# Водич за заштита на правото на приватност во дигиталниот простор

*(Практични насоки за правни професионалци)*

Јануари, 2024

Финансирано од Европска Унија

ЕУ со ТЕБЕ

Проектот е имплементиран од

ЦЕНТАР ЗА ПРАВНИ ИСТРАЖУВАЊА И АНАЛИЗИ
CENTER FOR LEGAL RESEARCH AND ANALYSIS

МЗМП

# *ИМПРЕСУМ*

*Наслов: Водич за заштита на правото на приватност во дигиталниот простор*

*Издавач: Центар за правни истражувања и анализи*
*Македонско здружение на млади правници*

*За издавачот: Лидија Стојкова Зафировска, ЦПИА*
*Александра Цветановска, МЗМП*

*Автор: Александар Гоџо*

*Придонес: Д-р Ева Сухрада Киршмаер*
*Доц. д-р Ирена Бојаџиевска*

*Уредник: Лидија Стојкова Зафировска*

*Редакција: Центар за правни истражувања и анализи*

*Лектура: Дејан Василевски*

*Графички дизајн: Вертиго*

*Печатница: Полиестердеј*

*Тираж: 30*

*Место и година на издавање: Скопје, 2024*

*CIP – Каталогизација:*
*Национална и универзитетска библиотека "Св. Климент Охридски", Скопје*
*342.738.037:004.738.5(036)*
*ГОЏО, Александар*
*Водич за заштита на правото на приватност во дигиталниот простор : (практични насоки за правни професионалци) / [автор Александар Гоџо]. - Скопје : Центар за правни истражувања и анализи : Македонско здружение на млади правници, 2024. - 91 стр. : илустр. ; 25 см*

*Фусноти кон текстот*

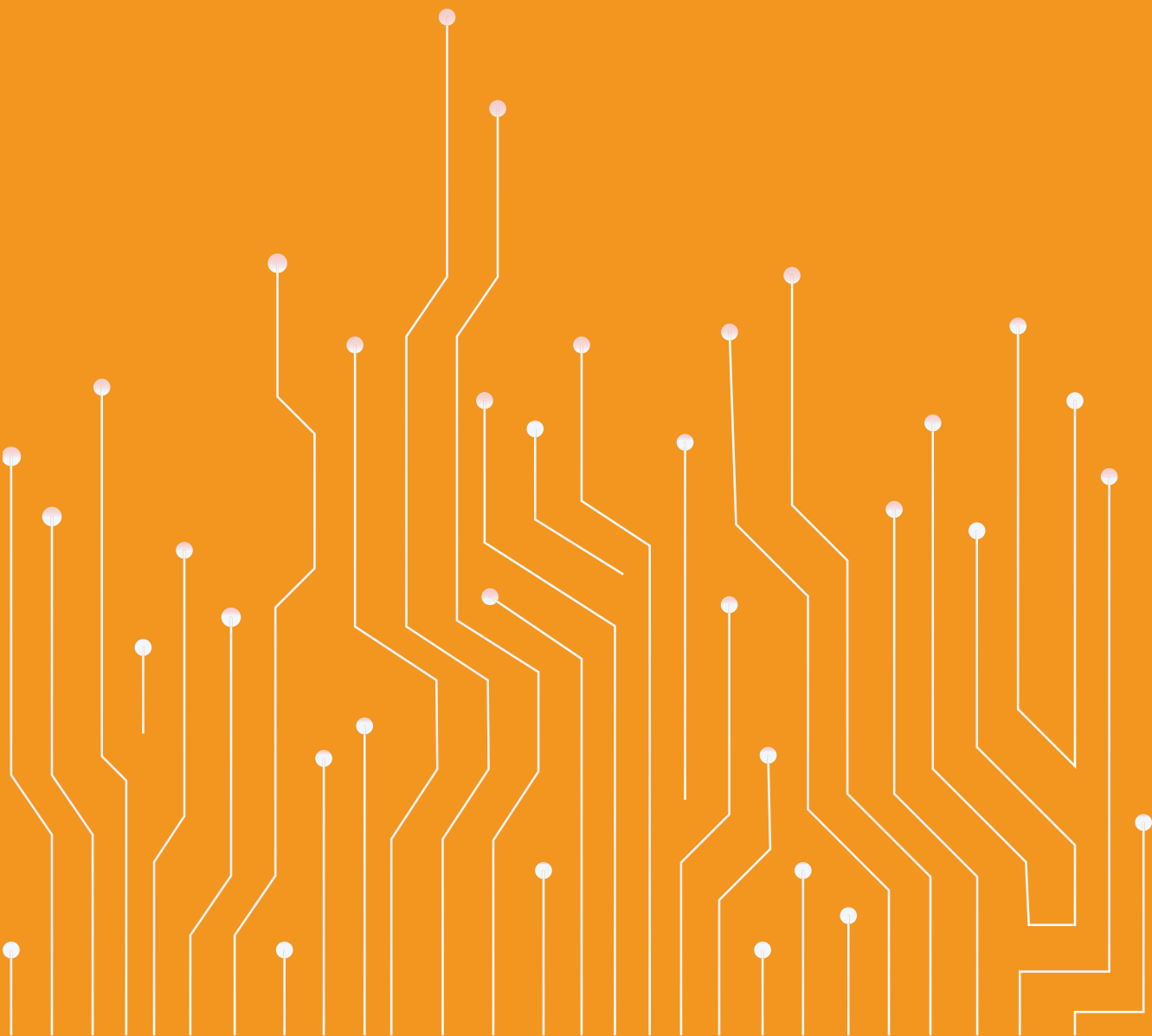
*ISBN 978-608-4926-11-5 (Центар за правни истражувања и анализи)*
*ISBN 978-608-4843-84-9 (Македонско здружение на млади правници)*

*а) Право на приватност -- Заштита -- Интернет -- Водичи б) Лични податоци -- Заштита -- Интернет -- Водичи*

*COBISS.MK-ID 62786821*

*Оваа публикација е изработена во рамките на проектот „Ефикасна правда за заштита на основните слободи и правото на приватност во онлајн-просторот“, финансиран од Европската унија. Содржината на публикацијата е единствена одговорност на авторите и на никаков начин не може да се смета дека ги одразува гледиштата на Европската унија.*

# СОДРЖИНА



# ЛИСТА НА КРАТЕНКИ

GDPR – General Data Protection Regulation

ЗЗЛП – Закон за заштита на личните податоци

КЗ – Кривичен законик

ЗКП – Закон за кривична постапка

ЗПП – Закон за парнична постапка

ЗОО – Закон за облигациски односи

ЗОУП – Закон за општа управна постапка

ЗУС – Закон за управни спорови

ЕУ – Европска унија

TAIEX – Technical Assistance and Information Exchange instrument

ЕСЧП – Европски суд за човекови права

ЕСП – Европски суд на правдата

ЕКЧП – Европска конвенција за човекови права

ГСОН – Генерално собрание на Обединетите нации

ИКТ – Информатичко-компјутерски технологии

АЗЛП – Агенција за заштита на лични податоци

МВР – Министерство за внатрешни работи

ОЈО – Основно јавно обвинителство

ЈО – Јавно обвинителство

***„ПРИВАТНОСТА НЕ Е ПРИВИЛЕГИЈА, ТАА Е ОСНОВНО ЧОВЕКОВО ПРАВО“***

ВИВИЕН РЕДИНГ

# ВОВЕД

Наместо предговор, еден податок што мошне јасно може да ја отслика големината на феноменот со кој се соочуваме.

Според истражување направено во 2022 година на интернет-страници што содржат и социјални медиуми и имаат загубено најмногу кориснички податоци (без притоа да се навлегува во судбината на овие податоци и потенцијалните штети што настанале), состојбата е следната:

### 1. „Јаху"- 3,5 милијарда

Повеќе од 3,5 милијарди корисници се погодени од прекршување на податоците во врска со „Јаху", вклучително и три милијарди фатени во прекршувањето во 2013 година.

### 2. „Фејсбук" – 2,1 милијарда

Четири одделни прекршувања во 2019 година го зголемија бројот на корисници на „Фејсбук" на кои им биле украдени податоци на над две милијарди.

### 3. „Линкдин" – 1,1 милијарда

Мнозинството од 1,1 милијарда корисници на „Линкдин", чии податоци беа изложени беа погодени од прекршување во 2021 година што резултираше со продажба на 700 милиони податоци.

### 4. „Мајспејс" – 719 милиони

Тие три прекршувања ги открија податоците на 719 милиони корисници на „Мајспејс". Сега неактивната страница имаше само седум милиони корисници во 2019 година.

### 5. „Сина веибо" – 538 милиони

Податоците на 539 милиони корисници на кинеската страница за социјални медиуми, вклучително и 172 милиони телефонски броеви, беа ставени на продажба во 2020 година.

### 6. „Твитер" – 370 милиони

„Твитер" во јуни потврди дека хакер добил пристап до деталите за контакт за 5,4 милиони сметки, додавајќи го вкупниот број на засегнати корисници на страницата за микроблогирање.

### 7. „Куора" – 100 милиони

„Куора", интернет-страница на која корисниците можат да поставуваат и да одговараат на прашања, откри дека лозинките и безбедносните прашања на сто милиони корисници биле откриени во хакирање во 2018 година.

### 8. „Дејлимоушн“ – 85 милиони

Хакер украл повеќе од 85 милиони уникатни адреси на е-пошта и кориснички имиња од системите на платформата за споделување видео на „Дејлимоушн“, како и лозинки за 18,3 милиони сметки во рација во 2016 година.

### 9. „Тамблер“ – 65 милиони

„Тамблер“ во 2016 година објави дека неговата безбедност била загрозена три години претходно, што резултирало со украдени податоци за корисничката сметка на 65 милиони луѓе.

### 10. „Инстаграм“ – 49 милиони

Околу 49 милиони корисници на платформата за споделување фотографии „Инстаграм“, во сопственост на „Фејсбук“, беа изложени откако незаштитен сервер беше протечен на интернет во 2019 година.[1]

Дигиталната трансформација на нашето општество е секако една од најбрзите и најдлабоките транзиции на цивилизацијата што сме ги доживеале некогаш. Оваа дигитална ера нè води да комуницираме сè повеќе и повеќе онлајн, за информации, забава, потрошувачка или работа. Пандемијата со КОВИД-19 го откри потенцијалот на дигиталните услуги што им овозможија на луѓето да продолжат да комуницираат и да се ангажираат и нè направија поотпорни. Но, остануваат многу прашања за последиците од оваа трансформација и нејзиното влијание врз човековите права.

Прашањето за приватноста одамна е многу актуелно во нашиот секојдневен живот, но зголемената употреба на виртуелниот простор и развојот на технологијата, како што е вештачката интелигенција, ги доведува овие расправи уште повеќе во центарот на вниманието. Наместо да ја намалат дискриминацијата или нееднаквоста, некои алгоритамски системи за донесување одлуки можат да ја влошат, особено во јавната сфера. Со употребата на предвидливи карактеристики во правосудниот систем, се чини дека се појавува дури и нов извор на правото. Алатките за препознавање лице ги враќаат концептите како што се физиономијата и верувањето дека карактеристиките на однесувањето можат да се заклучат од физичките карактеристики.

Целосното уживање на нашите права во киберпросторот доаѓа со соодветна заштита од ризиците во онлајн-опкружувањето. Правото на приватен живот, човечкото достоинство, безбедноста, интегритетот на личноста, недискриминацијата се загрозени под закана од киберкриминалот.[2]

1 https://businessplus.ie/tech/social-media-lost-user-data/

2 ECHR Symposium: Human Rights in the Digital Sphere.

# ЦЕЛ И ОПСЕГ

Овој водич е замислен да биде еден вид практична алатка, каде што ќе бидат сублимирани во еден документ сите поважни поими, правни рамки, закани, принципи, актери, механизми, правни лекови и процедури што се предвидени во законодавството и практиката на Република Северна Македонија, како и некои практични дилеми, примери и сентенции како на овие прашања гледаат Европскиот суд за човекови права и Европскиот суд на правдата.

Примерите и насоките дадени во овој водич треба да им служат на државните органи, пред сè АЗЛП, но и на актерите во правосудството (судиите, јавните обвинители, адвокатите) во Република Северна Македонија, како и на сите правни и физички лица, кога се занимаваат со прашања за заштита на податоците, без разлика дали вршат надзор или супервизија над примена на прописи, одлучуваат за жалби или тужби поврзани со ракување, обработка или злоупотреба на лични податоци, откриваат и/или гонат сторители на казнени дела и прекршоци, даваат правна помош или самите треба да ја почитуваат заштитата на податоците во рамките на вршењето на нивната дејност. Воедно, овие примери и насоки се секако и препорачано четиво и за сите физички и правни лица, кои на еден или на друг начин се инволвирани или од нив се бара да ги почитуваат правилата и прописите што владеат во оваа сфера, да ги препознаваат опасностите и предизвиците и да можат соодветно да ги користат алатките што им се на располагање со цел да се заштитат, да се минимизираат ризиците по нивните права на приватност и заштита на личните податоци во киберпросторот, како и соодветно и ефикасно да ги користат правните механизми и правни лекови во рамките на домашниот правен поредок, а секако и во меѓународниот.

## Клучни принципи

Документот е базиран на клучните принципи за изработка на „ Водич за заштита на правото на приватност во дигиталниот простор “, што беа подготвени како резултат на Експертската TAIEX мисија што беше имплементирана во периодот од 31 октомври до 2 ноември 2023 година во Република Северна Македонија. Целта на TAIEX мисијата беше да обезбеди поддршка и совети за подготовка на „Насоки за судските чинители за приватност и заштита на податоците во Република Северна Македонија“, во согласност со GDPR и acquis на ЕУ во оваа област.

Овој документ ги содржи препораките и соодветно ги обработува подетално.

## Некои клучни термини

За потребите на овој водич, пред сè треба да ги дефинираме најосновните поими што ја претставуваат срцевината на тематиката.

### *„Лични податоци“*

значи секоја информација што се однесува на идентификувано или физичко лице кое може да се идентификува („субјект на податоци“); физичко лице кое може да се идентификува е она што може да се идентификува, директно или индиректно, особено со повикување на идентификатор, како што се име, идентификациски број, податоци за локација, онлајн-идентификатор или на еден или повеќе фактори специфични за физичкиот, физиолошкиот, генскиот, менталниот, економскиот, културниот или социјалниот идентитет на тоа физичко лице.

### *„Посебни категории на податоци“*

се лични податоци што откриваат информации за расното или етничкото потекло, политичките мислења, религиозните или филозофските убедувања или членството во синдикат, како и генски податоци, биометриски податоци, податоци за здравјето или податоци за полот на физичкото лице или сексуална ориентација. Тие подлежат на посебен режим (член 13 од ЗЗЛП).

### *„Обработка“*

значи секоја операција или збир операции што се изведуваат на лични податоци или на збирки лични податоци, без разлика дали се со автоматизирани средства или не, како што се собирање, снимање, организација, структурирање, складирање, приспособување или измена, пронаоѓање, консултација, употреба, откривање со пренос, ширење или на друг начин ставање на располагање, усогласување или комбинација, ограничување, бришење или уништување.

### *„Контролор“*

значи физичко или правно лице, јавна власт, агенција или друго тело кое само или заедно со други ги утврдува целите и начините на обработка на личните податоци; кога целите и средствата за таква обработка се утврдени со законодавството на Унијата или земјата-членка, контролорот или специфичните критериуми за негово назначување можат да се предвидат со законодавството на Унијата или земјата-членка.

### *„Обработувач“*

значи физичко или правно лице, јавен орган, агенција или друго тело кое обработува лични податоци во име на контролорот.

### *„Прима тел“*

значи физичко или правно лице, јавен орган, агенција или друго тело на кое му се откриваат личните податоци, без разлика дали е трето лице или не. Меѓутоа, јавните органи што можат да добијат лични податоци во рамките на одредена истрага во согласност со законот нема да се сметаат за примачи; обработката на

тие податоци од страна на јавните органи треба да биде во согласност со важечките правила за заштита на податоците во согласност со целите на обработката.

## *Киберпростор (cyber space)*

Термин воведен од писателот на научнофантастични романи Вилијам Гибсон во 1984 година.

Киберпросторот е местото каде што човечката интеракција се јавува преку компјутерски мрежи, преку е-пошта, игри или симулации.[3] Терминот киберпростор – (А) значи меѓузависна мрежа на инфраструктури за информатичка технологија; и (Б) вклучува интернет, телекомуникациски мрежи, компјутерски системи и вградени процесори и контролори.[4]

3 https://www.lexisnexis.co.uk/legal/glossary/cyberspace#:~:text=%27Cyberspace%27%20is%20where%20human%20interaction,through%20email%2C%20games%20or%20simulations

4 https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=50-USC-119985075-325479117&term_occur=999&term_src=title:50:chapter:35:section:1708

# 01
# ПРАВНА РАМКА

I.

