, можеби најдобро го отсликува овој случај.

Во оваа насока, на пример, на 6 октомври 2017 година, две од компаниите управувани од македонски државјанин, Иво Малинковски, по име „Сајшарк“ и „Сајтрокс“, ќе побараат од македонското Министерство за внатрешни работи дозвола за производство, промет и извоз на софтверски продукт, којшто може да се користи за заштита на личните податоци, но и за упад во приватноста.[50] Ова како што покажува истражувачката сторија на ИРЛ и „Инсајт“ е наведено во дописите на Малинковски испратени во службите на МВР. Во дописот, според истражувачката сторија, се наведува дека софтверот би им се продавал исклучиво на сертифицирани владини агенции во согласност со законите, а станува збор за озагласениот „Предатор“. Ова е најеклатантен пример за тоа како во пракса немањето стандардизирана рамка и критериум за проценка, но и капацитет кај органите за проценка, може да биде предизвик заз ефикасна заштита на податоците, а со тоа и на приватноста на граѓаните.

Недоволната стручност да се изврши соодветна проценка во овој случај се поврзува и со немањето мултисекторски пристап во праксата кај голем дел од органите. Имено, спроведувањето на проценката предвидена со Законот за заштита на лични податоци, бара комбинација од правна, техничка и организациска експертиза. Кај голем број од македонските контролори недостасуваат професионалци со потребните вештини за извршување сеопфатна проценка и консултации со кои инцидентот и штетата, односно ризикот за приватноста преку интернет за македонските граѓани во наведениот пример би бил спречен.[51] Во оваа насока е точно дека Секторот при МВР задолжен за издавање дозвола, на пример, не располага со кадар што има ваква комбинирана експертиза, што можеби е и разбирливо ако се знае дека

49 Јасмина Јакимова, (14 февруари , 2023), „Неизвесност и многу нервози по сајбер-нападот на Фондот за здравство" Радио „Слободна Европа", достапно https://www.slobodnaevropa.mk/a/%D0%BD%D0%B5%D0%B8%D0%B7%D0%B2%D0%B5%D1%81%D0%BD%D0%BE%D1%81%D1%82-%D0%B8-%D0%BC%D0%BD%D0%BE%D0%B3%D1%83-%D0%BD%D0%B5%D1%80%D0%B2%D0%BE%D0%B-7%D0%B8-%D0%BF%D0%BE-%D1%81%D0%B0%D1%98%D0%B1%D0%B5%D1%80-%D0%BD%D0%B0%D0%BF%D0%B0%D0%B4%D0%BE%D1%82-%D0%BD%D0%B0-%D1%84%D0%BE%D0%B-D%D0%B4%D0%BE%D1%82-%D0%B7%D0%B0-%D0%B7%D0%B4%D1%80%D0%B0%D0%B2%D1%81%D1%82%D0%B2%D0%BE/32270938.html

50 ИРЛ, (18 јули, 2023), „ Македонската компанија 'Сајтрокс' заврши на црна листа на САД поради злоупотреба на софтвер за шпионажа", достапно на: https://irl.mk/makedonskata-kompani-a-sa-troks-zavr-shi-na-crna-lista-na-sad-poradi-zloupotreba-na-softver-za-shpionazha

51 За деталите за барањето и немањето забрана види на ИРЛ, цитирано дело

други сектори при МВР имаат ваква експертиза. Меѓутоа нивото на ниска свест, заедно со несоодветната експертиза, најверојатно, влијаеле на тоа да нема целосни проценки на ризикот, а со тоа и на неуспехот да се идентификуваат и ефикасно да се решат ризиците за приватноста.

Со оглед на ниското ниво на свест кај македонските лидери во доменот на контролорите, но и во рамките на клучните институции, воспоставувањето сеопфатно разбирање на тековите на податоци и создавањето точни залихи на податоци може да биде мошне тешко. Организациите што располагаат со огромни количини податоци и сложени системи за обработка на податоци во вакви случаи, поради ограниченият број на вработени кои се стручни во оваа област, неточно или нецелосно може да ги мапираат податоците, што, пак, може да доведе до несоодветно согледување на потенцијалните ризици за приватноста преку интернет. Поголемиот број институции во државата имаат ваков проблем кога станува збор за соодветен персонал.[52]

Близок до овој предизвик, кој влијае врз ефикасноста во проценката, а со тоа и врз ефикасната заштита на приватноста преку интернет, се и ограничените ресурси. Имено, проценката на влијанието врз заштитата на податоците бара време, посебни напори и ресурси. Македонските институции, а особено помалите претпријатија, често се соочуваат со ограничувања на ресурсите, што ја влијае врз нивната способност да спроведат темелни проценки на активности за обработка на податоци.[53] Несоодветните ресурси може да резултираат со избрзани или нецелосни DPIA, оставајќи ги ризиците за приватност нерешени.

Како предизвик во време на зголемена трка по ефикасност и профит, но и поради законската можност за тоа како офицери за заштита на податоци да се користат лица што не се дел од внатрешната организација на контролорот, може да дојде до несоодветна проценка со која се прави директна штета врз приватноста преку интернет на македонските граѓани. Дополнително, во овој контекст организациите често се потпираат на трети лица продавачи за различни услуги, што само по себе генерира предизвик да се проценат практиките за приватност на овие надворешни субјекти. Осигурувањето за тоа дека трети страни се усогласени со барањата за приватност е исто така предизвик, кој може да создаде низа слабости во ефикасната заштита на приватноста преку интернет. Несоодветната проценка на практиките за приватност на трети страни може да резултира со прекршување на податоците или прекршување на приватноста, кои можеби нема да бидат веднаш видливи. Тоа што македонските власти не го набавиле илегалниот софтвер, но дозволиле тој да се развива и да се дистрибуира од македонска територија до нарачателите од кои голем дел го користеле нелегално и опресивно врз своите граѓани, е можеби најеклатантен пример за тоа како овој предизвик може да се манифестира во пракса.[54]

Развојните процеси на технологиите секогаш ги сметаат овие мерки како потрошувачка кошница. Оттука, отпорот кај клучните функционери во рамките на контролорите или производителите, заедно со сите предизвици што беа споменати, може да влијаат на тоа да се спроведат еднократни проценки што често може да доведат до превид во проценката што бара проактивно решавање на проблемите со приватноста во текот на процесот на развој.

Решавањето на овие предизвици бара проактивен и стратешки пристап кон DPIA. Организациите треба да инвестираат во градење експертиза, интегрирање на DPIA во нивните развојни процеси и да бидат ажурирани за технолошките и регулаторните промени за да се обезбеди тековната ефективност на нивните мерки за заштита на дигиталната приватност.

52 Владимир Калински, (25 април, 2023), „Тешко до кадар за новата Агенција за дигитализација", Радио „Слободна Европа", достапно https://www.slobodnaevropa.mk/a/%D1%82%D0%B5%D1%88%D0%BA%D0%BE-%D0%B4%D0%BE-%D0%BA%D0%B0%D0%B4%D0%B0%D1%80-%D0%B7%D0%B0-%D0%BD%D0%BE%D0%B2%D0%B0%D1%82%D0%B0-%D0%B0%D0%B3%D0%B5%D0%BD%D1%86%D0%B8%D1%98%D0%B0-%D0%B7%D0%B0-%D0%B4%D0%B8%D0%B3%D0%B8%D1%82%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%98%D0%B0-/32378814.html

53 Мирјана Спасовска, (16 ноември, 2019), „Како се штити државата од сајбер-напади?", достапно на https://www.slobodnaevropa.mk/a/30271497.html

54 Види подетално околу ова во: ИРЛ, (13 јули, 2023), „ Како класифицирани документи на македонските и грчките разузнавачки агенции завршија во рацете на креаторите на шпионскиот софтвер 'Предатор'", достапно на: https://irl.mk/kako-klasificirani-dokumenti-na-makedonskite-i-grchkite-razuznavachki-agencii-zavrshi-a-vo-racete-na-kreatorite-shpionskiot-softver-predator/

4.2 Предизвици што влијаат врз заштитата на приватноста преку интернет специфични за Република Северна Македонија

Предизвиците што влијаат врз намалувањето на ефективната заштита на приватноста преку интернет во Република Северна Македонија може да се класифицираат во две групи. Првата група се политизација на јавниот сектор и за сметка на тоа непрофесионален пристап кон прашањата и делокругот на области поврзани со приватноста. Втората група, поврзани со претходната, се ниско ниво на свест важноста на заштитата на приватноста преку интернет.

Во однос на политизацијата и партизацијата на јавниот сектор би рекле дека овој феномен, кој е специфичен за македонското поднебје, претставува ендемски проблем во секоја сфера на јавното функционирање, па така и во контекст на заштитата на приватноста преку интернет. Иако е факт дека во Република Северна Македонија во последните неколку години има намалување на невработеноста, поразително е тоа што Владата и нејзините институции и понатаму се главниот работодавач. Според одредена анализа, за ваквиот феномен се вели:

„Кога основната егзистенција луѓето не можат да ја остварат преку работа во приватен сектор во услови на правичен натпревар, тие ја бараат егзистенцијата или надвор од државата или во единствениот сектор што нуди некаква „иднина“, а тоа е сé уште јавниот сектор во Република Македонија. Проблемот е во тоа што побарувачката за вработување во јавниот сектор е преголема. Луѓето го бараат најприродното нешто за себе и своите деца, а тоа е сигурна работа и некаква егзистенција, во услови на очај подготвени се на многу компромиси – по цена тоа да значи и кршење закони. Оваа неповолна ситуација во која голем дел од населението во Република Македонија живее, политичките партии можат да ја (зло)употребат за свои цели”.[55]

Слични констатации доаѓаат и од ЕУ. Македонската јавна администрација не е реформирана и земјава е умерено подготвена во оваа област – ова може да се заклучи од последниот Извештај на Европската комисија за напредокот во една од најважните области во првиот кластер од преговорите со ЕУ. Неопходноста од реорганизација и трансформација на институциите во државната управа и јавната администрација е забележана во речиси сите досегашни извештаи, но мерки и дејствија не се преземени. За минус се зема што сè уште не е усвоен ревидираниот закон за јавни службеници.[56]

Партизацијата на јавниот сектор, покрај преку непрофесионалноста, влијае и на намалувањето на транспарентноста. Иако една од клучните новини што се прават во насока на заштита на приватноста претставува транспарентноста на институциите, повикувањето на одговорност на јавниот сектор, каде што се случија низа сајбер-напади во кои постои основан сомнеж дека се загрозени личните податоци на граѓаните, и да не постои.[57] Дополнително, она што зачудува кон овој податок е и фактот дека најголемиот дел од државните институции за одржување на своите веб-сајтови ангажираат надворешни компании. Сајтот на МВР, на пример, е изработен и одржуван од „Унет“, а е хостиран на серверите од „Телеком“, кој треба да обезбедува безбедносни мерки за спречување хакерски напади.[58]Ако кон ова се додадат и високите цени за одржување на безбедноста што се плаќаат од страна на јавните институции, кои, на пример, беа посочени погоре во контекст на Фондот за здравство, се јавува сомнеж за корупциски манипулации за сметка на приватноста на граѓаните. Ваквите сомнежи се засилуваат и со податокот за уште еден сличен случај, каде што, иако на тендер, беше избрана фирма што за 160 илјади евра во една година ќе реализира проект за сајбер- безбедност на дел од државните институции, токму овие институции станаа жртви на сериозни хакерски напади.[59] Анализата направена од истражувачка сторија во однос и на овој договор со користење јавно достапни

55 „Фактор“, „Јавна администрација: Партиска пирамида на моќта!“, достапно на: https://faktor.mk/javna-administratsija-partiska-piramida-na-mokta

56 „Локално“, (10 ноември, 2023), „Јавната администрација како 'биро за вработување на партиски луѓе': Вакво неработење, а земање плата никаде не постои во светот“, достапно на: https://lokalno.mk/javna-ta-administracija-kako-biro-za-vrabotuvanje-na-partiski-lugje-vakvo-nerabotenje-a-zemanje-plata-nikade-ne-postoi-vo-svetot/

57 Радио МОФ, „Никој не одговара за хакирањето на државните веб-сајтови“, достапно на: https://www.radiomof.mk/nikoj-ne-odgovara-za-hakiranjeto-na-drzhavnite-veb-sajtovi/

58 Радио МОФ, „Никој не одговара за хакирањето на државните веб-сајтови“, достапно на: https://www.radiomof.mk/nikoj-ne-odgovara-za-hakiranjeto-na-drzhavnite-veb-sajtovi/