# ПРАВНА РАМКА

Во правото, се води дискусија и постои своевидна конфузија околу тоа дали воопшто постои единствена правна рамка што може да ги обедини човековите права, личните податоци и се однесува на киберпросторот. Поради својата прекугранична, информациско-центрична природа, киберпросторот претставува предизвик за државниот пристап кон управувањето. Од една страна, физичката инфраструктура што го сочинува киберпросторот е предмет на национални јурисдикција и овластување. Од друга страна, протокот на податоци и информациите преку таа инфраструктура постојано можат да минуваат низ (повеќе) територијални јурисдикции, што отежнува една јурисдикција да врши „ефикасна контрола" над овој проток на информации. Ова доведе многумина да се повикаат на развој на нова нормативност, односно да се воведат режими за регулирање на киберпросторот.

Во денешно време не е спорно дека принципите на меѓународното право треба да бидат применливи во киберпросторот. Помалку јасно е како овие принципи се претвораат во практиката.

Следствено, овој јаз меѓу политиката и практиката доведува до правни несигурности, па дури и правни празнини што можат да ја поткопаат заштитата на човековите права на корисниците на интернет. Затоа, меѓународните и регионалните организации презедоа активности за иницијативи, со цел да се идентификува и да се толкува како постојните правни принципи на меѓународното право се применуваат во киберпросторот.[5]

Сепак, стремежот е колку што е можно повеќе да се стават во законска норма сите нови технолошки достигнувања, со цел тие да можат да се нормираат и да се регулира поведението. Доколку тоа не е направено во детали, правните празнини се пополнуваат според најсродната норма.

5 Guide to Good Governance in Cybersecurity, 2019, ©DCAF – Geneva Centre for Security Sector Governance, Geneva – 2019.

# Домашни правни норми, Устав, Закон за заштита на личните податоци, други прописи

Во рамките на домашниот правен поредок, се разбира, постојат Уставот, како највисок акт, и законите.

ЗЗЛП е легислативата што најдиректно ги регулира прашањата опфатени во овој водич. Другите процесни и материјални закони, како што се ЗПП, ЗКП, ЗОУП, ЗУС, Законот за облигации, Законот за електронски комуникации, Законот за медиуми итн., секој сам за себе е дел од мозаикот за заштитата на личните податоци, правото на приватност и човековите права.

Според Уставот[6], меѓународните инструменти се составен дел на домашниот правен поредок и тие имаат супрематија. Тие ќе бидат анализирани во делот меѓународно-правни инструменти.

# Меѓународно-правни инструменти

## *1.2.1. Универзална декларација за човекови права и Меѓународен пакт за граѓански и политички права*

Во рамките на меѓународниот поредок општо е прифатено дека меѓународното право за човекови права, вклучувајќи ги и Универзалната декларација за човекови права и Меѓународниот пакт за граѓански и политички права, се применува во дигиталниот простор. Ова го потврди Советот за човекови права (HRC) во резолуцијата A/HRC/20/L.13, со која се утврдува дека „истите права што луѓето ги имаат офлајн мораат да бидат заштитени и на интернет". Оваа резолуција е важна зашто тоа беше првпат меѓународното тело експлицитно да изјави дека заштитата на човековите права се однесува и на киберпросторот. По откритијата на Сноуден, ГСОН одлучи да се формира нов специјален известувач за правото на приватност со цел подобро да се одговори на приватноста во дигиталната ера и да се создаде побезбедна дигитална средина во 2015 година. Специјалниот известувач за правото на приватност има мандат да врши државни посети, да направи препораки и да се справува со поединечни жалби.

6 Член 110. Меѓународни договори

**ИЗВЕШТАЈ НА ГРУПАТА НА ВЛАДИНИТЕ ЕКСПЕРТИ НА ООН**

Извештајот на ОН за 2015 година ги наведува следните препораки за одговорно однесување на државите, за да придонесат за отворен, безбеден, стабилен, пристапен и мирен киберпростор:

ПОЗИТИВНИ НОРМИ:

- Државите треба да соработуваат за да ги зголемат стабилноста и безбедноста во користењето на ИКТ и да се спречат штетните ИКТ-практики.
- Државите треба да ги земат предвид сите релевантни информации во однос на атрибуцијата во ИКТ-околината.
- Државите треба да преземат соодветни мерки за заштита на националните критични инфраструктури од ИКТ-закани и да одговорат на соодветните барања за помош од друга држава.
- Државите треба да преземат разумни чекори за да обезбедат интегритет и да го спречат ширењето на малициозните ИКТ-алатки и ИКТ-техники.
- Државите треба да поттикнат одговорно известување за ранливостите на ИКТ и споделување на поврзани информации.

ОГРАНИЧУВАЧКИ НОРМИ:

- Државите не треба свесно да дозволат нивната територија да се користи за меѓународно ниво и за погрешни дејства со користење на ИКТ.
- Државите треба да се придржуваат до резолуциите на Генералното собрание на Обединетите нации поврзани со човековите права.
- Државите не треба да спроведуваат свесно поддршка на ИКТ-активност спротивно на нивните обврски според меѓународното право.
- Државите не треба да спроведуваат или свесно да поддржуваат активности за да им наштетат на информациските системи на овластените тимови за одговор при итни случаи.

## *1.2.2. Регулатива (EU) 2016/679 (General Data Protection Regulation)*

Оваа регулатива утврдува правила во врска со заштитата на физичките лица во однос на обработката на личните податоци и правилата што се однесуваат на слободното движење на личните податоци. Таа ги штити основните права и слободи на физичките лица, а особено нивното право на заштита на личните податоци.

Според неа, слободното движење на личните податоци во рамките на Унијата нема да биде ниту ограничено ниту забрането од причини поврзани со заштитата на физичките лица во однос на обработката на личните податоци.[7]

7 Regulation (EU) 2016/679 (General Data Protection Regulation), член 1.

Оваа регулатива се применува на обработката на личните податоци во контекст на активностите на воспоставување контролор или обработувач во Унијата, без оглед на тоа дали обработката се одвива во Унијата или не.[8]

### *1.2.3. Резолуција на ОН за создавање на глобална култура на кибербезбедност*

Друга важна резолуција на ГСОН е A/RES/57/239 за создавање на глобалната култура на кибербезбедноста што го препознава киберкриминалот како голем предизвик за кибербезбедноста.[9]

### *1.2.4. Водечки принципи на Обединетите нации за бизнис и човекови права*

Понатаму, инструментот на ОН релевантен за идентификација на нормите во киберпросторот се водечките принципи на Обединетите нации за бизнис и човекови права (познати и како „Принципи Раги"), усвоени во 2011 година. Принципите нудат насоки за државите и бизнисите во однос на заштитата на човековите права. Принципите Раги се засноваат на рамката на ОН – „Почитувај, заштити и лекувај". Во воведниот дел на овие водечки принципи е наведено дека „од деловните претпријатија како специјализирани органи на општеството што вршат специјализирани функции се бара да ги почитуваат сите важечки закони и да ги почитуваат човековите права".

Во контекст на регулирање на одредени форми на незаконски говор на интернет – говорот на омраза, извештајот на високиот комесаријат за човекови права на ОН, усвоен од Советот за човекови права во 2013 година (познат како „Акционен план Рабат"), ги идентификува критериумите, служи за идентификување на говорот на омраза и може да обезбеди насоки и во онлајн-доменот.

### *1.2.5. Европска конвенција за човекови права*

Еден од најмаркантните правни инструменти на 20 век, Конвенцијата, во текот на својата интерпретација преку член 8 дава дефиниција на она што значи правото на приватност во контекст на модерното време. Според ЕКЧП, член 8 и неговата интерпретација е опсегот каде што припаѓа правото на заштита на приватноста, личните податоци и нивното користење, како и заштитата на правата во интернет-просторот. Советот на Европа го има ЕСЧП како орган што дава интерпретација на конвенцијата и дава заштита преку индивидуални жалби. За да се повика на член 8, апликантот мора да покаже дека неговата или нејзината жалба спаѓа во најмалку еден од четирите интереси наведени во членот, имено: приватен живот, семеен живот, дом и кореспонденција.

8 Ibid., член 3.

9 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/22/PDF/N0255522.pdf?OpenElement

Се разбира, некои работи опфаќаат повеќе од еден интерес. Прво, Судот утврдува дали барањето на апликантот спаѓа во опсегот на член 8. Следно, Судот испитува дали имало мешање во тоа право или дали се ангажирани позитивните обврски на државата за заштита на правото. Условите под кои државата може да се меша во уживањето на заштитеното право се наведени во став 2 од член 8, имено, во интерес на националната безбедност, јавната безбедност или економската благосостојба на земјата, заради спречување безредие или криминал, за заштита на здравјето или моралот или за заштита на правата и слободите на другите. Ограничувањата се дозволени доколку се „во согласност со законот" или „пропишани со законот" и се „неопходни во едно демократско општество" за заштита на една од целите наведени погоре. Во оценката на тестот за неопходност во едно демократско општество, Судот често треба да ги балансира интересите на жалителот заштитени со член 8 и интересите на третата страна заштитени со други одредби од Конвенцијата и нејзините протоколи.[10]

## *1.2.6. Конвенција за компјутерски криминал на Советот на Европа*

Потребата за уедначување и систематизирање на глобално ниво на материјалните и процесните норми од областа на компјутерскиот криминал и електронските докази свој одраз најде во Конвенцијата за компјутерски криминал на Советот на Европа (во понатамошниот текст: Конвенцијата). Иако претходно постоеја обиди за дефинирање на материјалните норми што ја регулираат меѓународно-правната соработка, сепак Конвенцијата по својата сеопфатност, флексибилност и можност за лесно инкорпорирање во националните законодавства, иако првично наменета за државите во Европа, стана препознатлив механизам за лесна комуникација меѓу државите од целиот свет.

На Конвенцијата за компјутерски криминал подоцна се надоврзуваат и Конвенцијата за заштита на личните права при автоматизиран процес на обработка на личните податоци[11] со амандманите и Дополнителниот протокол за авторизиран проток на лични податоци надвор од државата[12], Дополнителниот протокол на Конвенцијата за компјутерски криминал за заштита од расизам и ксенофобија[13], Конвенцијата за заштита на децата од сексуална експлоатација и сексуално малтретирање[14] и Директивите на ЕУ.

Советот на Европа ја усвои Конвенцијата за компјутерски криминал во Будимпешта на 23.11.2001 година. Вкупно 58 држави се потписнички на Конвенцијата, од кои 28 со ратификација. Конвенцијата беше потпишана од страна на нашата држава на 23.11.2001 година, ратификувана на 15.09.2004 година, а влезе во сила на 01.01.2005 година.

10 https://www.echr.coe.int/documents/d/echr/guide_art_8_eng

11 https://azlp.mk/wp-content/uploads/2022/11/Zakon_za_ratifikacija_na_Konvencijata_108.pdf

12 https://azlp.mk/wp-content/uploads/2022/11/Dopolnitelen_protokol_Konvencija_108.pdf

13 https://www.pravdiko.mk/wp-content/uploads/2013/11/Dopolnitelen-protokol-na-Konventsijata-za-kompjuterski-kriminal-za-inkriminatsija-na-dela-od-rasistichki-i-kesnofobistichki-vid-ETS-189.doc

14 http://www.childrensembassy.org.mk/WBStorage/Files/Konvencija%20na%20Sovetot%20na%20Evropa%20za%20zastita%20na%20deca%20od%20seksualna%20zloupotreba.pdf

Конвенцијата содржи материјални, процесни норми и норми за меѓународна соработка. Одредбите од областа на материјалното право се однесуваат на: недозволен пристап, недозволено пресретнување, упад во податоци, упад во систем, злоупотреба на уред, фалсификување поврзано со компјутер, измама поврзана со компјутер, дела поврзани со детска порнографија, дела поврзани со повреда на авторски и други сродни права.

Според Објаснувачкиот протокол кон Конвенцијата за компјутерски криминал од 2001 година, брзите случувања во областа на информатичката технологија имаат директно влијание врз сите делови на современото општество. Интеграцијата на телекомуникациските и информациските системи овозможува складирање и пренос, без разлика на оддалеченоста, на сите видови комуникација, што отвора цел опсег на нови можности. Овие случувања беа поттикнати со појавата на информативни супераутопати и мрежи, вклучително и интернет, преку кои практично секој ќе може да има пристап до која било електронска информативна услуга, без разлика каде се наоѓа. Преку комуникациските и информативните услуги, корисниците создаваат еден вид заеднички простор, наречен „киберпростор", кој се користи за легитимни цели, но може да биде и предмет на злоупотреба и доверливост на компјутерските системи и телекомуникациските мрежи или тие се состојат од употреба на такви мрежи на нивните услуги за извршување на традиционални прекршоци. Прекуграничниот карактер на таквите прекршоци, на пример, кога е извршено преку интернет, е во конфликт со територијалноста на националните органи за спроведување на законот.[15]

### *1.2.7. Конвенција за заштита на лица во однос на автоматска обработка на лични податоци*

Според Објаснувачкиот меморандум кон оваа конвенција, правото на почитување на семејниот и приватниот живот е предвидено во член 8 од ЕКЧП. Ова право дополнително се толкува со судската практика на Судот и дополнето и засилено е со Конвенцијата 108 на Советот на Европа.

Приватниот живот е поим што не е подложен на исцрпна дефиниција. Судот нагласи дека член 8 опфаќа широк опсег на интереси, имено приватен и семеен живот, дом и кореспонденција, вклучувајќи пошта, телефонски комуникации и е-пошта на работното место. Приватниот живот се однесува на правото на една личност на својот имиџ, на пример со помош на фотографии и видеоклипови. Исто така, се однесува на идентитетот и личниот развој на една личност, правото на воспоставување и развивање односи со други човечки суштества. Опфатени се и активности од професионална или деловна природа.

15 https://rm.coe.int/16800cce5b

# 02
# ПРАВО НА ПРИВАТНОСТ И ЗАШТИТА НА ПОДАТОЦИ

II.

# ПРАВО НА ПРИВАТНОСТ И ЗАШТИТА НА ПОДАТОЦИ

Анализирајќи ги овие два термина, тие не претставуваат синоними. Во праксата има различни дебати околу финесите на овие две права. Но, едно е јасно, правото на приватност е поширок поим од заштитата на податоци.

## 2.1. Право на приватност

Приватноста не е само индивидуално право туку и општествена вредност. Тоа е врежано во концептот на индивидуализмот, слободата и правото на заштита на индивидуата. Во некои држави, на пример во САД, приватноста често се смета за елемент на слободата, односно тоа претставува право да се биде ослободен од упади од страна на државата. Приватноста е едно од основните права и речиси секоја земја во светот, на некој начин, ја признава приватноста, било да е тоа во нивниот устав или во други одредби, бидејќи правото на приватност или приватен живот е вградено во Универзалната декларација за човекови права (член 12), Европската конвенција за човекови права (член 8) и Европската повелба за фундаментални права (член 7).

Една од иманентните разлики е таа што приватноста е признаена како универзално човеково право, додека заштитата на податоците не е (барем сè уште не е).[16]

## 2.2. Концепт на заштита на податоци

Заштитата на податоците се однесува на заштита на какви било информации што се однесуваат на идентификувано или препознатливо физичко лице, вклучувајќи имиња, датуми на раѓање, фотографии, видеоснимки, е-адреси и телефонски броеви. Други информации, како што се ИП-адресите и комуникациската содржина – поврзани или обезбедени од крајните корисници на комуникациските услуги – исто така се сметаат за лични податоци.

Поимот за заштита на податоците потекнува од правото на приватност. И двете се инструментални за зачувување и промовирање на основните вредности и права; и да остваруваат други права и слободи – како што е слободата на говор или правото на собирање.

Заштитата на податоците има прецизни цели да обезбеди правична обработка (собирање, употреба, складирање) на личните податоци и од јавниот и од приватниот сектор.[17]

16 https://edps.europa.eu/data-protection/data-protection_en

17 Ibid.

## 2.3. Заштита од индиректна идентификација

Сите актери наведени во овој водич кои работат или имаат допир со податоци важно е да знаат дека информациите што ги имаат можат да доведат до тоа индиректно да се идентификува извесен поединец и затоа дури и таквите навидум посредни или индиректни податоци добиваат третман на лични податоци. Со тоа, тие подлежат на системот на заштита според GDRP/ЗЗЛП.

Ако поединец не може да се идентификува директно од информациите што ги обработува професионалецот (на пример, кога сите идентификатори се отстранети), тоа не значи дека поединецот не може да биде идентификуван на друг начин, на пример, од информациите што претходно ги поседувал професионалецот (оној што ги употребува, обработува) или информациите што треба да ги добијат од друг извор. Слично на тоа, трето лице може да ги користи информациите што ги поседува професионалецот, па доколку ги комбинира со други информации што му се достапни на тоа трето лице, процесот може да доведе до идентификација на поединецот.

Во ваков случај, товарот на оцена паѓа на секој актер наведен во овој водич, кој треба да процени кои информации најверојатно ќе се користат за обработка, а кои би довеле до откривање на поединецот, односно негово идентификување со цел да се избегне ненамерно да објави или да открие информации што би можеле да се поврзат со други информации и (несоодветно) да се идентификува поединецот.

### Кои се тие информации што можат да го откријат поединецот индиректно?

Не постои исцрпна листа, но приближно вакви информации, односно нивно комбинирање може да доведе до идентификација на поединецот:

- регистарски број на автомобил,
- број на пасош, или
- комбинација на значајни критериуми (на пример, возраст, занимање, место на живеење).

Клучната точка на индиректната идентификација е кога информациите се комбинираат со други информации што потоа разликуваат и овозможуваат идентификација на поединецот.

## 2.4. Право на заштита на податоци

Приватноста и заштитата на податоците се две права содржани во Договорите на ЕУ и во Повелбата за основни права на ЕУ.[18] Повелбата содржи експлицитно право на заштита на личните податоци (член 8). Влегувањето во сила на Лисабонскиот

18 https://edps.europa.eu/data-protection/data-protection_en

договор во 2009 година, на Повелбата за основните права ѝ даде иста правна вредност како и уставните договори на ЕУ. Така, институциите и телата на ЕУ и земјите-членки се обврзани со него. Дополнително, член 16 од Договорот за функционирање на Европската унија (ТФЕУ) ја обврзува ЕУ да утврди правила за заштита на податоците за обработка на лични податоци. ЕУ е единствена што предвидува таква обврска во нејзиниот устав.

## 2.5. Прописи за заштита на лични податоци

Во април 2016 година, ЕУ усвои нова правна рамка – Општата регулатива за заштита на податоците (GDPR) и Директивата за заштита на податоците за областа на спроведувањето на законот и полицијата.

Целосно применлив низ ЕУ во мај 2018 година, GDPR е најсеопфатниот и најпрогресивен дел од законодавството за заштита на податоците во светот, ажуриран за да се справи со импликациите на дигиталната ера.

Република Северна Македонија ја има транспонирано оваа регулатива преку донесувањето на ЗЗЛП.

# 03
# ХОРИЗОНТАЛЕН ПРИСТАП

III.

# ХОРИЗОНТАЛЕН ПРИСТАП

Заштитата на податоците е хоризонтално прашање, што во основата значи дека во секој конкретен сектор треба да се земе предвид Законот за заштита на личните податоци (ЗЗЛП) за секоја правна работа што е предмет на решавање. Понатаму, исто така треба да се земат предвид и законите што можат да содржат одредби за заштита на податоци специфични за секторот (закон за телекомуникации, закон за е-трговија, закон за медиуми итн.) што соодветно треба да се применат. Овие прописи исто така мораат да бидат земени предвид при решавањето на конкретна правна ситуација.

Покрај законите, при оценувањето на случаите поврзани со заштитата на податоците ќе се земе предвид и судската практика на Европскиот суд за човекови права (ЕКЧП), имајќи ги предвид аспирациите на нашата држава кон Европската унија и соодветните правни резонирања на Европскиот суд на правдата (ЕСП). Исто така, би можело да биде корисно да се повикаат насоките и мислењата на Европскиот одбор за заштита на податоци (одбор каде што се претставени сите органи за заштита на податоци на земјите-членки на ЕУ).

## 3.1. Принципи за заштита на податоци

ЗЗЛП ги утврдува принципите со кои се регулира обработката на личните податоци.

Овие принципи опфаќаат:

- законитост,
- правичност и транспарентност,
- ограничување на целта,
- минимизирање на податоците,
- точност на податоците,
- ограничување на складирањето,
- интегритет и доверливост,
- одговорност.[19]

19 ЗЗЛП, член 9.

### 3.1.1. Законитост

Обработката на личните податоци ќе се смета дека е законита само доколку се врши врз некој од основите што се дозволени, односно определени во легислативата.[20]

### 3.1.2. Правичност

Кога е задоволена законитоста како принцип, тогаш се преминува на воспоставување на правична, односно фер обработка. Тоа значи дека субјектот на личните податоци мора да биде свесен дека ќе се обработуваат неговите лични податоци. Тоа ќе му овозможи да донесе информирана одлука за тоа дали се согласува со таквата обработка и ќе му овозможи исполнување на своите права во однос на заштитата на своите лични податоци.

20 Законитост на обработката на личните податоци
Член 10
(1) Обработката на личните податоци е законита само ако и до оној степен доколку е исполнет најмалку еден од следните услови:
– субјектот на лични податоци дал согласност за обработка на неговите лични податоци за една или повеќе конкретни цели,
– обработката е потребна за исполнување договор каде што субјектот на лични податоци е договорна страна или за да се преземат активности на барање на субјектот на лични податоци пред неговото пристапување кон договорот,
– обработката е потребна за исполнување на законска обврска на контролорот,
– обработката е потребна за заштита на суштинските интереси на субјектот на лични податоци или на друго физичко лице,
– обработката е потребна за извршување работи од јавен интерес или при вршење на јавно овластување на контролорот утврдено со закон,
– обработката е потребна за целите на легитимните интереси на контролорот или на трето лице, освен кога таквите интереси не преовладуваат над интересите или основните права и слободи на субјектот на лични податоци што бараат заштита на личните податоци, особено кога субјектот на личните податоци е дете.
(2) Одредбите од став 1 алинеја 6 на овој член нема да се применуваат за обработка на личните податоци од страна на органите на државната власт при спроведување на нивните надлежности.
(3) Правната основа за обработка на личните податоци наведена во став 1 алинеја 3 и 5 на овој член се утврдува со закон. Во законот задолжително се предвидуваат одредби за: условите што ја одредуваат законитоста на обработката од страна на контролорот, целите на обработката, категориите на лични податоци што се предмет на обработката, категориите на субјекти на личните податоци; субјекти на кои можат да бидат откриени личните податоци, како и целите за кои се откриваат личните податоци, ограничувањата во однос на целите на обработка, периодот на чување, операциите и постапките за обработка, вклучувајќи и мерки за обезбедување на законска и правична обработка, а со цел да се исполни целта од јавниот интерес и да биде пропорционално на извршување на легитимната цел. Законот мора да содржи и процена на влијанието на заштитата на личните податоци за случаите предвидени во член 39 од овој закон.
(4) Ако личните податоци се обработуваат за друга цел различна од целта за која првично биле собрани, при што обработката не се врши врз основа на согласност на субјектот на личните податоци или врз основа на закон, кој е неопходна и пропорционална мерка за заштита на целите утврдени во член 27 став 1 од овој закон, тогаш контролорот, за да утврди дали обработката за други цели е во согласност со првичната цел за која биле собрани личните податоци, е должен, меѓу другото, да ги земе предвид:
– секоја поврзаност помеѓу целите заради кои се собираат личните податоци и целите за предвидената понатамошна обработка,
– контекстот во кој биле собрани личните податоци, особено во поглед на односите помеѓу субјектите на лични податоци и контролорот,
– природата на личните податоци, а особено дали се обработуваат посебни категории на лични податоци согласно со член 13 од овој закон или се обработуваат лични податоци што се однесуваат на казнени осуди и казнени дела согласно со член 14 од овој закон – можните последици од предвидената понатамошна обработка за субјектите на лични податоци,
– постоењето на соодветни заштитни мерки што можат да вклучуваат криптирање или псевдонимизација.

### 3.1.3. Транспарентност

Директно поврзан со принципот на правична обработка е принципот на транспарентност, што значи дека контролорот мора да биде отворен и јасен кон субјектот на личните податоци при обработка на неговите лични податоци. Наместо досегашното известување на Агенцијата за заштита на личните податоци за збирките на лични податоци што се обработуваат, со новите законски правила контролорот има обврска да ги известува субјектите на личните податоци за тоа. Известувањето мора да биде навремено, со користење на јасен и едноставен јазик.

### 3.1.4. Ограничување на целта

Ограничувањето на целта подразбира дека контролорите можат да ги обработуваат личните податоци само за исполнување на конкретни, јасни и легитимни цели. Тоа значи дека контролорите најпрвин мораат да ја идентификуваат конкретната цел за чие исполнување ќе ги обработуваат личните податоци и таа идентификувана конкретна цел да ја претставува рамката во којашто ќе се одвива обработката. Понатамошната (секундарна) обработка, за цел поинаква од првичната, може да биде законска само доколку се смета за компатибилна со првичната цел за чие исполнување на личните податоци биле првично обработувани.

### 3.1.5. Минимален обем на податоци

Принципот на обработка на минимален обем на податоци значи дека контролорите ќе ги обработуваат само оние лични податоци што се соодветни, релевантни и ограничени на она што е неопходно за остварување на целта. Контролорот мора да се осигури дека обработката е навистина неопходна и дека обемот на лични податоци што се обработуваат се пропорционални со целта на обработка.

### 3.1.6. Точност

Принципот на точност подразбира дека контролорот мора да имплементира соодветни мерки за личните податоци што ги обработува. Тие да бидат точни и, доколку е потребно, ажурирани, како и мерки за навремено бришење и коригирање на личните податоци што се неточни или нецелосни.

### 3.1.7. Ограничување на рокот на чување

Според овој принцип, личните податоци ќе се чуваат во форма што овозможува идентификација на субјектите на личните податоци не подолго отколку што е потребно за исполнување на целите поради кои се врши обработката. Со други зборови, обработката на личните податоци ќе се врши само онолку време колку

што е неопходно за да се исполни целта поради која се обработувале личните податоци.

### *3.1.8. Интегритет и доверливост*

Личните податоци можат да се обработуваат само на начин што обезбедува соодветно ниво на безбедност на личните податоци со примена на соодветни технички или организациски мерки. За да ги заштитат личните податоци, контролорите треба да имплементираат систем за информациска сигурност што е подетално опишан во седмото поглавје од овој прирачник. При процена и воспоставување на системот за информациска сигурност, честа и добра практика е тимот да биде составен од правници и технички лица со цел посоодветно дефинирање на стратегиите и политиките на контролорот.

### *3.1.9. Одговорност*

Одговорноста во сферата на личните податоци е двонасочна улица. Секој е должен да се грижи за заштитата на сопствените лични податоци и да не ги изложува на јавноста или да ги доведува во опасност да бидат злоупотребени. Секако, одговорност имаат и сите што на кој било начин вршат обработка, складирање и располагање со личните податоци што им се направени достапни врз основа на законски предвидени основи и цели.

# 04

# КОРИСТЕЊЕ НА ЛИЧНИ ПОДАТОЦИ ВО ЗАКОНСКИ ЦЕЛИ И ВРЗ ОСНОВА НА ЗАКОНСКА ПРАВНА РАБОТА

IV.

# КОРИСТЕЊЕ НА ЛИЧНИ ПОДАТОЦИ ВО ЗАКОНСКИ ЦЕЛИ И ВРЗ ОСНОВА НА ЗАКОНСКА ПРАВНА РАБОТА

Концептот на доверување на лични податоци, односно нивната обработка, складирањето и нивното располагање во законски цели подразбира добивање согласност од субјектот. Во определени случаи не е потребна согласност, кога за тоа постојат правно валидни и оправдани причини и околности. Сепак, обврската за грижа останува иста.

## 4.1. Согласност

Во денешно време, со напливот на новите технологии, речиси и да нема веб-сајт, апликација, социјална мрежа или друг вид мрежа за споделување податоци што нема свои правила што бараат да се согласиме со нив, пред да ги користиме. Овие правила најчесто се во форма на правила за користење, правила за колачиња и правила и/или политика за приватност, EULA (End User License Areement – договор со краен корисник итн.). Есенцијално, согласноста претставува влегување во контрактуален однос, кој може да биде прекинат под условите наведени во тие правила, односно договор. Принципите што мораат да се запазат при давањето согласност се следните:

### *4.1.1. Слободно дадена согласност*

• Го подразбира изборот што субјектот на лични податоци го има дали ќе ја даде согласноста или не, како и можноста таа да ја повлече во кое било време. Во проценувањето дали согласноста е слободно дадена особено треба да се земе предвид дали субјектот на личните податоци е условен со извршувањето договор во којшто тој е договорна страна.

### *4.1.2. Конкретна согласност*

• Подразбира дека субјектот се согласил само за конкретна обработка на неговите лични податоци. Доколку контролорот врши обработка на личните податоци во повеќе процеси, посебна согласност треба да биде дадена за секој процес посебно.

### *4.1.3. Информирана согласност*

• Подразбира дека субјектот на личните податоци ја дал согласноста откако претходно му биле презентирани сите детали за обработката на јазик и во форма што се разбирливи за да може соодветно да го процени влијанието што обработката може да го има врз него.

### *4.1.4. Недвосмислена согласност*

• Подразбира дека дадената изјава или потврдното дејство на субјектот не остава простор за сомнеж во неговата намера да се согласи на обработката на неговите лични податоци.

## 4.2. Кога не е потребна согласност

Според ЗЗЛП, согласноста на субјектот на податоците не е единствената правна основа за обработка на податоците.

На пример, обработката на податоците може да се заснова и на одреден закон или легитимен интерес што го следи контролорот или трето лице, освен кога таквите интереси се надминати од интересот на основните права и слободи на субјектот на податоците. Оваа одредба, односно постулат, мора да се толкува тесно, што се однесува конкретно на оние случаи кога би била неопходна согласност од субјектот на податоците.

Во практиката, оваа одредба се применува за компјутерски криминал, на пример, за случаи кога сторителите дејствуваат под лажен профил (под име на друго лице), користејќи лични податоци за да извршат измама или кога обработуваат податоци поврзани со детска порнографија или кога објавуваат фотографии и други чувствителни информации поврзани со други лица на интернет за да му наштетат на достоинството и угледот на овие лица со нивно изложување во јавноста.

## 4.3. Права на субјектот на лични податоци

Субјектот треба:

- Да биде информиран за идентитетот на контролорот и неговиот претставник во Република Северна Македонија;
- Да оствари увид во збирката на лични податоци;
- Да знае кои лични податоци се чуваат за него во електронска или во хартиена форма;
- Да ги знае целите на обработката на неговите лични податоци;
- Да ги знае корисниците или категориите корисници на податоците;
- Да не се согласи со употребата на податоците за комерцијални цели или нивен пренос на трети лица заради такви цели;
- Да има пристап до податоците и да изврши нивна исправка.

IV.

На пример:

„Фејсбук“ ги користи податоците добиени од корисниците на својата социјална мрежа за да обезбеди повеќе насочени пазари за огласувачите. „Гугл“ е во состојба да го идентификува интересот на корисниците или веб-локациите што се посетени преку анализа на барањата за пребарување на корисниците на неговата услуга на пребарувачот, како комерцијална основа за насочена реклама. Кога креирате сметка со „Фејсбук“ или „Гугл“, постои политика за приватност со која се согласувате пред да продолжите со кликнување на „регистрирај се“ или „во ред“.

## 4.4. Принцип на пропорционалност

Пропорционалноста значи рамнотежа помеѓу употребените средства и наменетата цел. Принципот на пропорционалност значи воспоставување разумна рамнотежа помеѓу обработката на податоците и наменетата цел. Со други зборови, тоа значи дека обработката на податоците е до степен до кој ја исполнува целта.

За да се намалат недостатоците и ризиците за уживањето на правата на приватност и заштита на податоците важно е ограничувањата да содржат соодветни заштитни мерки.

Кога правото на приватност и заштитата на податоците, од една страна, и другите човекови права, од друга страна, се спротивставени, принципот на пропорционалност е главната правна алатка што се користи за балансирање на различните човекови права. Потоа, треба да се направи тест за балансирање.

Тестот на пропорционалност се врти околу три чекори: соодветност (дали мешањето е навистина соодветно за да се постигне наводната цел), неопходност (исто така „помалку рестриктивна алтернатива“ или „минимално оштетување“; дали преземената мерка е најмалку рестриктивната алтернатива) и пропорционалност во строга смисла (дали придобивките што се постигнати се надминати со ограничувањата предизвикани). Понатаму, обработката на податоците мора да се мора да се заснова на националното право и да се стреми кон легитимна цел.

# 05

# БЕЗБЕДНОСТ ВО КИБЕРПРОСТОРОТ – КИБЕРБЕЗБЕДНОСТ И КИБЕРХИГИЕНА

V.

# БЕЗБЕДНОСТ ВО КИБЕРПРОСТОРОТ – КИБЕРБЕЗБЕДНОСТ И КИБЕРХИГИЕНА

Особено во социјалните мрежи приватните лични податоци се достапни за трети лица, понекогаш дури и објавени и затоа достапни за секого. Исто така, тие можат да содржат приватни информации, како лични фотографии, и информации што – во аналогниот свет не би биле лесно достапни. Многу прекршувања на заштитата на податоците се случуваат во онлајн-околината. Лицата кои вршат прекршување на заштитата на податоците ја користат опасноста од интернетот, а понекогаш и од невнимателноста на корисниците и ги обработуваат личните податоци на корисниците за свои цели.