59 Јасмина Јакимова (10 август, 2023), „Сајбер-безбедност на институциите: Податоците на извол'те“, „Призма“, достапно на: https://prizma.mk/sajber-bezbednost-na-institutsiite-podatotsite-na-izvol-te/

информации од веб-страницата на Бирото за јавни набавки, покажува дека бил делумно реализиран, а реалноста една година по неговото завршување, покажува дека веб-страниците се далеку од унифицирани и се сеуште ранливи. Епилогот, како што заклучува анализата и Државната комисија за спречување на корупција, е дека овие практики водат кон корупција на секторот.[60]

Партизацијата е мошне опасна кога станува збор за евентуалната злоупотреба на приватноста преку интернет преку можноста за онлајн-следење на комуникациите. После големата и девастирачка афера за масовното прислушкување на граѓаните од 2015 година[61], реформите на разузнавачко-безбедносниот сектор, како да застанаа во ќор-сокак.[62] Во таа насока незаконското прислушкување, останува отворена можност која има сериозни последици, покрај останатото по приватноста на македонските граѓани преку интернет. Ако кон ова се додадат и анализите од претходно поврзани со Македонската компанија „Сајтрокс“, и изјавата на еден од членовите на Комисијата за надзор врз следењето на комуникациите дека недонесувањето на потребните законските измени со кои ќе се продолжи реформата во разузнавачко безбедносниот сектор се должи на немање политичка волја,[63] во тој случај е јасно колку е штетно влијанието на партизацијата на јавниот сектор врз приватноста на македонските граѓани преку интернет. Тоа можеби најдобро го објаснува и фактот зошто изминативе околу три децении самостојност на државата ги одбележаа неколку разузнавачки афери и постојано сомнежи и политички прозивки за нелегално следење на комуникациите.[64]

Немањето на доволна свест со години кај државното раководство пак каскадно влијае на низа предизвици со кои директно се влијае на загрозување на приватноста на граѓаните преку интернет. Иако дел од нив беа елаборирани погоре, овде само системски би ги повториле, а тоа покрај останатото опфаќа: слаби инвестиции за заштита, не почитување на прописите и обврските, лош менаџмент со човечки ресурси и генерално потценување на овој сектор.

Само колку за пример, на конференција одржана по повод на заштитата на приватноста, меѓу другото е констатирано дека законската легислатива не се применува доследно. Така според директорот на АЗЛП, АЗЛП бележи непочитување на обврската за доставување на материјали, предлог-закони, подзаконски акти и други прописи кои се на кој било начин поврзани со заштитата на личните податоци до Агенцијата од страна на предлагачите, министерствата и другите органи. Покрај ова, друг момент е не постапувањето на министерствата и другите органи при усогласувањето на законските и подзаконските решенија, а според дадените мислења, укажувања и препораки од страна на Агенцијата.[65]

Ниското ниво на свест за потребата од заштита на приватноста на граѓаните во рамките на државниот врв можеби е најдобро отсликано што токму директорот кој е именуван од страна на Владата посочува дека се потребни нови вработувања и дополнителни финансиски средства за мотивирање, задржување и професионално усовршување на човечките ресурси во агенцијата со цел да се спречи заминување на постоечкиот, но и да се обучи нов кадар. Во таа смисла, предизвикот со човечките ресурси за кој стана збор и претходно е специфичен во овој контекст исто така.

Во оваа насока, е и ставот на претставник на АЗЛП за тоа дека контролорите не ја обавуваат својата законска должност. Имено, според оваа забелешка „Претходната година (2022) имавме законски решенија кои предизвикаа негативни реакции во јавноста, а Агенцијата воопшто не беше консултирана.“[66]

60 Извештајот за ова на ДКСК може да се види на: https://dksk.mk/wp-content/uploads/2023/07/12-3636-1-__-2021-__-12-1480-__-2021-1.pdf

61 Академик, (Декември 9, 2015), „КОМИСИЈА ЗА СКАНДАЛОТ СО ПРИСЛУШКУВАЊЕТО: Груевски требаше да биде сослушан како сведок, но не дојде заради „редовните обврски“, достапно на: https://akademik.mk/komisija-za-skandalot-so-prislushkuvanjeto-gruevski-trebashe-da-bide-soslushan-kako-svedok-no-ne-dojde-zaradi-redovnite-obvrski/

62 Зоран Јовановски, Октомври 27, 2020), „ Прислушувањето сè уште без ефективна контрола – Советот за граѓански надзор постои само на хартија“, 360 степени, достапно на: https://360stepeni.mk/video-prislushuvaneto-se-ushte-bez-efektivna-kontrola-sovetot-za-graganski-nadzor-postoi-samo-na-hartija/

63 Зоран Јовановски, Октомври 27, 2020), „ Прислушувањето сè уште без ефективна контрола – Советот за граѓански надзор постои само на хартија“, 360 степени, достапно на: https://360stepeni.mk/video-prislushuvaneto-se-ushte-bez-efektivna-kontrola-sovetot-za-graganski-nadzor-postoi-samo-na-hartija/

64 Александар Самрациски, (Декември 11, 2023), „ За опозицијата скандал, властите уверуваат нема нелегално следење“, Радио Слободна Европа, достапно на: https://www.slobodnaevropa.mk/a/za-opozicijata-skandal-vlastite-uveruvaat-nema-nelegalno-sledenje/32725634.html

65 АЗЛП, Конференција на тема „Заедно за заштита на личните податоци“, достапно на: https://azlp.mk/%25D0%25BA%25D0%25BE%25D0%25BD%25D1%2584%25D0%25B5%25D1%2580%25D0%25B5%25D0%25BD%25D1%2586%25D0%25B8%25D1%2598%25D0%25B0-%25D0%25BD%25D0%25B0-%25D1%2582%25D0%25B5%25D0%25BC%25D0%25B0-%25D0%25B7%25D0%25B0%25D0%25B5%25D0%25B4%25D0%25BD%25D0%25BE-%25D0%25B7%25D0%25B0-%25D0%25B7%25D0%25B0%25D1%2588%25D1%2582%25D0%25B8/

66 АЗЛП, Конференција на тема „Заедно за заштита на личните податоци“, достапно на: https://azlp.mk/%25D0%25BA%25D0%25BE%25D0%25BD%25D1%2584%25D0%25B5%25D1%2580%25D0%25B5%25D0%25BD%25D1%2586%25D0%25B8%25D1%2598%25D0%25B0-%25D0%25BD%25D0%25B0-%25D1%2582%25D0%25B5%25D0%25BC%25D0%25B0-%25D0%25B7%25D0%25B0%25D0%25B5%25D0%25B4%25D0%25BD%25D0%25BE-%25D0%25B7%25D0%25B0-%25D0%25B7%25D0%25B0%25D1%2588%25D1%2582%25D0%25B8/

4.3 Препораки за пополнување на воочените празнини и за унапредување на политиките за заштита на личните податоци

Заради поголема систематичност, препораките од овој дел се организирани во препораки што се однесуваат на унапредување на законската регулатива, препораки што се однесуваат на технички решенија и препораки што се однесуваат на креирањето политики и добро управување со податоците со цел поефикасна заштита на приватноста преку интернет.