## 5.1. Три типа кибербезбедност

Полето за кибербезбедност опфаќа огромен опсег на алатки и техники, што есенцијално подразбира:

### *5.1.1. Безбедност на податоците*

Хакерите често бараат податоци. Сакаат да гледаат или да украдат информации што се надвор од границите. Нивните причини се различни. Во некои случаи, хакерот едноставно краде информации како броеви на кредитни картички за да ги продаде на црниот пазар (Dark web). Во други случаи, целта не е лукративна, туку е да се наштети со објавување на лични податоци или, пак, само да се добијат податоците сами по себе, со цел да се задоволат политички, деловни или други апетити. Безбедноста на податоците вклучува заштита на податоците од неовластен пристап. Вклучува шифрирање податоци, технологии и политики за контрола на пристап до податоци.

### *5.1.2. Мрежна безбедност*

За да може да функционира кибернападот, во речиси секоја ситуација најпрвин е потребно хакерот да добие пристап до мрежата на целта. Заштитата на мрежите е една од најсериозните области на кибербезбедноста и обично е фокус на

значителни инвестиции. Мрежна безбедност е збир на правила и конфигурации дизајнирани да го заштитат интегритетот, доверливоста и пристапноста на компјутерските мрежи и податоци со користење на софтверски и хардверски технологии.

### *5.1.3. Безбедност на апликациите*

Хакерите исто така сакаат да влезат во софтверски апликации како Enterprise Resource Planning (ERP), CRM, сервери за е-пошта и слично. Присутноста внатре во апликацијата е одличен начин да се шпионира целта или да се наруши нејзиното работење. Безбедноста на апликациите има многу аспекти, но обично ги комбинира политиките (на пример, кому му е дозволен пристап до апликацијата и нејзиниот административен „заден крај“) и контролите врз интерфејсите за програмирање на апликациите (API) што им дозволуваат на другите софтверски програми да добијат пристап до апликацијата.

## 5.2. Типови закани

Според тоа кон кого можат да бидат насочени, заканите се делат на:

- Закани кон лица
- Закани кон имот
- Закани кон систем

Постојат седум вообичаени типа закани за кибербезбедноста. Киберзаканата е метод за напад на средство за податоци. Тоа не е вистинскиот напад. Тоа е повеќе како план за напад. Таму има буквално стотици милиони киберзакани. Во принцип, тие се следните:

ВИРУСИ/МАЛВЕР – Вирусот е форма на код за злонамерен софтвер што сам се инсталира на вашиот уред. Откако ќе се вгради, вирусот може да направи повеќе различни лоши работи, вклучително и замрзнување на системот, кражење податоци, па дури и киднапирање на уредот за криминални цели како ископување криптовалути без ваша дозвола, на пример, „криптоџекинг“.

КРАЖБА НА ИДЕНТИТЕТ – Кражба на идентитет е кривично дело каде што хакер краде доволно од вашите приватни, лични информации (на пример, број на социјално осигурување, датум на раѓање, адреса итн.) за да може да ве имитира. Преправајќи се дека сте вие, хакерот можеби ќе може да украде пари од вашата банкарска сметка, да отвори сметки на кредитни картички на ваше име и многу повеќе.

НАПАДИ СО ЛОЗИНКА – Ако хакер ја има вашата лозинка, тој или таа може да влезе во вашите сметки. Нападите со лозинки користат специјален софтвер за погодување лозинки, честопати испробувајќи илјадници можности пред да ја погодат точната.

„ТРОЈАНЦИ“ – Како и познатиот Тројански коњ од античките времиња, тројанецот е кибернапад што навлегува во мрежата на целта под лажни изговори. На пример, хакер може да вгради вирус во ПДФ-документ и да ви го испрати како прилог на е-пошта. Кога ќе го отворите ПДФ-от, датотеката го вградува вирусот во вашиот систем додека документот се отвора во „Акробат ридер“.

РАНСОМВЕР – Варијанта на малициозен софтвер што ги шифрира вашите податоци и ве тера да платите откуп, обично во биткоин, за да го отклучите.

ФИШИНГ – Обид, обично преку е-пошта, да ве измами да кликнете на хиперврска што ќе постави малициозен софтвер на вашиот компјутер. Пософистициран облик на напад, познат како спиар фишинг, го вклучува напаѓачот како имитирање пријател или колега, обично со цел да ве натера да ги споделите акредитивите за најавување на сметката. Фишинг е социјално-инженерска техника што се користи за кражба на податоци или за измама. Тоа се прави со испраќање на лажни реклами преку лажни интернет-страници до доверливи корисници. Рекламите обично содржат продажни промоции за различна стока, вклучувајќи, на пример, додатоци или возила по примамливо ниски цени. Ова е направено за да се намамат потенцијалните жртви да споделуваат чувствителни информации, како што се лични податоци, кориснички имиња и лозинки, како и податоци за платежна картичка и банка.

НАПРЕДНА ПОСТОЈАНА ЗАКАНА (APT) – АПТ се веројатно најмоќните киберзакани. АПТ е дизајниран да навлезе скришум, а потоа да демне во вашата мрежа со месеци, неоткриен. Се движи странично, инсталирајќи се одново и одново во различни делови од вашата инфраструктура додека не се активира. Потоа, може да направи неверојатна штета.

## 5.3. Киберхигиена

Киберхигиената се однесува на збир практики и мерки што можете да ги преземете за да ја одржите вашата дигитална безбедност и да се заштитите од киберзакани. Исто како што практиките за лична хигиена, како миење раце и четкање на забите, помагаат да се спречи ширењето на бактерии и болести, така практиките за киберхигиена помагаат да се спречи ширењето на малициозен софтвер, вируси и кибернапади.

# 06

# РАЗЛИЧНИ „АКТЕРИ“ НА ТЕРЕНОТ НА ЗАШТИТАТА НА ПРИВАТНОСТА И ЛИЧНИТЕ ПОДАТОЦИ

VI.

# РАЗЛИЧНИ „АКТЕРИ“ НА ТЕРЕНОТ НА ЗАШТИТАТА НА ПРИВАТНОСТА И ЛИЧНИТЕ ПОДАТОЦИ

Прашањето за заштита на личните податоци е комплексно. Тоа е конгломерат на мерки, активности, органи, лица и компании кои немаат секогаш јасни и делимитирани граници и надлежности.

## 6.1. Собрание на Република Северна Македонија

Законодавниот дом ја дава уставната и законската рамка, inter alia и во оваа област. За потребите на овој водич е важно да се напомене дека концептот на независно надзорно тело е имплементиран во правниот поредок на РСМ, преку Агенцијата за заштита на лични податоци, која, пак, за својата работа одговара пред Собранието на Република Северна Македонија.[21]

## 6.2. Агенција за заштита на лични податоци

Како самостојно и независно регулаторно тело, нормативно исклучително јасно и силно е фундирана и афирмирана независноста на оваа институција. Агенцијата е целосно политички, финансиски и функционално независна при извршувањето на своите надлежности, задачи и овластувања и нејзините директор, заменик и вработените не смеат да примаат и да бараат инструкции од органите на државната власт, органите на општините, органите на градот Скопје и од кои било други правни и/или физички лица.

Својата надзорна функција оваа агенција ја врши преку супервизија, која може да биде:

- редовна супервизија,
- вонредна супервизија, и
- контролна супервизија.

21 ЗЗЛП, член 57.

Во рамките на своите надлежности АЗЛП може да поведе прекршочна постапка и да изрече парични казни на контролор кој ќе направи повреда на заштитата на податоците што е казниво поведение согласно одредбите на ЗЗЛП.

За својата работа одговара пред Собранието, а контрола на нејзините одлуки врши судството, согласно уставниот принцип во член 15 од Уставот и член 6 од ЕСЧП.[22]

Според ЗЗЛП, Агенцијата не е надлежна да врши надзор над судовите кога постапуваат во рамките на нивните судски функции, освен за надзор над законитоста на преземените активности при другата обработка на лични податоци што се врши од страна на судовите согласно со законот.

## 6.3. Судови

Според Уставот, гарантирана е судска заштита против актите на државната управа и државните органи. Исто така, правото на пристап до суд под еднакви услови за сите е исто така гарантирано право. Во РСМ, судовите се организирани според принципот на редовни судови. Редовните судови се организирани според принципот на стварна надлежност, и тоа во најосновната поделба се делат на граѓански, кривични судови, од една страна, и управни судови, од друга.

Судот во оваа област се јавува во двојна улога. Првата како контролор на податоците што ги има, бидејќи судиите не се имуни да не мораат да ги следат законите за заштита на податоците. На пример, при спроведувањето на нивните постапки тие треба да го земат предвид принципот на минимизирање на податоците (можат да собираат/обработуваат само лични податоци што се неопходни за постапката) и правилно да ги анонимизираат своите пресуди. Во списите ќе се обработуваат само личните податоци што се релевантни за решавање на случајот. Посебно внимание мора да се посвети на степенот до кој страните имаат пристап до досиејата. На пример, осомниченият не смее да има пристап до личните податоци на жртвата или на сведоците, како што се адресата, телефонскиот број и други податоци што се чувствителни во врска со ова.

Понатаму, судот се јавува во својство на актер во заштита на јавниот и приватниот интерес во врска со личните податоци. Овие својства ќе бидат разгледани подетално подолу.

### *6.3.1. Управни судови*

Управните судови inter alia се надлежни за давање на судска заштита на одлуките на Агенцијата за заштита на лични податоци, односно обезбедуваат правна заштита од областа на управната материја, а во врска со заштитата на лич-

22 Устав на РСМ, член 15

ни податоци и примената на ЗЗЛП. Овие судови ги обезбедуваат принципите на уставност и законитост (во поширока смисла, заедно со примена на меѓународните стандарди).

### *6.3.2. Граѓански судови (граѓанска област)*

Прашањето на заштита на личните податоци и човековите права, особено со киберпросторот, не е ограничено само на заштита на податоците и осигурувањето дека нечии податоци се правилно чувани. Консеквенција на лошата обработка, чување или откривање на податоците секако дека може да претставува повреда на личните права, за што е предвидена соодветна заштита пред граѓанските судови, за надоместок на штета. Во ваквите предмети владее правилото nemo iudex sine actore, како и принципот actori uncubit probatio. Првиот значи дека судот не постапува ex officio, туку само кога е повикан да расправа по истакнато правозаштитно барање (тужба), а на тужителот е да докаже дека елементите се исполнети на правната норма на која се повикува.[23] Во ваквите случаи, согласно општите принципи за надоместок на штета тужителот обично треба да докаже дека:

- постои штетно дејство (што може да биде со активно поведение или со пропуштање) и таквото соодветно да го опише, односно да го објасни;
- постои идентификуван штетник, кој е одговорен за таквото дејство или, пак, не презел мерки на надзор со цел да ги спречи таквите дејства или да го ремедира пропуштањето со тоа што ќе се постапи и да го идентификува него;

23 Основи на одговорноста
Член 141
(1) Тој што со вина ќе му причини штета на друг, должен е да ја надомести.
(2) За штета причинета од предмети или дејности од кои произлегува зголемена опасност од штета за околината, се одговара без оглед на вината.
(3) За штета без оглед на вината се одговара и во други случаи предвидени со закон.

Штета
Член 142
Штетата е намалувањето на нечиј имот (обична штета) и спречувањето на негово зголемување (испуштена корист), како и повреда на личните права (нематеријална штета).

Барање да се отстрани опасноста од штета
Член 143
(1) Секој може да бара од друг да го отстапи изворот на опасност од кој му се заканува позначителна штета нему или на неопределен број лица, како и да се воздржи од дејност од која произлегува вознемирување или опасност од штета, ако настанувањето на вознемирувањето или на штетата не може да се спречи со соодветни мерки.
(2) Судот, на барање од заинтересираното лице, ќе нареди да се преземат соодветни мерки за спречување на настанувањето на штета или вознемирување или да се отстрани изворот на опасноста, на трошок на држателот на изворот на опасноста, ако тој самиот не го стори тоа.
(3) Ако штетата настане во вршењето на општокорисна дејност за која е добиена дозвола од надлежниот орган може да се бара само надоместок на штетата што ги преминува нормалните граници (прекумерна штета).
(4) Во случајот од став 3 на овој член, може да се бара преземање на општествено оправдани мерки за спречување на настанувањето на штетата или за нејзино намалување.

Барање да се престане со повреда на личните права
Член 144
(1) Секој има право да бара од суд или од друг надлежен орган да нареди престанување на дејство со кое се повредува неговото лично право и да нареди отстранување на последиците настанати со ова дејство.

- е нанесена штета во кој било нејзин облик, а најчесто нематеријална штета како резултат на повреда на личните права, која соодветно треба да се објасни во што се состои;[24]
- постои nexus помеѓу штетното дејство и штетникот;
- штетата соодветно ќе се квантифицира со употреба на правилата за докажување и доказните средства на располагање;
- ако не може да се квантифицира штетата, односно нејзиното квантифицирање би предизвикало значителни тешкотии, тогаш Судот може да одлучи по слободна оцена.[25]

24 Како се надоместува нематеријалната штета
Член 187-а
Нематеријалната штета се надоместува нематеријално (морална сатисфакција) и материјално (материјална сатисфакција) во случаите предвидени со закон.

Објавување пресуда или исправка
Член 188
Во случај на повреда на личните права оштетениот може да бара, а судот да нареди на трошок на штетникот, објавување на пресудата, односно исправката, повлекување на изјавата со која е сторена повредата или нешто друго со што може да се оствари целта што се постигнува со справедливиот паричен надоместок.

Справедлив паричен надоместок
Член 189
(1) Во случај на повреда на личните права судот, ако најде дека тежината на повредата и околностите на случајот го оправдуваат тоа, ќе досуди справедлив паричен надоместок, независно од надоместокот на материјална штета, како и во нејзино отсуство.
(2) При одлучувањето за барањето за справедлив паричен надоместок судот ќе води сметка за силината и траењето на повредата со која биле предизвикани физички болки, душевни болки и страв, како и за целта за која служи надоместокот, но и за тоа надоместокот да не е во спротивност со стремежите кои не се спојливи со неговата природа и општествената цел.
(3) За повреда на правото на углед и другите лични права на правните лица судот, ако најде дека тежината на повредата и околностите на случајот го оправдуваат тоа, ќе досуди справедлив паричен надоместок, независно од материјалната штета, како и во нејзино отсуство.
(4) Покрај овие правила, во одделни случаи, кога тоа со друг закон поинаку е уредено ќе се применуваат и правилата од тој закон.

25 ЗПП
Член 209
Ако се утврди дека на странката ѝ припаѓа правото на надоместок на штета, на паричен износ или на заменливи предмети, но висината на износот, односно количеството на предметите не може да се утврди или би можела да се утврди само со несразмерни тешкотии, судот за ова ќе одлучи по слободна оцена.

VI.

## 6.3.3. Надоместок на штета според ЗЗЛП

Интересно, ЗЗЛП има одредби за надоместок на штета што се lex specialis. Согласно принципот lex specialis derogit legi general[26], на прв поглед се чини дека овие одредби ги заменуваат генералните одредби и принципи за надоместок на штета. Сепак, одредбата што е наведена во ЗЗЛП се однесува на прекршување на одредбите на овој закон.[27]

26 VIII ПРАВНИ СРЕДСТВА И ОДГОВОРНОСТ
Право на поднесување барање до Агенцијата
Член 97
(1) Секој субјект на лични податоци има право да поднесе барање до Агенцијата, доколку смета дека обработката на неговите лични податоци ги прекршува одредбите од овој закон, притоа не доведувајќи ги во прашање кои било други управни или судски средства за правна заштита.
(2) Агенцијата го информира подносителот на барањето за текот и исходот од постапката, вклучувајќи ја можноста за судска заштита во согласност со член 98 од овој закон.
(3) Формата и содржината на образецот на барањето од став 1 на овој член го пропишува директорот на Агенцијата.
(4) Агенцијата ќе одлучи дали во текот на постапката на спротивната страна ќе ѝ ги открие личните податоци на подносителот на барањето, како и на сведокот.
(5) За поднесеното барање од став 1 на овој член, Агенцијата спроведува супервизија согласно со овој закон. Право на ефективна судска заштита против одлуките на Агенцијата
Член 98
(1) Секое физичко или правно лице има право на ефективна судска заштита против правно обврзувачката одлука на Агенцијата која се однесува на него, притоа не доведувајќи ги во прашање кои било други управни или вонсудски средства за правна заштита.
(2) Не доведувајќи ги во прашање кои било други управни или вонсудски средства за правна заштита, секој субјект на лични податоци има право на ефективна судска заштита, кога Агенцијата согласно со надлежностите утврдени во член 65 и 66 од овој закон не постапила по барањето или не го информирала субјектот на лични податоци во рок од три месеци за исходот на постапката по поднесеното барање според член 97 од овој закон.

Право на ефективна судска заштита против контролор или обработувач
Член 99
(1) Не доведувајќи ги во прашање кои било достапни управни или вонсудски средства за правна заштита, вклучувајќи го и правото на поднесување на барање до Агенцијата во согласност со член 97 од овој закон, секој субјект на лични податоци има право на ефективна судска заштита кога смета дека се повредени неговите права утврдени со овој закон, како резултат на обработката на неговите лични податоци спротивно од овој закон.
(2) Субјектот на лични податоци правото од став 1 на овој член, го остварува со поднесување тужба до надлежниот суд согласно со закон.