а) Препораки што се однесуваат на унапредување на законската регулатива:

Постои потреба од усогласување на законските решенија со Регулативите на ЕУ и тоа во однос на:

1. Пренос на лични податоци. Потребата се јавува како резултат на зголемениот обем на дигитализација, кој се прелева во сите сфери, а во кои законските решенија не се обновени или не го следат текот на технолошкиот напредок и со тоа потребата од поефективна заштита на податоците;

2. Зголемување на независноста на Агенцијата за заштита на личните податоци (АЗЛП); АЗЛП, согласно законот, е самостоен орган, кој одговара пред Собранието. Сепак, поврзаноста со Владата и зависноста од Владата е евидентна, што посебно ќе биде образложена во делот за препораки од доменот на креирањето политики и управувањето со заштитата на податоците. Законските унапредувања што ќе овозможат поголема децентрализација, и во буџетска смисла и во смисла на зависност од извршната власт, со што ќе се намали можноста за евентуално влијание врз работата или ќе влијае на можноста за повикување на одговорност на претставници на политичките елити што се на власт.

3. Пречистување на застарени делови од старите национални закони што треба да се укинат. Потребно е предвидување строги казни за раководителите или министрите што се носители на ресорните министерства и надлежни за законите што треба да се усогласат со новиот закон за заштита на личните податоци.

4. Земјата треба да усвои национално законодавство во согласност со Директивата на ЕУ за спроведување на правото. Режимот за Директивата на ЕУ за примена на правото позната како („Law enforcement Directive-LED) се применува само во случаи кога контролорот на податоците е „надлежен орган“, а обработката се врши за „цели за спроведување на законот“. Ова значи дека потенцијално многу голем број и разновидни тела може да бидат опфатени со применливоста на овој режим. Тоа, како што се наведува и во Европската пракса на примена на оваа директива, ќе треба да се оценува од случај до случај. Мора да се подвлече дека овде е потребна голема професионалност и мултисекторски пристап. Причината за тоа е што не е едноставно да се одреди дали целата обработка извршена од органите за спроведување на законот ќе потпадне под режимот на ЛЕД или субјектот од приватниот сектор нема да биде предмет на ЛЕД. Во првиот случај, на пример, органот за спроведување на законот може да спроведе обработка на податоци што нема никаква врска со неговата функција за спроведување на законот (прашања за човечки ресурси, набавки итн.), а во вториот случај, на субјектите од приватниот сектор може да им е доверено или да вршат обработка на податоци за потребите на орган што спаѓа во делокругот на извршување на законите или јавната власт, при што обработката на податоците е за потребите на спроведување на законот. Последното е особено

важно и во однос на препораките што се однесуваат на професионализмот во управувањето со заштитата на податоците.

5. Ратификација на Протоколот за измените и дополнувањата на Конвенцијата 108 (CETS бр. 223), кој е отворен за потпишување на 10 октомври 2018 година.

а) Препораки што се однесуваат на унапредувањето на техничките аспекти и спроведувањето на законските решенија за заштита на приватноста преку интернет

1. Контролорите и државните органи треба да ги ревидираат постојните интерни акти за заштита на личните податоци.

2. Потребно е да се направи анализа за потребите за усогласување со новиот Закон за заштитата на личните податоци.

3. Неопходна е проценка на внатрешните капацитети, човечки, технички и финансиски, кои ќе можат да ги насочат во спроведувањето на процесот на усогласување на постојните законски решенија со новиот закон за заштита на личните податоци и другите закони поврзани со приватноста на македонските граѓани преку интернет.

4. Треба да се зголеми отчетноста на контролорите.

5. Потребна е поголема проактивност, транспарентност и отчетност од страна на АЗЛП во справувањето со повредата на приватноста преку интернет.

6. Зголемување на свеста, но и капацитетите на јавниот и приватниот сектор за поголема сајбер-безбедност, вклучително и медиумска и информатичка писменост со цел заштита на приватноста на граѓаните преку интернет.

7. Постојано следење на трендот и развојот на технологиите за шифрирање со цел примена на стандардизиран пристап кон употребата на овие технологии, кои играат клучна улога во обезбедувањето пренос на податоци, обезбедувајќи информациите да останат шифрирани и недостапни за неовластени страни.

8. Перманентна ревизија и унапредување на безбедносните мерки, како што се автентикација со повеќе фактори и редовно ажурирање на софтверите, за да се зајакне дигиталната одбрана од потенцијални прекршувања.

9. Преземањето проактивни мерки за подигањето на свеста кај корисниците за поставките за приватност и доделувањето грануларна контрола врз споделувањето податоци ја подобруваат индивидуалната автономија во дигиталните простори.

б) Препораки што се однесуваат на етичките и едукативните аспекти за унапредување на заштитата на приватноста на македонските граѓани преку интернет

1. Воспоставување сеопфатен холистички пристап, кој ќе го вклучи целото општество, не само на национален ранг, туку и на локално ниво - локалната заедница.

2. Контролорите во јавниот и приватниот сектор, заедно со компаниите, треба да усвојат принципи за приватност по дизајн, интегрирајќи ги размислувањата за приватност во развојот на производите и услугите од нивниот почеток.

3. Соработка со образовните институции на сите рамништа за креирање наставни програми и нивна синхронизација со тематски целини, и таму каде што тоа е соодветно, управувањето со заштитата на приватноста преку интернет.