Застапување на субјектите на лични податоци
Член 100
(1) Субјектот на лични податоци има право да овласти здружение, да поднесе барање во негово име во однос на заштитата на неговите лични податоци и да ги остварува правата од член 97, 98 и 99
од овој закон, како и кога тоа е предвидено во закон да го остварува и правото на надоместок од член 101 од овој закон.
(2) Во статутот на здружението од став 1 на овој член основано согласно со закон, задолжително треба да бидат наведени целите што се од јавен интерес, неговиот непрофитен карактер, како и тоа треба активно да дејствува во областа на заштитата на личните податоци и во заштитата на правата и слободите на субјектите на лични податоци.
Право на надоместок на штета и одговорност
Член 101
(1) Секое лице кое претрпело материјална или нематеријална штета како резултат на прекршување од овој закон, има право да добие надоместок од контролорот или обработувачот за претрпената штета.
(2) Секој контролор кој е вклучен во обработката на лични податоци е одговорен за штетата предизвикана од таа обработка што ги прекршува одредбите од овој закон. Обработувачот е одговорен за штетата што е предизвикана од обработката, само доколку не ги почитувал обврските од овој закон што се посебно наменети за обработувачите или кога дејствувал надвор од законските упатства на контролорот или во спротивност со нив.
(3) Контролорот или обработувачот се иззема од одговорност врз основа на став 2 на овој член, ако докаже дека на ниту еден начин не е одговорен за настанот што ја предизвикал штетата. (4) Кога во истата обработка се вклучени повеќе од еден контролор или обработувач или во иста обработка учествуваат и контролор и обработувач и кога, согласно со став 2 и 3 на овој член, тие се одговорни за каква било штета предизвикана со обработката, тогаш секој контролор или обработувач се смета за одговорен за целата штета, со цел да се обезбеди ефективен надоместок на штетата за субјектот на лични податоци (солидарна одговорност). (5) Кога контролорот или обработувачот согласност став 4 на овој член исплатил целосен надоместок за предизвиканата штета, контролорот или обработувачот имаат право да побараат од другите контролори или обработувачи кои се вклучени во истата обработка на лични податоци, надоместок што одговара на нивниот дел од одговорноста за предизвиканата штета, во согласност со условите утврдени во став 2 на овој член. (6) Постапката за остварување на правото на надоместок на штета на овој член се води пред надлежен суд согласно со закон.

27 ЗЗЛП, член 101.

### 6.3.4. Кривични судови (кривична област)

Слично како граѓанските судови, кривичните судови исто така вршат правораздавање и пресудување во предмети што ја допираат материјата што е обработена во овој водич. И кај нив исто така владее принципот nemo iudex sine actore, како и принципот actori incubit probatio. Со тоа што во кривичните постапки императивен принцип што е над сите е пресумпцијата на невиност.

Кривичните судови не се само актери кога пресудуваат предмети што имаат како заштитено општествено добро – лични податоци и човекови права туку истовремено тие се и гаранти на тие права, во поглед на сите учесници, а особено на лицата кои се осомничени или обвинети за кривични дела. Пред сè, тука станува збор за улогата на кривичните судови во сферата на посебните истражни мерки, нивното дозволување, времетраење, презентирање, чување и уништување.

Кога зборуваме, пак, за судовите кога се повикани да пресудуваат во индивидуални казнени дела, компарирано со ЗЗЛП, во практиката постои определено преклопување на елементите што се однесуваат на тоа што претставува казниво дејство според одредбите на Законот за заштита на лични податоци и Кривичниот законик.

Ако се анализираат прекршочните одредби во ЗЗЛП, секоја повреда се однесува на определена одредба од законот и постапувањето спротивно на таа одредба повлекува прекршочна одговорност.

Кривичното дело што е најблиску до темата што ја обработува овој водич е Злоупотреба на лични податоци, по член 149 од КЗ[28]. Битието на ова дело претпочита во основниот облик да постои:

- Противправно поведение што е пер се спротивно на законот! (Иако првата асоцијација е дека за ЗЗЛП, сепак, може да има одредби за третман на лични податоци и во други закони, така што не е само ЗЗЛП.)
- Actus reus е прибирање, обработување или користење на лични податоци.
- Таквото дејство се прави без согласност на лицето чии податоци се злоупотребени.

28 Злоупотреба на лични податоци
Член 149
(1) 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.
(2) 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.
(3) Ако делото од став 1 и 2 го стори службено лице во вршење на службата, ќе се казни со затвор од три месеци до три години.
(4) Обидот е казнив.
(5) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

VI.

Дејствата на извршување на прекршоците се подетално опишани во прекршочните одредби на ЗЗЛП. Кривичното дело, пак, онака како што е пропишано има релативно широк опсег. На прашањето што претставува разлика помеѓу прекршочно и кривично дело, кога дејството на извршување е релативно исто, одговорот може да лежи во тоа што кај кривичното дело, барем во основниот облик, нема збирка на податоци, а додека кај прекршоците, тие се однесуваат кога е во прашање збирка на податоци. Сепак, генерално и универзално правило не може да постои и секој случај треба да биде оценуван поединечно, со сите факти и околности што го опкружуваат.

Кривичните судови, односно постапки, не се повикани да постапуваат само кај ова кривично дело туку и кај друг дела што имаат како цел незаконско користење на личните податоци. Така, мноштво на кривични дела ги имаат како допирна точка повеќе или помалку личните податоци, а ова се некои од нив:

- Неовластено објавување на лични записи – член 148;
- Неовластено откривање тајна – член 150;
- Неовластено прислушкување и тонско снимање – член 151;
- Неовластено снимање – член 152;
- Производство и дистрибуција на детска порнографија – член 193-а;
- Оштетување и неовластено навлегување во компјутерски систем – член 251;
- Правење и внесување на компјутерски вируси – член 251-а;
- Компјутерска измама – член 251-б;
- Компјутерски фалсификат – член 379-а;
- Тероризам – член 394-б;
- Ширење на расистички и ксенофобичен материјал по пат на компјутерски систем – член 394-г;
- Изнуда – член 258;
- Уцена – член 259.

Сепак, кривичните судови не се само повикани да пресудуваат туку имаат и обврска за чување на податоците што се добиени со ПИМ-мерки, определени докази, особено електронски/дигитални докази, ДНК-материјал, биолошки материјал итн.

## 6.4. Јавно обвинителство

Јавното обвинителство е дел на правосудниот апарат на една држава, и тоа како една од неопходните алки. Организирани според принципот на хиерархија, но и законитост и легалитет, ограничен опортунитет, ЈО ја има задачата да врши казнено гонење на сторители на кривични дела поврзани со заштитата на податоци и човековите права во киберпросторот. Во поново време, јавното обвинителство се соочува со сериозен наплив на дела од новата генерација, поттикнати и водени од новите технологии, на пример, говор на омраза на социјални мрежи и слично. Во секој индивидуален случај се испитува што претставува побениген говор, односно изразување, наспроти поостар, кој ги содржи елементите на кривичното дело. Всушност, супсумпцијата на правната норма единствено може да се изврши по

целосно расчистување на фактите и околностите, односно по целосна и темелна истрага.

Во пораката се среќаваат со случаи каде што се потребни докази и/или информации од т.н. VASP (Virtual Assets Service Provider), односно Сервис-провајдер на виртуелни средства (биткоин, ФТХ, лајткоин итн.). Во Република Северна Македонија засега има само еден.

Типичен случај од практиката претставуваат измамите на лица кои се заинтересирани за тргување, односно купување на виртуелни средства (криптовалути) и кога ги даваат своите лични податоци на овие провајдери, некои од нив легално регистрирани во некои јурисдикции, но некои и не. Интересно, иако тие физички можат да се наоѓаат на една територија, всушност, тие се податоци, односно записи што најчесто се наоѓаат во странство, на некој сервер, во некоја друга јурисдикција, на пример во виртуелни банки итн.

Повторно, сите злоупотреби на личните податоци, односно приватноста се мери и се оценува од случај до случај, врз основа на сите факти и собрани докази.

За да има основи за сомневање, а подоцна и основано сомнение дека е сторено кривично дело, типично од член 149 од КЗ, потребно е да постои минимум ниво на загрозување, не само податоците да се земат или да се стекнат туку и да се употребат спротивно на законот.

Меѓутоа, ова кривично дело не е секогаш тоа што ги содржи сите елементи, бидејќи целта на оној што ги злоупотребува е нивно искористување за сопствена противправна придобивка или за друг. Така, не се ретки случаите кога се земаат лични податоци со цел да бидат искористени за земање на брзи кредити, за остварување на други права како резултат на овие податоци (социјални, пензиски), да се прават осигурителни измами и слично. Сите овие ситуации имаат слични факти, но крајниот производ од аспект на супсумирана правна норма не мора да биде само делото од член 149 туку и како резултат на таа злоупотреба на податоците, може да стане збор за едно или повеќе казнени дела. Било во реален или идеален стек.

### *6.4.1. Обезбедување на патот на доказите или Chain of Custody*

Во ваквите случаи, исклучително важно е да се осигури интактноста на доказите, односно на податоците до кои се доаѓа во текот на истрагата. Доколку доказите немаат јасно движење низ синџирот на лица и органи низ кои поминуваат, не е осигурена нивната безбедност, не само физичка туку и од аспект да не бидат подложни на алтерација или модификување, тогаш тие ја губат доказната вредност.

Од практичен аспект треба да се напомене дека овие вакви случаи според дефиницијата бараат инволвирање на технички лица-експерти/вештаци со цел да се екстрахираат податоците потребни во една постапка. Тука јасно треба да се напомене дека улогата на техничките лица е да ја објасни содржината на податоците, во смисла на тоа каде се најдени, кој ги поседува, односно кој е одговорен за

нив (метадата, кој ги создал, кој ги прибрал, на кој медиум, кога и колку пати и како се модифицирани), но не и да сведочи, односно да дава мислење за податоците. Крајната цел е да се создаде, односно да се докаже поврзаност помеѓу податоците и осомниченио т. Секако, за да се задоволат интересите на фер постапка и одбраната ќе има право вкрстено да го распраша ова лице.

## 6.5. Адвокатура

Адвокатурата како дел на правосудството има мошне специфична улога во оваа сфера. Од една страна, има законска и етичка обврска согласно актите и кодексот на комората да чува и да обработува лични податоци за сопствените клиенти, а од друга страна, има и соодветна обврска за нивна заштита, дури и кога овие податоци имаат значење во определена постапка. Пред сè, тука се мисли на обврската за чување на адвокатска тајна, онаа што му е доверена или е дознаена во текот на работата, како и правото да не се сведочи за она што го дознал адвокатот во текот на својата работа и односот со својата странка.

Од друга страна, адвокатурата е јавна професија и поради тоа таа собира податоци за кои, пак, исто така е одговорна, како и сите други ентитети. Особено денес, во дигиталното време, кога податоците сè повеќе се во дигитална форма. Како што расте комуникацијата на адвокатурата со своите странки и со органите, така се зголемуваат и обврските. Тоа значи дека адвокатите немаат имунитет кога се во прашање личните податоци и аспектот на човековите права во киберпросторот, туку имаат позитивна облигација за чување и укажување на можноста од злоупотреби.

Една од најголемите обврски на адвокатурата е правилно и колку што е можно поцелосно да ги запознаваат новите технологии и нивните нормативни аспекти, со цел да можат да ги препознаваат опасностите што ги носат тие од аспект на злоупотреби, со цел да можат да овозможат навремен, точен и ефикасен правен совет. Од друга страна, преку овие постулати, да можат и правилно да ги користат процесните и материјалните овластувања кога се јавуваат во улога на процесен помошник, односно полномошник и бранител во постапките (граѓански, управни, кривични, прекршочни итн.).

Во текот на постапките, адвокатурата има можност да прибавува наоди и мислења од вешти лица и технички советници еднакво како и обвинителот во кривичната постапка и под еднакви услови со спротивната страна. За постулатите што важат во овие услови зборувавме погоре во делот за јавен обвинител.

## 6.6. Полиција

Кога зборуваме за полицијата, секако, првата асоцијација е дека нејзината улога од аспект на предметот на овој водич е во откривање на казнени дела и прекршоци. Согласно поставеноста на казнено-правниот систем во РСМ, постојат два

типа истраги, односно предистраги, што ги преземаат полициските службеници. Тоа се реактивна и проактивна истрага. Постулатите и примерите што важат за постапувањето на јавното обвинителство, важат и за полицијата, односно за правосудната полиција.

Кај личните податоци, полицијата мора да се адаптира соодветно со развитокот на општеството и со појавата на новите форми на криминалитет.

Кривичните дела што се извршуваат низ компјутерски системи и/или интернет, а имаат како цел повреда на правото на приватност, како човеково право, и цел да се повредат личните податоци, можат да се опишат на четири начини:

1. Тоа се незаконски постапувања што претставуваат повреда на важни индивидуални и општествени добра за кои законот предвидува кривична санкција.
2. Направени се на конкретен начин, со употреба на конкретни средства и цел на кривичното дело – а тоа е со употреба на компјутерски системи и мрежи.
3. Овие дела се под посебен предмет на заштита – на пример, безбедност на компјутерските системи и мрежи, стриминг на складирани компјутерски податоци во целина или одреден дел.
4. Целта на сторителот на овие дела е да се добие незаконска корист (материјална или нематеријална) или предизвикување штета на други.[29]

Сепак, полицијата не може да се гледа како на изолиран ентитет во борбата со криминал, бидејќи прекршувањата на законот не се секогаш кривични дела и обратно. Она што е покриено со регулативата што ги пропишува личните податоци и нивната заштита не е секогаш во надлежност на полицијата. Така, на пример, кога се работи за злоупотреба на личните податоци, тука надлежност воспоставува полицијата, бидејќи најверојатно постои основа на сомнение за сторено казнено дело. Наспроти тоа, ако се работи за незаконито водење на збирката на лични податоци, иако истиот сет факти може prima facie да даде сомнение за кривично дело и за регулаторен прекршок согласно ЗЗЛП, веројатно ќе преовлада второто, бидејќи сепак постои збирка на лични податоци, што од која било причина може да има определени неправилности во нејзиното водење, без притоа да има кривично дело.

29 I. Marcella, Albert J. II. Greenfield, Robert, Cyber Forensics, CRC Press, 2005, стр. 48.

# VI.

***Ако земеме дека***

**кривично дело = дејство (пропуштање)** + **противправност** + **да биде пропишано како казниво** +

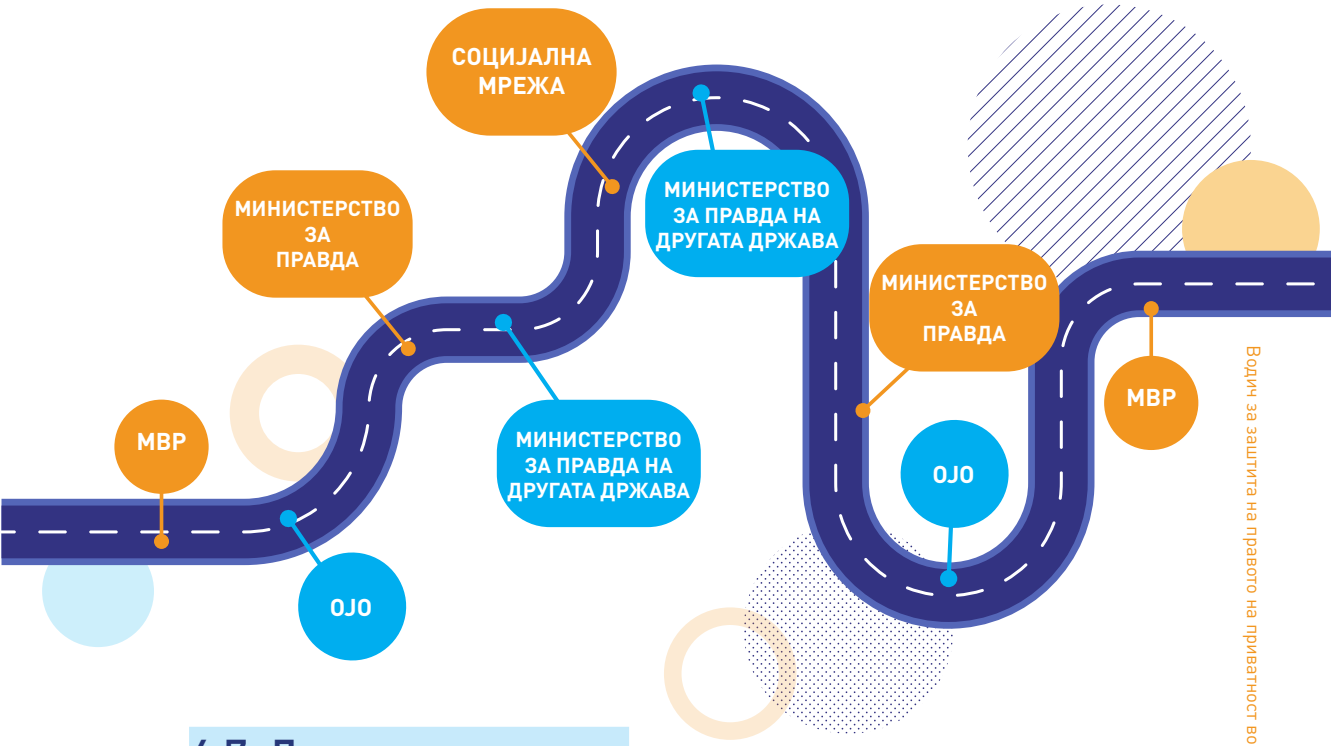
**волев однос кон делото (умисла/ небрежност )**

Тогаш отсуството на кој било од овие елементи значи дека нема кривично дело. Но, тоа не исклучува постоење на некој друг деликт.