4. Одржување на државно спонзорирани (значи кои доаѓаат од генеричкиот буџет на РСМ, не од донатори) обуки за јавниот и приватниот сектор, но и за граѓаните посебно на локално рамниште за подигање на свеста за заштита на приватноста преку интернет.

в) Препораки што се однесуваат на унапредувањето на политиките за управување и заштита на приватноста на македонските граѓани преку интернет

1. Зголемување на професионализацијата во АЗЛП.

2. Намалување на политизацијата на јавниот сектор.

3. Зголемување на практиките за добро, одговорно, отчетно и транспарентно владеење со што ќе се намалат ризиците од непрофесионално клиентилистичко управување со јавниот сектор, особено деловите што имаат надлежност во заштитата на приватноста на македонските граѓани преку интернет.

4. Зголемување на свеста кај политичките лидери и подигање на нивото на важност на органите што се директно инволвирани во заштитата на приватноста преку интернет АЗЛП, АЕК и сл.

5. Стимулирање креативни форми (натпревари или забавно-рекреативни емисии и настани) за јакнењето на граѓаните со знаење за ризиците за приватност, најдобрите практики за безбедно однесување на интернет и за важноста од редовно прегледување и управување со поставките за приватност низ дигиталните простори.

Кратка биографија на авторите

Љубица (Пендароска) Крстевска

е меѓународен експерт, консултант и обучувач во сферата на заштитата на личните податоци, приватноста и сајбер-безбедноста. Со повеќе од 15 години професионално меѓународно искуство во различни средини, вклучувајќи ги земјите од ЕУ, Балкан, САД, Африка и Блискиот Исток, Љубица е наградена меѓу топ-50 жени со влијание во сајбер-безбедноста на Европа 2019 и 2021. Таа е докторски кандидат од областа на меѓународното право и правото на Европската Унија, посебна област: Правна рамка за заштита и трансфер на лични податоци во ЕУ. Во досегашната кариера, таа работела како асистент на Правниот факултет, консултант за Групацијата на Светска банка и канцеларијата на УНИЦЕФ за Европа и Централна Азија за приватност и заштита на податоците, како водечки сениор експерт за заштита на податоци во различни проекти финансирани од ЕУ, меѓу кои неколку проекти Хоризонт2020, ИПА и Еразмус+, како и експерт за сајбер-безбедност и приватност на НАТО SPS и проекти на НАТО ПДД, обучувач за заштита на податоци и приватност за Институт што работи во земјите од Блискиот Исток. Љубица ги поседува највисоките акредитиви за приватност – Certified Information Privacy Professional IAPP Europe, (сертифициран професионалец за приватност на податоци). Таа е основач и претседател на Women4Cyber North Macedonia, Национално поглавје на EU Women4Cyber, експертски член на European Information Technologies Certification Institute Brussels и коосновач на Иницијативата за сајбер-безбедност, корпоративна безбедност и кризен менаџмент C3I.

Д-р Методи Хаџи-Јанев

е професор по меѓународно право на Воената академија „Генерал Михаило Апостолски“ - Скопје, на Правниот факултет при Универзитетот „Гоце Делчев“ од Штип и придружен професор на Универзитетот Аризона, САД. Потесната академска и експертска област на д-р Хаџи-Јанев е фокусирана на меѓународно-правните аспекти во областа на сајбер-безбедноста (управување и креирање политики), хибридните закани, борбата против тероризмот и организираниот криминал. Во наведените области д-р Хаџи-Јанев бил активен консултант во повеќе наврати за потребите на Стејт департментот (каде што организирал обуки во доменот на правните аспекти, управувањето и креирањето политики - вклучително и заштитата на човековите права, управување и заштита на податоците од областа на сајбер-безбедноста), а во моментот работи на два повеќегодишни проекта за градење на капацитетите на граѓанскиот сектор за реформи во разузнавачко-безбедносниот сектор базирано на принципот на човековите права и соодветно градење еластично (резилиентно) општество за сајбер-безбедност. Д-р Хаџи-Јанев е и активен евалуатор на програми со над десетгодишно искуство на евалуација на тематски програми, а во повеќе наврати бил и раководител на проекти спонзорирани од НАТО-програмата Наука за мир и безбедност, НАТО-дивизијата за јавни политики и на други проекти на ЕУ и Hedaya. Д-р Хаџи-Јанев е автор и коавтор на повеќе дела, меѓу кои и едиција од областа на сајбер-безбедноста и одбраната, која е меѓу најдобрите 10 книги за 2017 година во оваа област (повеќе може да се види на: https://www.igi-global.com/book/handbook-research-civil-society-national/129591). Тој се залага за промоција на граѓанскиот сектор и е дел од експертскиот тим на Global Initiative against Transnational Organized Crime. Тој е еден од коосновачите на Евро-атлантскиот совет на Македонија (каде е и потпретседател) и коосновач на Иницијативата за сајбер-безбедност, корпоративна безбедност и кризен менаџмент C3I.