Така, на пример, за бришење на лажните профили на социјални мрежи надлежност постои кај АЗЛП, додека за последицата што настанала како резултат на тој креиран лажен профил (штета, измама, изнуда итн.) надлежност би имала полицијата, бидејќи тоа претставува казнено дело пропишано со КЗ.

Посебен тип постапки се барањата за меѓународна правна помош, кои се чести, имајќи ги предвид околностите дека личните податоци на интернет-просторот не се наоѓаат на територијата на една држава, туку напротив, тие можат да бидат не само во една странска држава туку и во неколку од нив. Конечно, неретко, и не можат да се идентификуваат субјектите кои оперираат со ваквите системи, што значи дека мора да се побара меѓународна правна помош. Иако живееме во општество каде што претежно се комуницира по електронски пат, сепак овие процедури се строго писмени, инволвираат мноштво институции и многу се чека на повратни информации.

***Патот на таа меѓународна правна помош изгледа вака:***




## 6.7. Државни органи

Државните органи исто така имаат важна улога. Тие се јавуваат првенствено како контролори на лични податоци и имаат збирки на лични податоци што можат да бидат и од највисок степен на заштита. Во административните постапки може да се бара заштита, особено за правата на субјектите на податоците (на пример, правото на пристап, исправка, бришење и приговор) или утврдување незаконитост на обработката на податоците (бидејќи тоа не е во согласност со принципите за заштита на податоците и/или други одредби во врска со законитоста на обработка на податоци).

## 6.8. Граѓански организации

Граѓанските организации имаат извонредна улога во градењето на демократски институции и развивање на свеста за важноста на заштитата на човековите права, вклучително и оние на интернет-просторот. Преку обуки, кампањи, стратешки застапувања и учество во креирање на јасни политики, граѓанските организации неретко се клучната алатка во подигнувањето на свеста во општеството и градењето механизми за заштита.

VI.

## 6.9. Компании

Во текот на своето секојдневно работење, компаниите собираат и обработуваат лични податоци и со тоа тие ја имаат улогата на контролори. Нивната обврска е двострана, и кон регулаторот, односно легислативата, да бидат на линија на законските барања за заштита, и кон лицата чии податоци ги чуваат и ги обработуваат, односно нивните вработени, но и кон трети лица кои не се во работен однос, но до чии податоци доаѓаат.

Овде особено мораат да се споменат големите меѓународни конгломерати, односно мултинационалните компании што собираат податоци во рамките на нивните надлежности, односно услугите и производите што ги нудат. Тука спаѓаат неизбежните социјални мрежи („Фејсбук", „Инстаграм", „X", „Линкдин" итн.) и провајдерите на интернет-сервиси („Гугл", „Јаху" итн.).

## 6.10. Индивидуи

Едно од основните правила за заштита на податоците е, всушност, дека тоа е примарна обврска на индивидуата. Секој има право на приватност, но и обврска дилигентно да се грижи за сигурноста на сопствените податоци. Во поново време, со развитокот на технологијата, токму физичките лица се тие што со сопствено дејство, односно пропуштање на должен надзор, ги откриваат сопствените податоци и со тоа се изложуваат на опасности. Така, на пример, еклатантни примери се споделувањето пин-код за платежни картички, оставањето податоци за сметки на интернет-страници без да се провери нивната сигурност, давањето на медицински податоци насекаде, отворањето на сомнителни електронски пораки што имаат цел да инсталираат малициозни софтвери итн. Затоа, индивидуалните лица не се само жртви туку се и активен актер на полето на заштита на податоците, бидејќи самозаштитата е некогаш најдобра заштита.

# 07
# ЛИЧНИ ПОДАТОЦИ, ЧОВЕКОВИ ПРАВА И ПРАШАЊЕ НА АРБИТРАБИЛНОСТ

VII.

# ЛИЧНИ ПОДАТОЦИ, ЧОВЕКОВИ ПРАВА И ПРАШАЊЕ НА АРБИТРАБИЛНОСТ

Примената на Општата регулатива за заштита на податоците (GDPR) од 25 мај 2018 година предизвика бран реакции надалеку, што не ја одмина ниту арбитражната заедница.

Накратко, прашањето гласи дали личните податоци се поле на правото што е арбитрабилно, односно може да потпадне под еден од режимите за алтернативно решавање на споровите (арбитража), и тоа не само домашните туку и меѓународните. Примената на Законот за заштита на лични податоци во текот на арбитражната постапка навистина може да биде мошне сложена (и потенцијално оптоварена) и може да наметне дополнителни обврски на страните (на арбитражните институции) вклучени во постапката што мораат да бидат земени многу сериозно со оглед на ризиците од одговорност што произлегуваат од GDPR.

И покрај важноста на примената на GDPR на меѓународната арбитража, се чини дека преовладува мислењето дека би било жално да се смета дека новите правни режими што ги регулираат и ги штитат податоците (како што е GDPR) се само извор на загриженост за глобалната арбитражна заедница. Напротив, овие правни режими што создаваат нови законски обврски веројатно ќе генерираат нови правни предизвици и правни спорови што повторно би можеле да се поднесат на арбитража и на други алтернативни механизми за решавање спорови во одредени околности. Последователно, не е изненадувачки што се појавија даватели на арбитража и други услуги за алтернативно решавање спорови (ADR) со цел да понудат алатки за решавање спорови онлајн поврзани со GDPR (конкретно за спорови за прекршување податоци). Во секој случај, јасно е дека во нашата економија, управувана од податоци во која податоците се и ќе бидат клучен двигател на иновациите и моќта, обемот и стратешкото значење на „споровите за податоците", генерално дефинирани како спорови поврзани со условите за заштита, пристапот до податоците и/или користењето на податоците во одредени околности, ќе (продолжи) значително да се зголемува во иднина.[30]

30 Using arbitration and adr for disputes about personal and non-personal data: what lessons from recent developments in Europe? – ARIA – Vol. 30, No. 2, Jacques de Werra, March, 2020.

# 7.1. Одговорност за заштита на приватноста и личните податоци во рамките на внатрешниот правен поредок и во рамките на меѓународниот правен поредок

Во домашниот поредок, одговорноста е на контролорот или обработувачот или на друго правно или физичко лице кое сториле каков било деликт кон приватноста. Со други зборови, ако определено физичко лице стори деликт во доменот на казненото право кон друго правно или физичко лице, тоа одговара sui generis, во рамките на домашниот правен поредок. Се разбира дека сторител на каков било деликт (со активно или пасивно дејство) може да биде и државата. Таа во домашниот правен поредок е изедначена според нејзината странкарска способност со другите актери.

Во меѓународниот правен поредок, правен субјективитет секогаш има државата.

**Зошто воопшто ја отвораме оваа тема во овој водич?**

Вообичаено, домашните органи, кога одлучуваат во рамките на нивните надлежности, се задржуваат на нормите на домашниот правен поредок кога ги вршат своите уставни и законски надлежности, без притоа да ги земаат предвид меѓународните стандарди кон кои пристапила државата и тие станале дел на домашниот поредок.

Во дваесеттиот век, а сега особено во дваесет и првиот век, најголем предизвик на секој правен поредок е да разбере дека, иако државите се суверени и самостојни, сепак правниот поредок што прифатил меѓународни норми не е ексклузивно нивен, туку е дел на поголем и поширок меѓународен правен поредок. Секако, во сегашниот степен на развиток на правото тоа претставува цивилизациска придобивка и атрибут на секое демократско општество.

Домашните авторитети кои одлучуваат во рамките на правниот поредок на Република Северна Македонија имаат обврска, а не опција, за имплементирање на меѓународните стандарди, односно прописи. Таквата обврска произлегува не само од Уставот туку и од мноштво други прописи, на пример Законот за судовите, Законот за граѓанска одговорност за навреда и клевета итн.

Ваквиот постулат најсликовито ќе се објасни преку следното: Државите можат да бидат одговорни и за своите постапки и пропусти, за неисполнување на меѓународно преземените обврски итн. Сепак, работите се малку посложени кога станува збор за разбирање на изворите на оваа доктрина, кога станува збор за секојдневното работење на кои било управни и судски тела во Република Северна Македонија, иако одредени закони јасно се насочени кон странските пресуди, како може да се примени директно, заедно со ставовите и образложението изразени во нив.

# VII.

Меѓународните документи и конвенции ги пропишуваат минималните стандарди за третман и процедури кога се во прашање нормите што ги пропишуваат тие. Постојат различни меѓународни инструменти што имаат донесено правила што треба да се испитаат, да се протолкуваат и да се аплицираат во рамките на домашното право.

Меѓународните стандарди се применливи поради различни причини:

- Прво, секој закон или корпус закони не можат да се гледаат и да се интерпретираат изолирано во рамките на домашниот правен поредок, а камоли во меѓународниот правен поредок.
- Второ, секоја земја што ќе избере да ратификува или да усвои одреден меѓународен правен инструмент се обврзува дека ќе се придржува до принципите на овој меѓународен инструмент и соодветно ќе ги приспособи своето законодавство и/или своите практики.
- Трето, тоа го бараат основните правила на меѓународното право во врска со одговорноста на државите за нивните штетни (wrongfull) акти. Акцентот е на секундарните правила за одговорност на државата, т.е. општите услови според меѓународното право државата да се смета за одговорна за погрешни постапки или пропусти и правните последици што произлегуваат од тоа. „Нацрт-членовите за одговорностите на државите за меѓународно штетни акти со коментари" (нацрт-членови)[31] практично го кодифицираат меѓународното обичајно право и затоа се обврзувачки за сите држави.

Според член 1, „секој меѓународно штетен акт на една држава повлекува меѓународна одговорност на таа држава". Меѓу другото, нејзиниот коментар го наведува член 1 како основниот принцип што лежи во основата на членовите како целина, а тоа е дека прекршувањето на меѓународното право од страна на една држава повлекува нејзина меѓународна одговорност.

Меѓународен штетен акт на една држава може да се состои од едно или повеќе дејства или пропусти или комбинација од двете. Дали имало меѓународно штетен акт зависи, прво, од барањата на обврската за која се вели дека е прекршена и, второ, од рамковните услови за такво дело, кои се наведени во првиот дел. Терминот „меѓународна одговорност" ги опфаќа новите правни односи што произлегуваат според меѓународното право поради меѓународно погрешниот чин на една држава. Содржината на овие нови правни односи е наведена во вториот дел.

Според член 2, постои меѓународно штетен акт на една држава кога однесувањето што се состои од дејство или пропуст:

(а) според меѓународното право ѝ се припишува на државата; и
(б) претставува прекршување на меѓународна обврска на државата.[32]

31 „Нацрт-членовите за одговорностите на државите за меѓународно штетни акти со коментари", 2001 година, Меѓународна правна комисија на ОН.

32 Нацрт-членовите за одговорностите на државите за меѓународно штетни акти со коментари", 2001 година, Меѓународна правна комисија на ОН.

Еден од најважните членови што ја разликува карактеризацијата на таквиот чин и неговата меѓусебна поврзаност со домашното право е член 3. Членот наведува дека „карактеризирањето на чинот на една држава како меѓународно штетно е регулирано со меѓународното право. Таквото карактеризирање не е засегнато со карактеризирање на истото дело како законито според внатрешното право".[33]

Во случајот ЕЛСИ, пред МСП, советот на Судот го нагласи ова правило, наведувајќи дека:

***Усогласеност со домашниот закон и усогласеност со одредбите на договор се различни прашања. Она што е прекршување на договорот може да биде легално во домашното законодавство и она што е незаконско во домашното законодавство може да биде целосно невино во однос на прекршување одредба од договор.***

***Мошне често, домашните власти (со право) сметаа дека нивните постапки и/или пропусти или примена/толкување на законот во одредена ситуација треба да се гледаат од перспектива на домашниот правен поредок. И кога ќе го преживеат тестот на правните лекови, тоа ги прави законски, односно не погрешни.***

***Меѓутоа, поради отсуство на какво било сомневање, овој напис има цел да ги избрише сите толкувања за односот помеѓу тоа како се гледа на еден акт од перспектива на домашното и меѓународното право и кое гледиште е релевантно, од перспектива на меѓународното право.***

Член 4 се однесува на однесувањето на органите на една држава и според овој член,

1. Однесувањето на кој било државен орган се смета за акт на таа држава според меѓународното право, без разлика дали органот врши законодавна, извршна, судска или која било друга функција, без оглед на позицијата што ја има во организацијата на државата и без оглед на нејзиниот карактер како орган на централната влада или на територијална единица на државата.

2. Орган вклучува секое лице или ентитет што го има тој статус согласно внатрешните закони на таа држава.[34]

33 Што се однесува до првиот од овие елементи, можеби најјасната судска одлука е онаа на PCIJ во третманот на полските државјани (Treatment of Polish Nationals and Other Persons of Polish Origin or Speech in the Danzig Territory, Advisory Opinion, 1932, P.C.I.J., Series A/B, No. 44, p. 4.) Судот ѝ го ускрати правото на полската влада да поднесува прашања до органите на Лигата на народите во врска со примената на одредени одредби од Уставот на Слободниот град Данциг со образложение дека: Според општоприфатените принципи, државата не може да се потпре, во аргументот против друга држава, на одредбите на Уставот на таа друга држава, но само за меѓународното право и меѓународните обврски што се уредно прифатени (...) [С] обратно, една држава не може да се изјасни против друга држава, која во својот Устав има одредби со цел избегнување на обврските што му се наметнати од меѓународното право или договорите во сила (...) Примената на Уставот за Данциг може (...) да резултира со повреда на меѓународна обврска (...) без разлика дали е според договорите или според општото меѓународно право (...) Но, во случаи од ваква природа, не е Уставот и другите прописи како такви, туку меѓународните обврски што повикуваат на одговорност на Слободниот град.

34 „Нацрт-членовите за одговорностите на државите за меѓународно штетни акти со коментари", 2001 година, Меѓународна правна комисија на ОН. Цитирано и во Judicial supervision in cases of deprivation of liberty of asylum seekers and the responsibility on the state to adhere to international legal standards. Aleksandar Godzo, Ana Dangova Hug, Dime Gjorchevski, 2021.

Што значи дека принципот на атрибуција се однесува за сите органи, вклучително и судовите.

Сумирано, тоа значи дека доколку едно дејство, процедура и слично може да биде целосно законита од аспект на домашно право, истото дејство, процедура може да биде целосно во колизија со меѓународното.

Важно за нас и за оваа анализа е тоа што ваквиот став е граден во текот на деценииите и на случаи што се и ден-денес актуелни и претставуваат извор на правна аргументација и право.

Домашните органи, а особено судовите, сметајќи исклучиво на домашното право и практично игнорирајќи го меѓународното, не ја доведуваат во прашање индивидуалната законитост во поширока смисла на кој било предмет, туку едновремено припишуваат и одговорност на државата чии органи се, и тоа не само во домашни туку и во меѓународни рамки.

Значи, она што е законито во домашното право не значи секогаш дека е на линија со меѓународното.

Во контекст на материјата на овој водич, особено кога како актер се јавува државата на полето на заштита на приватноста и личните податоци, императивно е да се применуваат и меѓународните стандарди, независно од регулативата во домашниот правен поредок, кој поинаку може да регулира едно прашање или некоја материја.

## 7.2. Заштита на податоци и слобода на изразување

Заштитата на податоците и слободата на изразување се две основни права меѓу кои треба да постои рамнотежа. Затоа, од големо значење е законското регулирање на критериумите што го балансираат правото на заштита на личните податоци со слободата на изразување и информирање. ЕКЧП разви голем број критериуми, кои треба да се земат предвид, кои исто така беа рефлектирани во некои национални закони. Според ЗЗЛП овој процес посветува особено внимание на:

- природата на личните податоци,
- околностите во кои се добиваат податоци,
- влијанието на објавените информации врз дискусијата за јавниот интерес,
- колку е познато засегнатото физичко лице и предметот на информацијата,
- претходно однесување на засегнатото физичко лице,
- претходна согласност од засегнатото физичко лице,
- содржината, формата и последиците од објавувањето на оваа информација.

Правото на изразување го опфаќа и правото на информирање.[35]

## 7.3. Заштита на правото на приватност и заштита на личните податоци преку релевантни сентенции од ЕСЧП и ЕСП

Судската практика на ЕСЧП релативно добро ги следи технолошките достигнувања на човештвото, барем што се однесува до Советот на Европа, чиј орган е.