Преглед на користена литература

- Daniele Rotolo, Diana Hicks, Ben R. Martin, (December 2015). "What is an emerging technology?", Research Policy, 44 (10): 1827–1843.
- James Murray, (December 18, 2011), "Cloud network architecture and ICT - Modern Network Architecture". TechTarget,
- NATO, (June 22, 2023), "Emerging and disruptive technologies", достапно на: https://www.nato.int/cps/en/natohq/topics_184303.htm
- Research Article & Bruno Oliveira Martins, (June 19, 2023),
- "Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination", Routledge https://www.tandfonline.com/doi/epdf/10.1080/14650045.2023.2224235?needAccess=true
- Shahrbanou Adjbakhsh, & Anuradha M. Chenoy, (2006), "Human Security: Concepts and Implications, London: Routledge, https://www.routledge.com/Human-Security-Concepts-and-implications/Tadjbakhsh-Chenoy/p/book/9780415473385
- The UNOHCR, (2022), "OHCHR And Privacy In The Digital Age", A/HRC/51/17, https://www.ohchr.org/en/privacy-in-the-digital-age
- Max Freedman, (Oct 20, 2023), How Businesses Are Collecting Data (And What They're Doing With It), Business News Daily, https://www.businessnewsdaily.com/10625-businesses-collecting-data.html
- UN General Assembly, (2022), The right to privacy in the digital age - Surveillance of personal devices and communications, Hacking, достапно на: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement
- Rosalie Chan, (October 9, 2019), "The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections", Business Insider, достапно на: https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10
- Alexander S. Gillis, (2021), "DEFINITION internet of things (IoT)", TechTarget достапно на: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT
- Истражувачка репортерска лабораторија Македонија, (28 јули, 2020), „Агенцијата за заштита на лични податоци ќе проверува дали ДИК безбедно ги чува податоците по сајбер-нападот на изборниот ден", достапно на: https://irl.mk/agentsiata-za-zashtita-na-lichni-podatotsi-e-proveruva-dali-dik-bezbedno-gi-chuva-podatotsite-po-saber-napadot-na-izborniot-den/
- „360 степени", (12 септември, 2022), „По хакерскиот напад на сајтот на МОН ќе се проверува дали имало нарушување на безбедноста на личните податоци", достапно на: https://360stepeni.mk/po-hakerskiot-napad-na-sajtot-na-mon-ke-se-proveruva-dali-imalo-narushuvane-na-bezbednosta-na-lichnite-podatotsi/
- IT MK, (септември 2022), „Vlada.mk 'препродава' патики, дресови, ташни и чевли по поволни цени", достапно на: https://it.mk/vlada-mk-preprodava-patiki-dresovi-tashni-i-chevli-po-povolni-tseni/
- Владимир Калински, (21 октомври, 2022), „Зачестените сајбер-напади на државни сајтови го вклучуваат црвениот аларм", Радио „Слободна Европа", достапно на: овде
- „еМагазин": Од Фондот за здравство тврдат дека податоците на граѓаните се безбедни и дека не се украдени, објавено на 17.2.2023, достапно на: https://emagazin.mk/od-fondot-za-zdravstvo-tvrdat-deka-podatocite-na-graanite-se-bezbedni-i-deka-ne-se-ukradeni/
- European Union (2016), "The European Union's General Data Protection Regulation (GDPR)", https://gdpr.eu/what-is-gdpr/
- Tsaone Swaabow Thapelo; Molaletsa Namoshe, Oduetse Matsebe, Tshiamo Motshegwa, Mary-Jane Morongwa Bopape, (July 28, 2021). "SASSCAL WebSAPI: A Web Scraping Application Programming Interface to Support Access to SASSCAL's Weather Data", достапно на: https://datascience.

codata.org/articles/10.5334/dsj-2021-024
- Martin Reddy, (2011), "API Design for C++", Elsevier Science, p. 1, https://books.google.mk/books?id=I-Y29LylT85wC&redir_esc=y
- Jenna Bunnell, (July 15, 2022), "10 Effective Ways to Gather Ecommerce Data And Information", UNSTACK, достапно на: https://www.unstack.com/blog/10-effective-ways-to-gather-ecommerce-data-and-information
- Carl French, (1996), Data Processing and Information Technology (10th ed.), Thomson. p. 2. ISBN 1844801004
- Johnson, Theodore (2009), "Data Profiling", Springer, Heidelberg (ed.). Encyclopedia of Database Systems
- PagerDuty, "What is Data Aggregation?", https://www.pagerduty.com/resources/learn/what-is-data-aggregation/#:~:text=In%20its%20simplest%20form%2C%20data,more%20consumable%20and%20comprehensive%20medium.
- Privacy Company, (2023), "What are the Differences Between Anonymisation and Pseudonymisation", достапно на: https://www.privacycompany.eu/blogpost-en/what-are-the-differences-between-anonymisation-and-pseudonymisation#:~:text=Pseudonymisation%20is%20the%20process%20of,not%20subject%20to%20the%20GDPR.
- Rutgers, (2022), "What Is Data Mining? A Beginner's Guide (2022)"
- Tiny, (September 2022), "Gathering the right data for personalization, in a privacy-driven world", достапно на: https://www.tiny.cloud/blog/personalization-and-personal-data-collection/
- Закон за заштита на личните податоци („Службен весник на Република Северна Македонија" бр. 42/20)
- Закон за изменување и дополнување на Законот за заштита на личните податоци („Службен весник на Република Северна Македонија" бр. 294/21)
- Закон за ратификација на Протоколот за измена на Конвенцијата за заштита на лица во однос на автоматска обработка на лични податоци („Службен весник на Република Северна Македонија" бр. 152/21)
- Закон за ратификација на Дополнителниот протокол кон Конвенцијата за заштита на поединците во поглед на автоматската обработка на лични податоци, во врска со надзорните тела и прекугранични пренос („Службен весник на Република Македонија" бр. 103/08)
- Закон за ратификација на Конвенцијата за заштита на лица во однос на автоматска обработка на податоци („Службен весник на Република Македонија" бр. 7/05)
- Закон за општата управна постапка, („Службен весник на РМ", бр. 124 од 23.7.2015 година)
- Правилник за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија" бр. 122/20)
- Правилник за содржината и формата на актот за начинот на вршење видеонадзор („Службен весник на Република Северна Македонија" бр. 122/20)
- Правилник за изменување на Правилникот за содржината и формата на актот за начинот на вршење видеонадзор („Службен весник на Република Северна Македонија" бр. 280/21)
- Правилник за содржината на анализата на целта, односно целите за кои се поставува видеонадзорот и извештајот од извршена периодична оценка на постигнатите резултати од системот за вршење видеонадзор („Службен весник на Република Северна Македонија" бр. 122/20)
- Правилник за начинот на вршење супервизија („Службен весник на Република Северна Македонија" бр. 122/20)
- Правилник за пренос на лични податоци („Службен весник на Република Северна Македонија" бр. 122/20) („Службен весник на Република Северна Македонија" бр. 122/20)
- Правилник за обука за заштита на личните податоци („Службен весник на Република Северна Македонија" бр. 122/20);