За подобра прегледност, судската практика е сублимирана во поднаслови, односно клучни зборови.[36]

### *7.3.1. Поим на лични податоци и нивниот опсег*

Во своите пресуди Судот го објаснува концептот на „лични податоци" со повикување на Конвенцијата на Советот на Европа бр. 108 за заштита на поединци во однос на автоматска обработка на лични податоци од 28 јануари 1981 година, кој стапи на сила во 1985 година и беше ажуриран во 2018 година („Конвенција 108"), чија цел е „да се обезбеди на територијата на секоја страна за секој поединец (...) почитување на неговите права и основни слободи, а особено неговото право на приватност, во однос на автоматската обработка на личните податоци што се однесуваат на него" (член 1) [Amann v. Switzerland (GC), 2000, § 65 Хараламби против Романија, 2009 година, § 77]. Судот јасно укажа дека, според член 2 од Конвенцијата 108, концептот на лични податоци е дефиниран како „секоја информација што се однесува на идентификувано или препознатливо лице" [Amann v. Switzerland (GC), 2000, § 65; Haralambie v. Романија, 2009 година, § 77].

### *7.3.2. Што опфаќаат*

Таквите податоци опфаќаат не само информации што директно го идентификуваат поединецот („субјектот на податоците"), како што се името и презимето [Guillot v. France, 1996, §§ 21-22; Mentzen v. Latvia (dec.), 2004; Güzel Erdagöz против Турција, 2008, § 43; Garnaga v. елемент што индиректно идентификува лице, како што е динамична ИП-адреса (интернет-протокол); Benedik v. Словенија, 2018, §§ 107-108].

35 ЗЗЛП, член 81 став 4.

36 Водич за судска практика на конвенцијата – Заштита на податоци, Европски суд за човекови права, 12/98. Последно ажурирање: 31.08.2022 година.

### 7.3.3. Правни лица и лични податоци

Иако се чини дека прашањето за заштита на личните податоци главно се однесува на поединци, во однос на нивното право од член 8 на почитување на нивниот приватен живот, правните лица исто така имаат право да се потпрат на ова право пред Судот доколку тие се директно засегнати со некоја мерка што го нарушува нивното право на почитување на нивната „преписка“ или „дом“. Ова беше случај, на пример, кога на компанијата ѝ беше наредено да обезбеди копија од сите податоци на сервер споделен со други компании (Bernh Larsen Holding AS and Others v. Norway, 2013, § 106) или каде што Министерството за одбрана, според налог, ги пресретнал комуникациите на невладините организации за граѓански слободи (Liberty and Others v. the United Kingdom, 2008, §§ 56-57). Меѓутоа, во случај што се однесува на мерки што вклучуваат заштита на личните податоци на членовите на религиозна организација и почитување на нивниот „приватен живот“, организацијата не била директно засегната и затоа не била „жртва“ во смисла на член 34 од Конвенцијата (Авилкина и други против Русија, 2013, § 59).

### 7.3.4. Форми на лични податоци

Личните податоци можат да имаат многу различни форми. На пример:

- Информации за интернет-претплатници поврзани со специфични динамични ИП-адреси доделени во одредени периоди (Benedik v. Словенија, 2018, §§ 108-109).
- Снимките земени за употреба како гласовни примероци, кои се од трајна природа и се предмет на процес на анализа директно релевантна за идентификување лице во контекст на други лични податоци (P. G. и J. H. против Обединетото Кралство, 2001, § 59).
- Клеточни примероци и ДНК-профили [S. and Marper v. the United Kingdom (GC), 2008, §§ 70-77] или отпечатоци од прсти (ibid., § 84), кои, и покрај нивниот објективен и непобитен карактер, содржеле уникатни информации на засегнатото лице и дозволи негово/нејзино прецизно идентификување во широк опсег на околности (ibid., § 85).
- Информации за одредено лице добиени од банкарски документи, без разлика дали се однесуваат на чувствителни детали или професионална активност (M. N. и други против Сан Марино, 2015, §§ 51 и понатаму).
- Податоците за професијата на идентификувано или препознатливо лице собрани и складирани од полицијата (Khelili v. Switzerland, 2011, § 56).
- Податоци за користење интернет и пораки („Jaxy“) од страна на вработен на работното место, добиени преку надзор [Bărbulescu v. Romania (GC), 2017, §§ 18, 74-81].
- Копија од електронски податоци запленети во адвокатска канцеларија, иако не биле дешифрирани, транскрибирани или официјално припишани на нивните сопственици (Kırdök and Others v. Turkey, 2019, § 36).
- Податоци собрани во контекст на неприкриен видеонадзор на универзитет (Антовиќ и Мирковиќ против Црна Гора, 2017, §§ 44-45).

- Информации за оданочливиот приход и имотот на голем број физички лица, без оглед на фактот што јавноста може да пристапи до таквите податоци под одредени услови [Satakunnan Markkinapörssi Oy и Satamedia Oy против Финска (GC), 2017, § 138].
- Податоци за раѓање и напуштање поединец, вклучувајќи информации потребни за откривање на вистината за важен аспект на личниот идентитет [Гаскин против Обединетото Кралство, 1989, § 39; Микулиќ против Хрватска, 2002, §§ 54-64 Odièvre против Франција (GC), 2003, §§ 28-29].
- Податоци вклучени во спогодбата за развод, кои опфаќаат детали за поделбата на брачниот имот, старателството и престојот на малолетните деца, договорот за алиментација и преглед на имотот/приходот на апликантот (Liebscher против Австрија, 2021, §§§ 31 и 68).

### *7.3.4. Специјални категории на податоци*

#### *7.3.4.1. Таканаречени „чувствителни" категории*

Според член 6 од Конвенцијата 108, личните податоци што откриваат расно потекло, политички мислења, религиозни или други убедувања и информации за здравјето или сексуалниот живот на поединецот или за какви било кривични пресуди, не можат автоматски да се обработуваат, освен ако домашното законодавство не предвидува соодветни заштитни мерки. Информациите што спаѓаат во овие категории, опишани од Судот како „чувствителни", налагаат зголемен степен на заштита според него.

#### *7.3.4.2. Податоци што откриваат расно или етничко потекло*

Етничкиот идентитет на поединецот мора да се смета како важен елемент на приватниот живот [C. и Марпер против Обединетото Кралство (GC), 2008, § 66; Ciubotaru против Молдавија, 2010, § 49]. Податоците се особено загрижувачки кога би можеле да го откријат етничкото или друго потекло на една личност, имајќи го предвид брзото темпо на развојот на полето на генетиката и информатичката технологија [S. and Marper v. the United Kingdom (GC), 2008, § 71]. Примероците и ДНК-профилите содржат многу чувствителни информации и им овозможуваат на властите да воспостават генски врски меѓу поединците и да го проценат нивното веројатно етничко потекло (ibid., §§ 72-77; Aycaguer v. France, 2017, § 33). Во случајот во врска со евидентирањето на етничкото потекло на поединецот во официјалните регистри, Судот, нагласувајќи ја високочувствителната природа на евидентирањето на таквите податоци, го призна постоењето на позитивна обврска од страна на државата да спроведе постапка да му се овозможи на субјектот на податоците да ја промени неговата/нејзината евидентирана етничка припадност врз основа на објективно проверливи докази (Ciubotaru против Молдавија, 2010, §§ 52-59).

### *7.3.4.3. Податоци што откриваат политички мислења и религиозни или други верувања, вклучително и филозофски*

Податоците што откриваат политички мислења се сметаат за „чувствителна" категорија на лични податоци и, според мислењето на Судот, неприфатливо е националните власти да го игнорираат овој аспект со обработка на таквите податоци во согласност со обичните домашни правила, без да се земат предвид потребата за заштита (Кат против Обединетото Кралство, 2019, § 112). Во случајот Catt против Обединетото Кралство од 2019 година, во врска со складирањето во полициска база на податоци за мирен демонстрант, националните судови само се повикаа на општиот закон за заштита на податоците при испитувањето на законитоста на мешањето. Судот утврди повреда на член 8, посочувајќи дека чувствителната природа на предметните податоци требаше да претставува клучен елемент на случајот пред домашните судови, како што беше пред Судот (ibid., § 112). Судот исто така утврди повреда на член 8 во M. D. and Others v. Spain, 2022 (§§ 63-64), во врска со извештајот составен од полицијата во однос на судиите кои ги извршувале своите функции во Каталонија и кои имале потпишан манифест во кој го изнесоа своето правно мислење во корист на можноста каталонскиот народ да го искористи таканаречената „право на одлучување", во извештајот што ги открива, особено, политичките ставови на некои од апликантите.

Правото на заштита на личните податоци што ги откриваат верските или другите верувања, вклучително и филозофските, на поединецот беше испитувано од Судот во случаите Синан Ишик против Турција, 2010 (§ 37) и Мокуте против Литванија, 2018 (§ 117). Што се однесува до наведувањето на религијата на личните карти на апликантите, Судот ја нагласи важноста на правото на заштита на податоците во врска со религиозните убедувања, што претставува еден од највиталните елементи што го сочинуваат идентитетот на верниците и нивната концепција за живот, како што е заштитено со член 9 од Конвенцијата (Sinan Işık против Турција, 2010, § 37).

### *7.3.4.4. Податоци што го откриваат членството во синдикатот*

Личните податоци што го откриваат членството во синдикатот на поединец, исто така, можат да бидат „чувствителни" и затоа бараат зголемена заштита. Во случајот Catt против Обединетото Кралство, 2019 (§ 112), полицијата собрала информации за учеството на жалителот на демонстрации организирани од голем број синдикати, особено неговото име, присуство, датум на раѓање и адреса. Во одредени случаи беше опишан и неговиот изглед, заедно со фотографии направени за време на предметните демонстрации (ibid., § 10). Вклучувањето во мирни протести има специфична заштита според член 11 од Конвенцијата, кој исто така содржи посебна заштита за синдикатите (ibid., § 123). Иако собирањето од страна на полицијата на лични податоци за апликантот може да се смета за оправдано, немаше итна потреба, според мислењето на Судот да се задржат податоците на апликантот, во отсуство на какви било правила што одредуваат дефинитивен максимален временски рок за задржување на такви податоци (ibid., §§ 117-119).

### *7.3.4.5. Генски и биометриски податоци*

Судот постапил со голем број случаи во врска со собирање или задржување на:

- клеточни примероци [Van der Velden против Холандија (одлука), 2005; Каруана против Малта (одлука), 2018; Трајковски и Чиповски против Северна Македонија, 2020; Бољевиќ против Србија, 2020];
- ДНК-профили [Ван дер Велден против Холандија (одлука), 2005; Шмит против Германија (одлука), 2006; С. и Марпер против Обединетото Кралство (GC), 2008; В. против Холандија (дек.), 2009; Перуцо и Мартенс против Германија (одлука), 2013; Канон против Франција (одлука), 2015; Ајкагуер против Франција, 2017; Мифсуд против Малта, 2019; Gaughran против Обединетото Кралство, 2020; Трајковски и Чиповски против Северна Македонија, 2020; Драган Петровиќ против Србија, 2020];
- отпечатоци од прсти [McVeigh, O'Neill и Evans против Обединетото Кралство, 1981; Kinnunen против Финска, 1993; S. and Marper против Обединетото Кралство (GC), 2008; Димитров-Казаков против Бугарија, 2011; М. К. против Франција, 2013; Супруненко против Русија (декември), 2018; Гауран против Обединетото Кралство, 2020; П. Н. против Германија, 2020; Вилемс против Холандија (дек.), 2021];
- отпечатоци од дланка (П. Н. против Германија, 2020);
- Водич за судска практика на Конвенцијата – Заштита на податоци
- Европски суд за човекови права 13/98 Последно ажурирање: 31.08.2022 година
- гласовни примероци (П. Г. и Ј. Х. против Обединетото Кралство, 2001; Алан против Обединетото Кралство, 2002; Доерга против Холандија, 2004; Ветер против Франција, 2005; Висе против Франција, 2005).

Податоци за здравје, сексуален живот или сексуална ориентација

Информациите што се однесуваат на здравјето на поединецот сочинуваат клучен елемент во приватниот живот (Ивон Шаве роденото Jullien против Франција, 1991, § 75; L. L. против Франција, 2006; Раду против Молдавија, 2014; L. Н. против Летонија, 2014, § 56; Коновалова против Русија, 2014, §§ 27, 41; Y. Y. против Русија, 2016, § 38; Суриков против Украина, 2017; Францу против Романија, 2020, § 52). Почитувањето на доверливоста на овие информации е од клучно значење, не само за почитување на чувството за приватност на пациентот туку и за зачувување на неговата или нејзината доверба во медицинската професија и во здравствените услуги воопшто. Овие размислувања се особено валидни во однос на заштитата на доверливоста на информациите за ХИВ-инфекцијата на една личност [Z v. Finland, 1997, § 96; Kiyutin v. Russia, 2011, § 64; Armonienė v. Lithuania, 2008, § 40; Biriuk против Литванија, 2008, § 39; I. против Финска, 2008, § 38; C. C. против Шпанија, 2009, § 33; Y. против Турција (одлука), 2015, § 65; P. T. против Република Молдавија, 2020, §§ 5-6, 26; Y. G. против Русија, 2022, § 45]. Откривањето на таквите податоци може да влијае драматично на неговиот/нејзиниот приватен и семеен живот, како и на социјалната и работната ситуација, со тоа што ќе го изложи на омаловажување и ризик од остракизам [Z v. Finland, 1997, § 96; C. C. v. Шпанија, 2009, § 33; П. и С. против Полска, 2012, § 128; Авилкина и други против Русија, 2013, § 45; Y. против Турција (одлука), 2015 година, § 65; Y. G. против Русија, 2022 година, § 45].

### 7.3.5. Тестови за пропорционалност

Дали мешањето било законско?

Судот го испита во голем број случаи прашањето дали е исполнето или не е исполнето барањето, како што е наведено во член 5 од Конвенцијата 108, дека личните податоци што се подложени на автоматска обработка мора да се добиени и обработени праведно и законски. Во голем број случаи, Судот утврди повреда на член 8 единствено врз основа на недостаток на правна основа на национално ниво за да одобри мерки способни да се мешаат во релевантните права (Тејлор-Сабори против Обединетото Кралство, 2002, §§ 17-19; Раду против Молдавија, 2014, § 31; Мокуте против Литванија, 2018, §§ 103-104; М. Д. и други против Шпанија, 2022, §§ 61-64).

Особено, во Mockutė против Литванија, 2018 (§§ 103-104), Судот забележа дека ниту Владата ниту националните судови не посочиле каква било одредба што би можела да ја формира правната основа за комуникацијата, од страна на психијатриската болница, информации за здравјето на жалителот, кој бил возрасен, на неговата мајка и на новинарите. Во Тејлор-Сабори против Обединетото Кралство, 2002 (§§ 17-19), каде што апликантот бил подложен на полициски надзор преку „клонирање" на неговиот пејџер, не постоел законски систем за регулирање на следењето на пораките на пејџер што се пренесуваат преку приватен телекомуникациски систем. Во M. D. and Others v. Spain, 2022 (§§ 61-64), полицијата подготви извештај во однос на судиите кои ги извршувале своите функции во Каталонија и кои потпишале манифест во кој ги навеле своите правни мислење во корист на можноста каталонскиот народ да го искористи таканаречената „право на одлучување", извештајот што ги открива личните податоци, фотографиите, професионалните информации и политичките ставови на некои од нив. Судот забележа дека составувањето на извештајот од страна на полицијата не било предвидено со закон и затоа што јавните органи ги користеле личните податоци за друга цел од онаа што го оправдува собирањето, постоењето на полицискиот извештај, кој бил изготвен во однос на поединци чие однесување не имплицирало никаква криминална активност, што претставува прекршување на член 8 од Конвенцијата.

### 7.3.6. Дали мешањето следело легитимна цел

Во голем број случаи, Судот испита дали е исполнето или не е исполнето барањето, како што е наведено во член 5 од Конвенцијата 108, дека личните податоци што се подложени на автоматска обработка мора да се собрани за експлицитни, специфицирани и легитимни цели. Во овие случаи, испитувањето на легитимните цели што можат да го оправдаат мешањето во остварувањето на правата од член 8, како што е наведено во став 2, е особено содржано. Овие цели се заштита на националната безбедност, јавната безбедност и економската благосостојба на земјата, спречување безредие или криминал, заштита на здравјето или моралот или заштита на правата и слободите на другите. Судот генерално го потврдува постоењето на една или повеќе од овие легитимни цели на кои се повикува Владата.

Судот го зазеде ставот, на пример, дека складирањето во регистарот на тајната полиција на податоци за приватниот живот на поединци, потоа употребата на тие податоци при проверката на кандидатите за функции од значење за националната безбедност, следеше легитимна цел за целите на член 8, имено заштита на националната безбедност (Леандер против Шведска, 1987, § 49). Набљудувањето на апликантот преку ГПС, наложено од обвинител за истрага за неколку дела на обид за убиство за кои терористичко движење ја презеде одговорноста и за да се спречат понатамошни бомбашки напади, според мислењето на Судот служеше на интересите на националната безбедност и јавната безбедност, спречувањето на криминалот и заштитата на правата на жртвите (Uzun v. Germany, 2010, § 77).

### *7.3.7. Дали мешањето било „неопходно во едно демократско општество"*

За да биде неопходна во едно демократско општество, секоја мерка што се меша во заштитата на личните податоци според член 8 мора да одговара на итна општествена потреба и не смее да биде непропорционална со легитимните цели што се следат (Z v. Finland, 1997, § 94; Келили против Швајцарија, 2011, § 62; Висенте дел Кампо против Шпанија, 2018, § 46). Причините на кои се повикува Владата мораат да бидат релевантни и доволни (Z против Финска, 1997, § 94). Додека националните власти треба да ја направат првичната процена во сите овие аспекти, конечната оценка за тоа дали мешањето е неопходно останува предмет на разгледување од страна на Судот за усогласеност со барањата на Конвенцијата [S. and Marper v. the United Кралство (GC), 2008, § 101].

### *7.3.8.Европски суд на правдата (ЕСП)*

#### *7.3.8.1. Пристап до информации за субјектите*

На 12 јануари 2023 година, Европскиот суд на правдата (ЕСП) донесе нова пресуда во случајот C-154/21 Österreichische Post во врска со информациите околу примателите на лични податоци. Граѓанин побарал од Поштата на Австрија, главен оператор на поштенски и логистички услуги во Австрија, да му го открие идентитетот на примателите на кои им ги открила неговите лични податоци. Тој се потпираше на Општата регулатива за заштита на податоците на ЕУ (GDPR). GDPR предвидува дека субјектот на податоците има право да добие од контролорот информации за примателите или категориите на примачи на кои им биле или ќе бидат откриени неговите/нејзините лични податоци. Како одговор на барањето на граѓанинот, Поштата на Австрија само изјави дека користи лични податоци и дека тие лични податоци им ги нуди на трговските партнери за маркетинг-цели. Сепак, се појави прашањето дали GDPR му остава избор на контролорот на податоците да го открие или специфичниот идентитет на примателите или само категориите примачи или дали на субјектот на податоците му дава право да го знае специфичниот идентитет на примателите на податоците.

ЕСП пресуди дека оваа одредба не им дава можност на контролорите на податоци да избираат помеѓу идентификување на конкретни примачи или категории на примачи. Наместо тоа, кога одговараат на барањата на субјектите на податоците, контролорите на податоци со седиште во ЕУ мораат да го откријат вистинскиот идентитет на примателите, освен онаму каде што не е можно да се идентификуваат или можат да покажат дека барањето за пристап е очигледно неосновано или прекумерно.

### *7.3.8.2. Право на надоместок на штета и параметри*

На четврти март 2023 година, Европскиот суд на правдата ја издаде својата пресуда за случајот C-300/21, UI против Österreichische Post AG, во која заклучи дека прекршувањето на GDPR не предизвикува право на компензација за поединци. Според мислењето на Судот, член 82 бара да се утврди: (i) „штета", било материјално или нематеријално; (ii) вистинско прекршување на GDPR; и (iii) причинско-последична врска помеѓу двете. Меѓутоа, исто така пресуди дека правото на компензација во GDPR не може да зависи од поединци кои исполнуваат одреден праг на „сериозност", што е случај според австриското право во моментов.

Меѓу другото, од ЕСП било побарано да разјасни дали прекршувањето на GDPR е доволно за да се создаде право на компензација според член 82 и, понатаму, дали каква било компензација за нематеријална штета може да биде зависна од наводната штета што ја има „некоја тежина" над „вознемирувањето", ефективно задоволувајќи одреден праг на „сериозност" во австриското право.

Согласно оваа пресуда, се поставуваат и стандарди, односно насоки за надоместок на штетата. Според резонирањето на ЕСП во овој случај:

- Правото на отштета предвидено со GDPR подлежи на три кумулативни услови: постоење на прекршување на GDPR, материјална или нематеријална штета што произлегува од тоа прекршување и причинско-последична врска помеѓу штетата и прекршувањето.
- Прекршувањето на GDPR не претставува барање за отштета.
- Меѓутоа, надоместокот за нематеријална штета не зависи од достигнување на одреден праг на материјалност.
- На засегнатото лице останува да докаже дека претрпел нематеријална штета.
- Критериумите за процена на висината на штетата се препуштени на правото на земјите-членки, земајќи ги предвид принципите на еквивалентност и ефективност.
- Штетата претрпена поради прекршување на GDPR мора да се надомести „целосно".
- Ваквото целосно обесштетување не бара изрекување на казнена штета (punitive damages).[37]

37 https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3810075

# 08

# СОВРЕМЕНИ ПРЕДИЗВИЦИ ЗА ЗАШТИТА НА ПОДАТОЦИТЕ

VIII.

# СОВРЕМЕНИ ПРЕДИЗВИЦИ ЗА ЗАШТИТА НА ПОДАТОЦИТЕ

## 8.1. Технолошки напредок, алгоритми и вештачка интелигенција

Во случаите што се однесуваат на земање и складирање од страна на властите, за целите на спречување на криминалот, на отпечатоци од прсти, биолошки примероци и ДНК-профили на лица осомничени или осудени за прекршоци, Судот јасно изјави дека употребата на современи научни техники не може да се овласти по секоја цена и без внимателно балансирање на потенцијалните придобивки од екстензивната употреба на таквите техники наспроти важните приватни интереси [S. и Marper против Обединетото Кралство (GC), 2008, § 112]. Секоја држава што тврди дека има пионерска улога во развојот на новите технологии има посебна одговорност за постигнување на правилен баланс во овој поглед (ibid., § 112). Имајќи го предвид брзото темпо на развојот на полето на генетиката и информатичката технологија, можноста дека во иднина приватните интереси поврзани со генски информации негативно можат да бидат засегнати на нови начини или на начин што не може да се предвиди со прецизност денес не може да се намали (ibid., § 71).

Според мислењето на Судот, брзиот развој на сè пософистицирани техники што овозможуваат, меѓу другото, техниките за препознавање и мапирање лица да се применат на фотографиите на поединци, го прави фотографирањето на нивните фотографии и складирањето и можното ширење на добиените податоци проблематична. Домашните судови мораат да ги земат предвид овие фактори при оценувањето на неопходноста од мешање во приватниот живот на засегнатото лице (Gaughran против Обединетото Кралство, 2020, § 70). Во тој случај (ibid., §§ 96-98), Судот нагласи дека модерната технологија е посложена и дека домашните судови не му дале доволно внимание на овој аспект при испитувањето на неопходноста од мешање во правото на почитување на приватниот животот на апликантот, чија фотографија била направена од властите по мал прекршок и била задржана дури и откако неговата осуда била избришана од евиденцијата по истекот на законскиот рок.

Во Breyer против Германија, според мислењето на Судот, обврската за мобилните телефонски оператори да складираат информации за претплатниците и да ги направат достапни на властите на барање, генерално, е соодветен одговор на промените во однесувањето на комуникацијата и во во средствата за телекомуникации.

Во Szabó и Vissy против Унгарија, 2016 (§ 68), случај во врска со масовното следење на комуникациите, Судот призна дека е природна последица на формите преземени од денешниот тероризам владите да прибегнат кон врвни технологии, вклучително и масивно следење на комуникациите, со цел да се спречат неизбежни напади. Во овој случај, Судот оцени дека законодавството што дозволува масовно следење не ги обезбедува потребните заштитни мерки против злоупотреба, бидејќи новите технологии им олеснуваат на властите да пресретнат големи количества податоци што се однесуваат дури и на луѓе кои не се во категоријата првично цел на операцијата. Дополнително, извршната власт може да нареди мерки од овој вид без никаква контрола и без каква било процена дали тие се строго неопходни и во отсуство на каков било ефикасен судски или друг правен лек (ibid., §§ 73-89).

Во случајот Роман Захаров против Русија (GC), 2015 (§§ 302-305), Судот одлучи дека ризикот од злоупотреба својствен за секој систем на тајно следење е особено висок во систем каде што тајните служби и полицијата имала директен пристап, со технички средства, до сите мобилни телефонски комуникации. Судот утврди повреда на член 8, сметајќи дека руските законски одредби што дозволуваат генерализирано следење на комуникациите не обезбедуваат соодветни и ефективни гаранции против самоволието и ризикот од злоупотреба својствени за секој систем на тајно следење.

Во случајот Akgün против Турција, 2021 (§§ 178-181), каде што во времето на првичниот притвор на апликантот, наодот дека тој го користел шифрираниот систем за пораки „Бајлок“ (ByLock) бил единствениот доказ што бил обезбеден за да го оправда сомнежот, за целите на член 5 став 1 (в), дека сторил прекршок, Судот нагласи дека употребата на такви докази како единствена основа за основање на сомнежот може да постави голем број деликатни прашања, бидејќи, по својата природа, постапката и технологиите применети при собирањето на овие докази се сложени и соодветно можат да ја намалат способноста на националните судови да ги утврдат нивната автентичност, точност и интегритет (види став 373 погоре).

Во случаите Centrum för rättvisa против Шведска (GC), 2021, § 261, и Big Brother Watch and Others против Обединетото Кралство (GC), 2021, §§ 322-323, Судот изречно призна дека употребата на режимот на масовно следење не беше сам по себе во спротивност со член 8, со оглед на ширењето на заканите со кои се соочуваат државите во моментов од мрежите на меѓународните актери, кои го користат интернетот за комуникација и постоењето на софистицирана технологија што им овозможи на овие актери да избегнат откривање. Судот сепак нагласи дека со оглед на постојаниот развој на современите комуникациски технологии, неговиот вообичаен пристап кон целните режими на надзор ќе треба да се приспособи за да ги одрази специфичните карактеристики на режимот за масовно следење, поради ризикот од злоупотребени информации и на легитимната потреба за тајност во таквите операции. Процесот мора да подлежи на „заштитни мерки од крај до крај“, што значи дека, на домашно ниво, треба да се направи процена во секоја фаза од процесот на неопходноста и пропорционалноста на мерките што се преземаат; дека масовното следење треба да биде предмет на независно овластување на

почетокот, кога се дефинираат предметот и опсегот на операцијата; и дека работењето треба да биде предмет на надзор и независна ex post facto ревизија.

### *8.1.2. Интернет и пребарувачи*

Интернет-страниците се информативна и комуникациска алатка различна од печатените медиуми, особено во однос на капацитетот за складирање и пренос на информации (M. L. и W. W. против Германија, 2018, § 91). Во светлината на неговата достапност и неговиот капацитет да складира и да пренесува огромни количества информации, интернетот игра важна улога во подобрувањето на пристапот на јавноста до вестите и олеснувањето на ширењето на информациите генерално [Times Newspapers Ltd против Обединетото Кралство (бр. 1 и 2), 2009, § 27].

Ризикот од штета предизвикана од содржината и од комуникациите на интернет за остварувањето и уживањето на човековите права и слободи, особено правото на почитување на приватниот живот, секако е поголем од оној што го носи печатот, особено поради важната улогата на пребарувачите (M. L. and W. W. v. Germany, 2018, § 91 и референциите цитирани таму).

Информациите што содржат лични податоци што ги чуваат медиумите лесно можат да ги најдат корисниците на интернет преку пребарувачите (ibid., § 97). Поради овој засилувачки ефект врз ширењето на информациите и природата на активноста во основата на објавувањето на информациите, обврските на пребарувачите кон поединецот кој е предмет на информацијата можат да се разликуваат од оние на субјектот кој првично ја објавил информацијата (исто, § 97). Оттука, во случај во кој две лица побарале целосните детали за нивниот идентитет и нивните фотографии да се отстранат од онлајн-архивите на одредени весници и радиостаници откако ќе завршат со издржување на долгогодишни затворски казни за убиство (ibid., §§ 7, 12, 33), Судот утврди дека балансирањето на засегнатите интереси може да резултира со различни исходи во зависност од тоа дали барањето за бришење на личните податоци се однесува на оригиналниот издавач на информациите, чија активност генерално била во срцето на она што слободата на изразување имаше цел да ја заштити или пребарувач чиј главен интерес не беше објавување на првичните информации за засегнатото лице, туку особено олеснување на идентификацијата на сите достапни информации за тоа лице и воспоставување на негов/нејзин профил (ibid., § 97).

Според мислењето на Судот, интернет-архивите придонесуваат за зачувување и ставање на достапни вести и информации [Times Newspapers Ltd против Обединетото Кралство (бр. 1 и 2), 2009, § 45]. Ваквите архиви претставуваат важен извор за образование и историско истражување, особено затоа што се лесно достапни за јавноста и генерално се бесплатни.

Случајот Бјанкарди против Италија, 2021, §§ 67-70, му ја даде на Судот својата прва можност да одлучи за компатибилноста со член 10 од граѓанската пресуда

против новинар поради тоа што не ги деиндексираше чувствителните информации објавени на интернет. Во врска со кривичната постапка против приватни лица и одлуката на новинарот да ги држи информациите лесно достапни, и покрај противењето од засегнатите. Прашањето за анонимизирање на идентитетите во написот на интернет не се појави во овој случај. Судот забележа дека статијата останала лесно достапна на интернет осум месеци по официјалното барање да се отстрани од засегнатите лица. Тежината на санкцијата – одговорност според граѓанското, а не кривичното право – и висината на досудениот надоместок не изгледаа претерани.

## 8.2. Трансфер на податоци и текови на податоци

Во Satakunnan Markkinapörssi Oy и Satamedia Oy против Финска, според мислењето на Судот, постоењето на јавен интерес за обезбедување пристап и дозволување собирање на големи количества податоци за оданочување за новинарски цели не мора автоматски да значи дека постои и јавен интерес за масовно ширење на такви необработени податоци во непроменета форма без никаков аналитички влез. Требаше да се направи разлика помеѓу обработката на податоците за новинарски цели и ширењето на необработените податоци до кои на новинарите им беше даден привилегиран пристап (ibid., § 175). Во тој контекст, фактот дека се забранува масовно објавување податоци за персоналното оданочување на начин некомпатибилен со финските правила и правилата на ЕУ за заштита на податоците не беше, како таков, санкција, и покрај тоа што, во практиката, ограничувањата наметнати на количеството од информациите што треба да се објават можеби некои од деловните активности на компаниите апликанти ги направиле помалку профитабилни (ibid., § 197).

Случајот Big Brother Watch and Others против Обединетото Кралство (GC), 2021, го иницираше, меѓу другото, прашањето за компатибилноста со член 8 од Конвенцијата за споделување податоци пресретнати од странски разузнавачки служби, во овој случај Американската агенција за национална безбедност (NSA). Судот наведе дека размената на податоци мораше да биде врамена со јасни детални правила што на граѓаните им даваат соодветна индикација за околностите и условите под кои властите се овластени да поднесат такви барања и обезбедуваат ефективни гаранции против употребата на оваа овластување за заобиколување на домашното право и/или обврските на државите според Конвенцијата. По приемот на материјалот за пресретнување, државата на прием мора да има соодветни заштитни мерки за негово испитување, употреба и складирање; за нејзино понатамошно пренесување; и за негово бришење и уништување. Овие заштитни мерки беа еднакво применливи за добивањето, од страна на државата-договорничка, на побаран материјал за прислушкување од странска разузнавачка служба. Ако државите не знаеле секогаш дали материјалот добиен од странски разузнавачки служби е производ на прислушкување, тогаш Судот сметал дека истите стандарди треба да важат за сите материјали добиени од странски разузнавачки служби што

би можеле да бидат производ на пресретнување. Конечно, секој режим кој дозволува разузнавачките служби да бараат или прислушување или пресретнување на материјал од недоговорни страни треба да бидат предмет на независен надзор, а исто така треба да постои можност за независна ex post facto ревизија (ibid., §§ 498-499).

## 8.3. Обука на актерите и органите во рамките на правосудството

Затоа што приватноста и заштитата на податоците е сложено прашање, органите на правосудството треба да добијат специфични обуки во оваа област. Секако, оваа обука ќе го вклучува Законот за заштита на податоци, но и сите други прописи и акти што се споменати во овој водич, со акцент на ЕСЧП и практиката на ЕСЧП. Секако дека е потребно и да се добијат малку понапредни знаења од основните познавања во компјутерските науки, интернетот итн. Во времето во коешто живееме, треба да се има и специфичен фокус на новите технологии, како што е вештачката интелигенција.

## 8.4. Кампањи за подигнување на јавната свест

Треба да се спроведат кампањи за подигнување на свеста за да се информираат луѓето за заштитата на податоците, опасностите од обработката на личните податоци во онлајн-опкружувањето и нивните права, вклучувајќи ја и можноста за ефективни правни лекови и што треба да вклучуваат овие правни лекови. Исто така, ова ќе им помогне на инволвираните актери да добијат информации за нивните права, обврски, одговорности и правни средства и лекови во заштита на нивното права на приватност и нивните лични податоци.

ЦЕНТАР ЗА ПРАВНИ
ИСТРАЖУВАЊА И АНАЛИЗИ
CENTER FOR LEGAL RESEARCH AND ANALYSIS