- Правилник за формата и содржината на службената легитимација и за начинот на нејзиното издавање и одземање („Службен весник на Република Северна Македонија“ бр. 122/20)
- Правилник за процесот на проценка на влијанието на заштитата на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20)
- Правилник за формата и содржината на барањето за утврдување прекршување на одредбите од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20)
- Правилник за начинот на известување за нарушување на безбедноста на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20)
- Правилник за известување за обработка на лични податоци со висок ризик („Службен весник на Република Северна Македонија“ бр. 122/20)
- Листа на видовите операции на обработка за кои се бара проценка на влијанието врз заштитата на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20)
- Листа на видовите операции на обработка за кои не се бара проценка на влијанието врз заштитата на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20)
- Одлука за утврдување стандардни договорни клаузули за пренос на лични податоци во трети земји („Службен весник на Република Северна Македонија“ бр. 280/21)
- Одлука за утврдување стандардни договорни клаузули помеѓу контролорите и обработувачите („Службен весник на Република Северна Македонија“ бр. 280/21)
- Одлука за утврдување методологија за хармонизација на секторската легислатива („Службен весник на Република Северна Македонија“ бр. 38/22)
- Правилник за дополнување на Правилникот за содржината на анализата на целта, односно целите за кои се поставува видеонадзорот и извештајот од извршена периодична оценка на постигнатите резултати од системот за вршење видеонадзор („Службен весник на Република Северна Македонија“ бр. 183/22)
- Правилник за дополнување на Правилникот за формата и содржината на барањето за утврдување прекршување на одредбите од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 183/22)
- Правилник за дополнување на Правилникот за начинот на известување за нарушување на безбедноста на личните податоци („Службен весник на Република Северна Македонија“ бр. 183/22)
- Закон за електронските комуникации („Службен весник на Република Македонија“ бр. 39/2014), 188/2014, 44/2015, 193/2015, 11/2018 и 21/2018 и „Службен весник на Република Северна Македонија“ бр. 98/2019 и Закон за електронска трговија („Службен весник на Република Македонија“ бр. 133/2007, 17/2011, 104/2015 и 192/2015 и „Службен весник на Република Северна Македонија“ бр. 31/2020)
- Закон за кривична постапка („Службен весник на Република Северна Македонија“ бр. 150/10, 100/12, 142/16 и 198/18)
- Кривичен законик („Службен весник на Република Северна Македонија“ бр. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017, 248/2018 и број 36/23
- Закон за следење на комуникациите („Службен весник на Република Северна Македонија“ бр.71/18)
- Закон за државна статистика („Службен весник на Република Македонија” бр. 54/1997, 21/2007, 51/2011, 104/2013 , 42/2014, 192/2015, 27/16, 83/18, 220/18, 31/20).
- Закон за социјална заштита („Службен весник на РСМ, бр. 104 од 23.5.2019 година“)

- Закон за попис на населението, домаќинствата и становите во Република Северна Македонија („Службен весник на РСМ. бр 19/2021)
- Закон за заштита на децата („Службен весник на Република Македонија“ бр. 23/2013, 12/2014, 44/2014, 144/2014, 10/2015, 25/2015, 150/2015, 192/2015, 27/2016, 163/2017, 21/2018 и 198/2018 и „Службен весник на Република Северна Македонија“ бр. 104/2019, 146/2019, 275/2019, 311/2020 и 294/2021)
- Закон за правда за децата („Службен весник на Република Македонија“ бр. 148/2013 и „Службен весник на Република Северна Македонија“ бр. 152/2019 и 275/2019)
- За оваа вест може повеќе да се види, на пример, на Радио МОФ, (20 јули, 2023) „Матичните книги пробиени – трговија со личните податоци на граѓаните“, достапно на https://www.radio-mof.mk/matichnite-knigi-probieni-trgovija-so-lichnite-podatoci-na-gragjanite/
- Влада на Република Северна Македонија (2024), достапно на: https://ener.gov.mk/Default.aspx-?item=pub_regulation&subitem=view_reg_detail&itemid=514
- Закон за правда на децата („Службен весник на Република Македонија“ бр.148/2013 и „Службен весник на Република Северна Македонија“ бр. 152/2019 и 275/2019)
- Закон за заштита на децата („Службен весник на Република Македонија“ бр. 23/2013, 12/2014, 44/2014, 144/2014, 10/2015, 25/2015, 150/2015, 192/2015, 27/2016, 163/2017, 21/2018 и 198/2018 и „Службен весник на Република Северна Македонија“ бр. 104/2019, 146/2019, 275/2019, 311/2020 и 294/2021)
- Trans-Lez „lex specialis derogat legi generali“, достапно на: https://www.trans-lex.org/910000/_/lex-specialis-principle/
- Законот за заштита на децата ги опфаќа законите од 2013 „Сл. весник на Република Македонија“ бр.23/13; Законот за дополнување на Законот за заштита на децата („Сл. весник на Република Северна Македонија“ бр.311/20).
- EUR Lex, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Document 32002L0058, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
- EUR-Lex, Consolidated text: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Document 02002L0058-20091219, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Date of end of validity: 24/05/2018; Repealed by 32016R0679, достапно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046
- Законот за заштита на личните податоци („Службен весник на Република Македонија” број 7/2005 и 103/2008)
- EUR-Lex Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Document 52017PC0010 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017PC0010
- „Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications“ е достапна на: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf
- United Nations, “Universal Declaration of Human Rights” proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A), член 12, достапно на: https://www.un.org/en/about-us/universal-declaration-of-human-rights
- United Nations, “International Covenant on Civil and Political Rights”, 16 December 1966, General Assembly resolution 2200A (XXI), Entry into force: 23 March 1976, in accordance with Article 49, достапно на: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-cov-

enant-civil-and-political-rights
- UN, General Assembly. Resolution 68/167. The right to privacy in the digital age. A/RES/68/167. 18 December 2013. https://undocs.org/en/A/RES/68/167
- Anupam Chander and Molly Land, (January 20, 2017), United Nations General Assembly Resolution on the Right to Privacy in the Digital Age, Cambridge University Press, https://www.cambridge.org/core/journals/international-legal-materials/article/abs/united-nations-general-assembly-resolution-on-the-right-to-privacy-in-the-digital-age/136942F57940B12E0733852518E4B68C
- Convention on the Rights of the Child, достапно на: https://www.coe.int/en/web/compass/convention-on-the-rights-of-the-child#:~:text=The%20Convention%20was%20adopted%20by,the%20age%20of%20eighteen%20years.
- Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990, достапно на: https://www.refworld.org/pdfid/3ddcafaac.pdf
- Organisation for Economic Co-Operation and Development, (2003), "Privacy Online: OECD Guidance on Policy and Practice, Volume 961, достапно на: https://books.google.mk/books/about/Privacy_Online.html?id=zW3dYG_RWYkC&redir_esc=y
- „Извештај 2023" на ОЕЦД, види во: OECD 2023, Recommendation of the Council on OECD Legal Instruments Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, DSTI/CDEP/DGP(2022)2/REV2, достапно на: https://legalinstruments.oecd.org/public/doc/119/119.en.pdf
- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security 2002,
- EBISA, OECD Guidelines, достапно на: https://www.enisa.europa.eu/topics/risk-management/current-risk/laws-regulation/corporate-governance/oecd-guidelines
- Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, широко позната и како European Convention on Human Rights, Rome, 4.XI.1950 достапно на: https://www.echr.coe.int/documents/d/echr/convention_eng
- Министерство за правда 6.12.2019, „Дескоска на средба со генералниот секретар на Советот на Европа: Потпишан Протокол за Конвенцијата за заштита на лица во однос на автоматска обработка на лични податоци"
- Збирка на меѓународни договори, (ажурирано август 2023)
- Лукина и партнерите од Хрватска, добар дел од нивните трудови може да се најдат на https://www.lexology.com/firms/24422
- Hrvatski Sabor, 2018, „Odluku O Proglašenju Zakona O Provedbi Opće Uredbe O Zaštiti Podataka", достапна на: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html
- Hrvatski Sabor, 2018, „Odluku O Proglašenju Zakona O Provedbi Opće Uredbe O Zaštiti Podataka", достапно на: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html
- Share Fondacia, (December 2021), Регулатива во областа на дигиталните права, компаративна анализа: Албанија, Босна И Херцеговина, Косово, Црна Гора, Северна Македонија, Србија, USAID
- Марина Митревска и Тони Милески, (2022) „Кон отпорност и заштита на критичната инфраструктура"студија на случај на Република Северна Македонија" Фондација „Фридрих Еберт Канцеларија Скопје, достапно на: https://library.fes.de/pdf-files/bueros/skopje/19769.pdf
- Ниското ниво на свесност кај македонските институции за заштита на приватноста и за сајбер-безбедноста е евидентирано преку повеќе случаи. Околу тоа повеќе може да се види на: „Фактор", (18 октомври, 2022), „Сајбер-напади ја 'дрмаат' Македонија и регионот - Кој стои зад нив?", достапно на: https://faktor.mk/sajber-napadi-ja-drmaat-makedonija-i-regionot---koj-stoi-zad-niv
- Јасмина Јакимова, (14 февруари, 2023), „Неизвесност и многу нервози по сајбер-нападот на Фондот за здравство" Радио „Слободна Европа",
- ИРЛ, (18 јули, 2023), „ Македонската компанија 'Сајтрокс' заврши на црна листа на САД поради

злоупотреба на софтвер за шпионажа“, достапно на: https://irl.mk/makedonskata-kompani-a-sa-troks-zavrshi-na-crna-lista-na-sad-poradi-zloupotreba-na-softver-za-shpionazha/

- Владимир Калински, (25 април, 2023), „Тешко до кадар за новата Агенција за дигитализација“, Радио „Слободна Европа“, достапно
- Мирјана Спасовска, (16 ноември, 2019), „Како се штити државата од сајбер-напади?“, достапно на https://www.slobodnaevropa.mk/a/30271497.html
- Види подетално за ова во: ИРЛ, (13 јули, 2023), „Како класифицирани документи на македонските и грчките разузнавачки агенции завршија во рацете на креаторите на шпионскиот софтвер ‘Предатор’“, достапно на: https://irl.mk/kako-klasificirani-dokumenti-na-makedonskite-i-grchkite-razuznavachki-agencii-zavrshi-a-vo-racete-na-kreatorite-shpionskiot-softver-predator/
- „Фактор“, „Јавна администрација: Партиска пирамида на моќта!“, достапно на: https://faktor.mk/javna-administratsija-partiska-piramida-na-mokta
- „Локално“, (10 ноември, 2023), Јавната администрација како „биро за вработување на партиски луѓе“: „Вакво неработење, а земање плата никаде не постои во светот“„ достапно на: https://lokalno.mk/javnata-administracija-kako-biro-za-vrabotuvanje-na-partiski-lugje-vakvo-nerabotenje-a-zemanje-plata-nikade-ne-postoi-vo-svetot/
- Радио МОФ, „Никој не одговара за хакирањето на државните веб-сајтови“, достапно на: https://www.radiomof.mk/nikoj-ne-odgovara-za-hakiranjeto-na-drzhavnite-veb-sajtovi/
- Истото
- Јасмина Јакимова (10 август, 2023), „Сајбер-безбедност на институциите: Податоците на извол’те“, „Призма“, достапно на: https://prizma.mk/sajber-bezbednost-na-institutsiite-podatotsite-na-izvol-te/
- Извештајот за ова на ДКСК може да се види на: https://dksk.mk/wp-content/uploads/2023/07/12-3636-1-__-2021-__-12-1480-__-2021-1.pdf
- „Академик“, (9 декември, 2015), „КОМИСИЈА ЗА СКАНДАЛОТ СО ПРИСЛУШКУВАЊЕТО: Груевски требаше да биде сослушан како сведок, но не дојде заради „редовните обврски“, достапно на: https://akademik.mk/komisija-za-skandalot-so-prislushkuvanjeto-gruevski-trebashe-da-bide-soslushan-kako-svedok-no-ne-dojde-zaradi-redovnite-obvrski/
- Зоран Јовановски, (27 октомври, 2020), „Прислушувањето сè уште без ефективна контрола – Советот за граѓански надзор постои само на хартија“, „360 степени“, достапно на: https://360stepeni.mk/video-prislushuvaneto-se-ushte-bez-efektivna-kontrola-sovetot-za-graganski-nadzor-postoi-samo-na-hartija/
- Александар Самраџиски, (11 декември, 2023), „За опозицијата скандал, властите уверуваат нема нелегално следење“, Радио „Слободна Европа“, достапно на: https://www.slobodnaevropa.mk/a/za-opozicijata-skandal-vlastite-uveruvaat-nema-nelegalno-sledenje/32725634.html
- АЗЛП, Конференција на тема „Заедно за заштита на личните податоци“, достапно на: https://azlp.mk/%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D1%98%D0%B0-%D0%BD%D0%B0-%D1%82%D0%B5%D0%BC%D0%B0-%D0%B7%D0%B0%D0%B5%D0%B4%D0%BD%D0%BE-%D0%B7%D0%B0-%D0%B7%D0%B0%D1%88%D1%82%D0%B8/